ISSN: 2710-0170

New Challenges and Legal Responses of Big Data Criminal Investigation to Personal Information Protection

Xin Fang

Law of School, Anhui University of Finance and Economics, Bengbu, Anhui 233030, China

Abstract

Big data criminal investigation is a new investigation method developed on the basis of information technology such as artificial intelligence and cloud computing. Relying on the collection and processing of big data, it makes comprehensive use of various information technologies to mine and analyze relevant data, and then discover case clues and lock criminal suspects, which has the characteristics of high efficiency, accuracy and convenience. However, due to the practical differences between big data criminal investigation and traditional investigation methods, It poses new challenges to the protection of personal information in terms of unclear legal positioning, lack of regulation of collection scope, increased risk of disclosure by sharing, and insufficient protection and relief mechanism. It is necessary to clarify the legal positioning of big data criminal investigation from the legislative level, clarify the scope of information collection from the practical level, improve the mechanism of information sharing, and improve protection and relief channels. So as to effectively deal with the challenges brought by big data criminal investigation to the protection of personal information.

Keywords

Criminal investigation, personal information, big data criminal investigation behavior.

1. Introduction

With the rapid progress of the Internet and communication technology, human society has stepped into the information age, and personal information is closely related to people's dignity, property and other rights and interests, and the protection of personal information has become increasingly prominent. At present, scholars are particularly concerned about how to provide institutional protection for citizens' personal information in market economic activities and social interactions, especially when public authorities are committed to maintaining social security and other actions, they should be more vigilant and prudent in dealing with the risk of interference with personal information that may be triggered. As personal information is both private and public, how to balance the value of both in the criminal justice field, protecting citizens' private rights and interests as well as safeguarding public power, has become an important indicator of the degree of civilization of a country's justice. Meanwhile, with the wide application of big data technology, big data criminal investigation has become a “new type of weapon” in the field of criminal investigation, which greatly improves the efficiency of investigation and the ability to solve cases. However, while bringing convenience, big data criminal investigation has also exacerbated the contradiction between the protection of personal information rights and interests and the fight against crime. How to balance the prosecution of crimes and the protection of personal information in big data criminal investigation has become an important issue facing the construction of the current criminal procedure system[2]. Therefore, scholars have called for strengthening the theoretical research and institutional construction of personal information protection in the field of criminal procedure law, and reasonably regulating the behavior of big data criminal investigation, with

ISSN: 2710-0170

a view to realizing a dynamic balance between the prosecution of crimes and the protection of human rights in criminal procedure in the era of big data information.

2. Current legal status of personal information protection in big data criminal investigations

2.1. Current situation of legislation on personal information protection in big data criminal investigation in China

The analysis of the current state of domestic legislation on criminal investigation of big data should focus on the legal norms that are closely related to it. From the perspective of the Criminal Procedure Law, the current law focuses mainly on the protection of traditional privacy rights, and the specific regulation of big data criminal investigation and the safeguards for the security of personal information in the investigation process are still insufficient. The Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security jointly issued the Provisions on Several Issues Concerning the Collection and Extraction of Electronic Data for Handling Criminal Cases and the Examination and Determination of Electronic Data, which covers the procedural requirements for investigating authorities in the collection and extraction of electronic data, such as those relating to the number of investigators and the production of transcripts, etc. However, these provisions are still insufficient in the protection of personal information, e.g., the scope of the extraction of electronic data has not been clearly defined, and the right of consent of the subject of information is not explicitly mentioned. In addition, although the Network Security Law requires network operators to assist public security organs and national security organs in maintaining national security and combating crime, there is a lack of a clear mechanism for the consent of the parties involved in the provision of information, and the Third Party Principle is still applied, which fails to adequately protect the rights and interests of personal information. Similarly, the Data Security Law emphasizes data security protection mainly from a national perspective, and lacks provisions on data and information security protection from an individual perspective. It is worth mentioning that the Rules on Electronic Data Forensics for Criminal Cases Handled by Public Security Organs, issued by the Ministry of Public Security in 2019, has made a breakthrough in the protection of personal information. The rules not only stipulate that investigating authorities are required to fulfill the obligation of confidentiality and the obligation to return or destroy materials unrelated to the case in a timely manner when retrieving electronic data involving personal privacy, but also explicitly require investigating authorities to issue a Notice of Evidence Retrieval when retrieving electronic data, and to require the party to be retrieved to sign or stamp on the return receipt of the notice. Although the above provisions do not directly involve specific measures for the protection of personal information, they reflect the respect for the private rights of data information holders and owners, and provide a useful direction of exploration for the improvement of subsequent legal norms.

2.2. Judicial status of personal information protection in big data criminal investigation in China

In current social practice, as new types of crime are gradually becoming professionalized, roving, intelligent and virtualized, traditional investigation methods are facing great challenges due to the lagging behind of technical means and thinking concepts. In recent years, big data technology has been deeply applied to all aspects of comprehensive social security management, especially in the investigation stage, its effect is particularly significant. Characterized by its massive, real-time and high efficiency, big data can comprehensively cover the information of criminal suspects, the environment of the crime scene, the pattern of criminal behavior and the relevant social background. By collecting, modeling, screening and

ISSN: 2710-0170

comparing the huge data in the network and computer system, big data criminal investigation reveals the hidden patterns and identifies the abnormal activities of high-risk personnel, providing important clues and evidence support for the investigation, thus greatly enhancing the efficiency of the investigation. However, the application of big data also heralds a fundamental change in the mode of investigation and is accompanied by a series of emerging issues and challenges. In order to grasp the dynamics of crime in a timely manner, investigating authorities have extensively collected and utilized multi-channel personal information, which, despite the remarkable results achieved, has inevitably infringed upon citizens' personal information to a certain extent. The investigative behavior of China's investigative agencies is highly autonomous and self-disciplined, but the lack of effective supervision and restriction is prone to corruption and disorder, which may cause excessive infringement of the right to personal information. The “self-management” mechanism within the investigative organs shows an administrative tendency in practice, which undoubtedly exacerbates the risk of power abuse[4]. Due to the lack of necessary external supervision, investigating authorities often sacrifice citizens' privacy when obtaining the identity information of criminal suspects, and even take illegal means to obtain evidence. In addition, factors such as the pressure to solve crimes lead to the subjectivity of investigators in the process of information selection and processing, and the data processing process that lacks supervision may produce misleading conclusions[5]. In the process of case handling, police officers can easily access citizens' information, but this information may face the risk of leakage under the influence of subjective and objective factors. In practice, information leakage incidents occur from time to time, and it is urgent to draw great attention to them.

3. The new challenge of big Data criminal investigation to personal information protection

3.1. Legislative level: The legal positioning of big data criminal investigation is unclear

Since the addition of technical investigative measures to China's Criminal Procedure Law, the Ministry of Public Security has followed suit with the promulgation of the Provisions on Procedures for the Handling of Criminal Cases by Public Security Organs, which are designed to refine the specific investigative methods, targets of application, application procedures, implementation deadlines, the scope of application of materials, and the confidentiality duties of public security organ personnel. Among other things, article 255 clearly states that technical investigative measures cover such means as record monitoring, whereabouts tracking, communications monitoring and premises monitoring. However, this provision appears to be broad in its definition of technical means, and as a decade-old statute, some of its contents are already difficult to adapt to current technological developments. Some scholars believe that big data criminal investigation technology includes data retrieval, data matching, data mining, data modeling, criminal network relationship analysis, drone investigation and face recognition monitoring and other means[6]. It is worth noting that these big data criminal investigation techniques have both similarities and significant differences in means with traditional technical investigation measures. In the field of criminal procedure, the nature of big data criminal investigation and whether it should be categorized as a technical investigation measure are still controversial. Specifically, the law clearly stipulates that the application of technical investigative measures is limited to criminal suspects, defendants and persons directly related to criminal activities. However, in practice, the potential targets of big data criminal investigations may exceed this scope, resulting in a blurring of the boundaries of their application[7]. This ambiguity in the nature of the law makes it possible for big data criminal investigations to circumvent legal procedures in the course of execution, thus increasing the

ISSN: 2710-0170

risk of information leakage. Currently, both the Criminal Procedure Law and the Provisions on Procedures for Handling Criminal Cases by Public Security Organs lack clear provisions on the nature of big data criminal investigation, which undoubtedly poses a potential threat to personal information security.

3.2. The practical level

3.2.1. Lack of regulation on the scope of information collection

Article 6 of the Act on the Protection of Personal Information stipulates the principles of clarity, reasonable purpose and minimal impact in the handling of personal information, but the provision is broad and has certain limitations for use in big data criminal investigation activities. There is no clear standard for the scope of collection and utilization of citizens' personal information, and the risk of infringement of citizens' personal information still exists. China's laws set different scope of information collection according to the type of case, such as the Criminal Procedure Law, which focuses on the collection of human biological information from criminal suspects or victims, and the Ministry of Public Security's "Four Laws of the Road", which requires the collection of information from all suspects of criminal offenses and their proper storage. Although the above legal provisions generally stipulate the scope of collection, in practice, investigating authorities often collect information on suspects without discrimination and compulsorily, and store it in the database for investigators to query with the help of big data[8]. In addition, investigating authorities also use big data technology to collect electronic data, but the relevant regulations only stipulate the procedure without limiting the scope. At the same time, the Criminal Procedure Law stipulates that network operators are required to assist in investigations, so that investigating authorities can obtain network data such as online shopping information and chat records to understand the behavioral trajectory and interests of criminal suspects, reflecting their connection with the case and thus facilitating the investigation of the case. It is worth noting, however, that without an effective definition of the scope of information collection, the duties of investigative authorities in protecting citizens' personal information will become ambiguous, which may result in the failure to adequately protect the personal information collected.

3.2.2. Information sharing increases the risk of leakage

In investigative work, the internal sharing of personal information resources has become a key link in promoting investigative efficiency. Such sharing not only covers investigative agencies in different regions and at different levels, but also realizes the interconnection and interoperability of internal data. This mode of sharing is an effective response to the trend of increasing cross-regionalization, networking and informatization of criminal activities, and has significantly improved the problems of lack of case clues and low detection rates caused by information blockage under the traditional investigation mode. By constructing a big data sharing platform, investigative agencies have significantly improved their ability to analyze cases, handle police information and make case predictions, further promoting the process of investigative intelligence integration. However, there are still many deficiencies in the current internal sharing mechanism of investigative agencies. Barriers exist between the databases of investigative agencies at different regions and levels, and there are frequent data interactions but insufficient information security measures, increasing the risk of personal information leakage. Specifically, although many databases were initially designed to achieve uniform application by investigative agencies at all levels throughout the country, in practice, investigative agencies at all levels and in all regions, and even staff in different positions, have different data permissions. The lack of information sharing standards, the confusion in the management of personal information, the blurring of the boundaries between data openness and confidentiality, and the lack of clarity in the form of information sharing have all increased the complexity and risk of data sharing[9].

ISSN: 2710-0170

In terms of external sharing, the right to manage citizens' personal information is usually vested in third-party subjects, and investigating authorities can only realize information sharing with third-party subjects within a specific scope[10]. This sharing model makes investigative authorities face many restrictions in obtaining personal information, and also increases the difficulty of personal information protection. In practice, investigative authorities obtain massive information resources and technical support by cooperating with Internet companies in the form of signing strategic cooperation framework agreements to realize data fusion and interaction. Public security organs are the initiators and leaders of the social security management system, and they have a great positional advantage in information resource sharing, so such cooperation agreements are rarely subject to legality review. Due to the lack of public participation, the cooperation model is highly secretive, which increases the difficulty of protecting personal information at the sharing stage. At the same time, different Internet companies have different requirements and processes for sharing personal information, and lack uniform norms, further exacerbating the risk of personal information leakage.

3.2.3. The relief mechanism of information protection is insufficient

As an emerging field of big data criminal investigation, its supporting legal norms and relief mechanisms are still insufficient. When citizens' personal information is infringed upon as a result of improper big data criminal investigation measures, it is often difficult for them to effectively safeguard their rights and interests due to the lack of remedies. As a fundamental right granted to citizens by the Constitution, the right of complaint is mainly limited to illegal acts such as seizure, detention, freezing and other illegal acts, as well as acts of not lifting or changing compulsory measures in accordance with the law in the current criminal procedure law, and the protection of the right to personal information has not been given sufficient attention. Given the secretive nature of big data criminal investigation, citizens' personal information may inadvertently be collected by the investigating authorities and utilized in the case. Once citizens realize that their information has been illegally obtained or misused, the issue of compensation becomes the focus of their attention. However, according to the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Compensation Cases and the relevant provisions of the State Compensation Law, the current state compensation system mainly focuses on the protection of citizens' personal and property rights, and does not explicitly include in the scope of compensation the infringement of personal information due to the criminal investigation of big data[11]. Personal information, as important data that can identify and locate individuals and reveal the trajectory of their activities in depth, deserves legal relief and protection in the face of possible infringement, just as much as the infringement of citizens' personal and property rights and interests.

4. Legal response of big Data criminal investigation to personal information protection

4.1. Clarify the legal positioning of big data criminal investigation

The operational mechanism of big data criminal investigation differs significantly from traditional investigation methods in terms of core principles. Traditional investigation mainly focuses on case tracking and in-depth analysis of criminal facts in physical space, while big data criminal investigation focuses on all available information resources in data space. Currently, there are different opinions in the academic community about the construction of norms for big data criminal investigation. Some opinions advocate that there is no fundamental difference in logic between big data criminal investigation and technical investigation, and suggest that the section of “technical investigation” in the Criminal Procedure Law should be incorporated into big data criminal investigation and renamed as “secret investigation” to unify the regulation[6]. However, another viewpoint emphasizes that there are obvious differences in the operation

ISSN: 2710-0170

mechanism between big data criminal investigation and technical investigation, and that a section on "big data criminal investigation" should be independently set up after the chapter on "Technical Investigation Measures" to ensure the rule of law operation of big data criminal investigation. Bian Jianlin, Qian Cheng[12]. This paper tends to the second view that big data criminal investigation should be regulated independently in a chapter. In view of the differences between big data criminal investigation and technical investigation in terms of the applicable objects, means and approval process, simply categorizing big data criminal investigation into technical investigation will raise the threshold of its application, which is not only inconsistent with the current investigation practice, but also restricts the effective application of the new technology of big data criminal investigation with early warning function. Therefore, the regulation of big data criminal investigation as an independent investigative technique can be achieved without changing the established procedures for technical investigation, with full consideration of the justification of purpose and the principle of proportionality, as well as the integration of the principle of data protection and the effective connection with the Personal Information Protection Law. Under the guidance of the principle of due process, a chapter on "Big Data Criminal Investigation" was added to the Criminal Procedure Law after the chapter on "Technical Investigation Measures", which explicitly stipulates that data collection, query and retrieval, data mining and data collision, and other acts carried out by investigating authorities using big data technology on databases are all big data criminal investigations. Collision and other behaviors belong to the scope of big data criminal investigation. At the same time, it is necessary to define the scope of the database for big data criminal investigation, covering not only the basic information database of the investigating authorities, but also the information databases of other governmental authorities and social third-party databases. In addition, it is also necessary to clarify the differences in the applicable procedures between big data criminal investigation and technical investigation, standardize the applicable scope and time limit of big data criminal investigation, and ensure that investigating authorities strictly follow the legal procedures when applying big data criminal investigation, and shall not arbitrarily expand the scope of monitoring and tracking, nor shall they set the investigation period without authorization[13]. By incorporating big data criminal investigation into the system of criminal measures, it is not only conducive to standardizing the conditions for its initiation and the objects of its application, but also helps to promote the expansion of the connotation and regulatory development of intelligent investigative measures.

4.2. Define the scope of information collection

The diversity of citizens' personal information collected by big data technology provides a rich data base for investigative work. Further mining of such data can yield a huge and immeasurable amount of information. In the implementation of big data criminal investigation, investigating authorities need to clearly define the scope of collection and use of citizens' personal information to ensure that there is no uncontrolled collection and misuse of citizens' personal information, so as to avoid the security risk of citizens' personal information. When citizens' personal information is infringed upon, a clear definition of the scope will be an important basis for seeking relief. When collecting and using citizens' personal information, the first task of the investigating authorities is to clarify its purpose. The activity must be initiated strictly for the purpose of predicting or detecting cases, not to satisfy the self-interest of the investigating authorities or individual personnel, and the collection and use of information should be halted as soon as the need to detect a case disappears or is inconsistent with the purpose. The "Minimum Scope Principle" provides guidance for investigative agencies to regulate the collection and use of citizens' personal information through the use of big data[14]. In terms of information collection, whether it is data used as evidence or investigative clues, or electronic data in electronic devices, it should be carried out within the minimum scope.

ISSN: 2710-0170

Investigative agencies need to elaborate on the purpose of collection, the type of information, the objects involved and the subsequent use before collection. At the level of information use, while deep mining of metadata can help to restore the life profile of a particular individual, it may also infringe on the privacy and dignity of the individual, and thus again needs to be kept to a minimum. For minor crimes, the use of technologies such as data mining should be restricted, and in cases of serious infringement of the public interest, if there is a need to use such data mining technology, it can be activated in accordance with the prescribed procedures to assist in the investigation of the case. In addition, when information is collected and used, its relevance to the case must be ensured. For information that is not relevant to the case, the investigating authorities should avoid collecting and using it, and delete unintentionally collected irrelevant information in a timely manner. This not only protects citizens' privacy, but also ensures the legality and effectiveness of investigative activities.

4.3. Improve the sharing mechanism of personal information in big data criminal investigation

The key to standardizing the internal sharing mechanism of investigative agencies is to break down the data barriers in both vertical and horizontal directions, and at the same time to establish hierarchical and standardized sharing standards[15].Examined from the vertical dimension, it is necessary to break through the data barriers between investigative organs at different levels. The national-level data center should be jointly led by the SPP and the Ministry of Public Security, assuming responsibility for the centralized management and coordination of investigative data across the country; provincial-level investigative authorities are responsible for the operation and management of provincial-level data centers; prefectural-level municipal-level investigative authorities manage their own data centers; and grass-roots-level investigative authorities share data with their higher-level authorities without the need to set up separate independent data centers. In the horizontal dimension, it is necessary to eliminate the data barriers between investigative organs at the geographic level. National-level data centers should have the authority to search and retrieve investigative data nationwide, while provincial-level data centers should have the authority to search and retrieve data within their own provinces, and inter-provincial data sharing and cooperation between provinces can be carried out on the premise of fully safeguarding personal information. In addition, in order to deepen data sharing, the coverage of the existing national shared database should be expanded to include key basic data, but while promoting data sharing, it is necessary to be alert to the risk of panoramic surveillance that may result from excessive sharing. Therefore, clear sharing rules need to be formulated to ensure that investigative authorities at all levels and in all regions complete data cleansing, standardize data formats, and eliminate problematic data before data sharing, so as to ensure the authenticity and integrity of the data in the shared database. At the same time, corresponding operating privileges should be set according to the level of the staff, and detailed operating records should be left for the querying, collection and utilization of data in the database, so as to enable effective supervision of the sharing behaviours.

In response to the lack of review of the legality of data-sharing framework agreements signed between investigative authorities and third-party data platforms, in order to ensure the legality and compliance of the content of the agreements, an external review mechanism should be introduced on a mandatory basis to break down their inherent closedness and confidentiality. This review may be undertaken by a cyber-credit department independent of the investigating authorities and third-party data platforms, which, as a specialized agency for Internet data management, may assume this supervisory responsibility. In conducting the legality review, the focus should be on a comprehensive and detailed examination of the core elements of the data sharing agreement, including the purpose of sharing, the manner, the scope and the duration of cooperation. If the illegal or unreasonable terms of the framework agreement infringe upon the

ISSN: 2710-0170

rights and interests of citizens' personal information, the investigating authority and the third-party data platform must bear the corresponding legal responsibility. In addition, to ensure that the actual implementation of the framework agreement meets the review requirements, a regular supervision mechanism should be established to prevent investigative authorities and third-party data platforms from expanding the scope of data sharing or changing the purpose of use without authorization[9]. At the same time, under the premise of safeguarding citizens' right to know, consideration can be given to moderately publicizing the parts of the framework agreement that involve citizens' personal information, so that the public can have a clear understanding of the scope and extent of data sharing, thus achieving a balance between data sharing and personal information protection.

4.4. Perfect the way of relief

In terms of substantive remedies, drawing on the model of remedies for personal and property rights and interests in criminal proceedings, citizens who have suffered infringement of their rights to personal information in the course of criminal investigations may be entitled to request compensation from the State. In due course, the law should be amended or judicial interpretations promulgated to include the infringement of personal information rights and interests by investigative authorities in the course of performing their duties in the scope of criminal indemnification under the State Indemnification Law, to clarify that the investigative authorities are the obligated authorities for indemnification, and to provide substantive remedies for the subject of the information through the payment of indemnification. With respect to the calculation of compensation, specific implementation measures can be formulated with reference to the Personal Information Protection Law and other relevant laws, based in principle on the actual loss of the subject of information, or discretionary in accordance with the actual situation if it is difficult to determine.

At the level of procedural remedies, platforms for complaints and appeals have been set up in the internal legal departments of investigative agencies, as well as in the procuratorates, which are the regulatory bodies for personal information. When a citizen believes that an investigating authority has violated his or her right to personal information, he or she may file a complaint with the legal department of the investigating authority, which shall be responsible for reviewing and handling the complaint, and if it finds that the case-handling department has indeed violated his or her right to personal information, it shall propose corrective action and report it to the head of the investigating authority for the record. If a citizen is dissatisfied with the outcome of the legal department's handling of the case, he or she may file a complaint with the procuratorate, which shall accept and review the complaint, and if it finds that there has been a violation of rights, it may put a stop to it in a timely manner by sending a procuratorial recommendation to the investigating authority. In addition, citizens may also file complaints directly with the procuratorate, urging the investigating authorities to pay greater attention to the protection of the personal information of the subject of the investigation in the course of the investigation of the case.

Conclusion

If you follow the “checklist” your paper will conform to the requirements of the publisher and facilitate a problem-free publication process.

5. Conclusion

The widespread application of big data criminal investigation technology has injected unprecedented innovation into the field of criminal investigation and greatly promoted the transformation and upgrading of investigative work. The massive aggregation and in-depth analysis of data have increased the risk of personal information leakage. By improving relevant

ISSN: 2710-0170

laws and regulations, clarifying the legal positioning and scope of information collection for big data criminal investigation, and improving the information sharing mechanism, we can effectively respond to the new challenges to personal information protection posed by big data criminal investigation. In the future, we still need to face up to the risk of infringement of personal information due to big data criminal investigations, and persistently explore effective coping strategies to effectively respond to and solve the problems of personal information protection, so as to ensure that the protection of personal information is truly implemented and strengthened in practice.

References

[1] Li Xianghui. On the Protection of Personal Information in Criminal Investigation [J]. Journal of Fujian Police College, 2024, 38(01): 55-66.

[2] Zheng Xi. The Right of Personal Information as the right of Criminal Procedure [J]. Forum on Political Science and Law, 2019,38(05):133-144.

[3] Li Ning, YU Jingyao. On Personal Information Protection in Big Data Investigation [J]. Journal of Jiangsu Police College,2023,38(01):99-108.

[4] Ren Yongzhe: The dilemma and way out of Cyber crime investigation from the perspective of Big Data (MS., Zhejiang Gongshang University, China 2018), p.15.

[5] Chen Qiwei, Liu Qianyang. Personal Information right and its legal Protection in the era of Big Data [J]. Jiangxi Social Sciences,2017,37(09):187-194.

[6] Cheng Lei. Legal control of big data investigation [J]. Chinese Social Sciences,2018,(11):156-180+206-207. (in Chinese)

[7] Liu jiyang: Criminal litigation areas for personal information protection research. (MS., Shanxi university of finance and economics, China 2023), p.24.

[8] Jiang Yong. Introduction of personal information right into investigation procedures in the era of big Data [J]. Journal of Wuhan University (Philosophy and Social Sciences), 2019, 72 (03): 156-164.

[9] Chen Lu: Research on Personal Information Protection in Big Data Investigation. (MS., Zhejiang Gongshang University, China 2023), p.18.

[10] Wang Liming. Data Sharing and Personal Information Protection [J]. Modern Law,2019,41(01):45-57.

[11] Jiao Zixuan: Research on the Protection of Citizens' Personal Information in Big Data Investigation. (MS., Inner Mongolia University,China 2023), p.21.

[12] Bian Jianlin, Qian Cheng. Application limits and procedural regulations of big data investigation [J]. Guizhou Social Science,2022,(03):78-86.

[13] Miao Xianggong: Research on Application of Big Data Investigation and its legal Regulation. (MS., Central South University,China 2023), p.12.

[14] Pei Wei. Procedural Regulation of data investigation -- Based on investigation behavior correlation [J]. Law Science (Journal of Northwest University of Political Science and Law),2019,37(06):43-54.

[15] Wang Yan: Big Data Investigation (Tsinghua University Press, China 2017). p.32.