Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.122, 2022

Legal Dilemmas Encountered in the Judicial Practice of Big Data Investigation in China and Some Suggestions for Improvement

Shuang Zhang*
Criminal Law School, East China University of Political Science and Law
No.1575 Wan Hang Du Road, Shanghai, 200042, China

Abstract
Today's big data technology has spread to all areas of society, and the criminal justice sector is no exception. In Chinese criminal justice practice, big data technology has become one of the most common tools used by the police to handle criminal cases and is often used to prevent and combat crime. Given the rapid development of big data technology in China and the many advantages of its application in Chinese judicial practice, its use is becoming increasingly widespread. One of the most prominent applications of big data technology in the criminal justice sector is big data investigation. However, Chinese law does not explicitly regulate big data investigation, and there are still some legal difficulties in its use in criminal justice practice. For example, there are difficulties in the application of Big Data investigation in terms of legal attributes, cross-border data jurisdiction, applicable procedures, interference with privacy and personal information, and Big Data technology bias that need to be resolved. In order to promote a more rule of law for big data investigation in China's judicial practice, the current legal dilemmas faced by big data investigation can be solved by clarifying the legal attributes of big data investigation, solving the difficulties of cross-border big data jurisdiction, regulating the application procedures of big data investigation, coordinating the balance between big data investigation and the right to privacy and personal information, and setting up an independent big data supervision body.
Keywords: Big data investigation, privacy, personal information, legal attributes, cross-border data jurisdiction, data regulators
DOI: 10.7176/JLPG/122-06
Publication date: July 31st 2022

1. Introduction

In China, big data technology is developing at an increasingly rapid pace, and big data investigation should also keep pace with the rapid integration into the criminal justice field. Big data technology has not only changed the operation of traditional crime but also influenced the prevention and combating of crime. On the one hand, criminals use big data technology to commit criminal acts more covertly and the selection of criminal targets is more precise; on the other hand, criminals use big data to commit criminal acts also brings many challenges to the police, and it becomes more difficult for the police to combat and prevent criminal activities. Given the advantages of big data technology in analysing and predicting criminal behaviour, more and more Chinese police officers are applying big data technology in the process of handling criminal cases. The term "big data investigation" has since spread. In China's judicial practice, big data investigation has gradually become a major tool for Chinese public security authorities to investigate criminal cases (Hongkui 2016), and is widely used by police officers in handling various types of criminal cases.

However, China's existing laws do not have clear provisions on big data investigation, and the judicial staff's understanding of big data is often in a vague state. As a result, judicial practice encounters many dilemmas with respect to big data investigations, such as the lack of uniform understanding of the legal attributes of big data investigations, the ambiguity of cross-border data jurisdiction, the lack of clear legal procedures governing the implementation of big data investigations, the excessive interference of big data investigations with privacy and personal information, and the inherent flaws of big data technology used by the police.

Based on comparing the differences between big data investigation and traditional investigation, this paper specifically analyses the problems encountered by big data investigation in Chinese judicial practice and then puts forward some targeted improvement strategies to provide solutions for the judicial research of big data investigation in China. The first part of the paper briefly introduces the purpose of the study and an overview of big data investigation, the second part specifies the differences between big data investigation and traditional investigation; the third part focuses on the dilemmas encountered in big data investigation in Chinese judicial practice; the fourth part proposes some targeted improvement strategies, and finally, the conclusion part briefly summarises the findings of the article.

2. China's Big Data Investigation is a New Stage of Development Based on Traditional Investigation

Traditional investigations focus on the legal control of individuals' rights to personal freedom and property in physical space. Unlike traditional investigation, big data investigation focuses more on virtual personal data, and functions through the collection, processing and use of personal data (Jun 2021). In terms of the relationship

between the two, big data investigation and traditional investigation are a kind of backward and forward, with hierarchical progression, close relationship between the two development stages. To a certain extent, big data investigation can be regarded as a kind of expansion of traditional investigation power in line with the development of the times. In the big data investigation, it retains the traditional investigative powers on the basis of some new expansion, mainly in the following aspects.

2.1 Big Data Investigations Move from Traditional Cause-and-Effect Thinking to Correlation Thinking

Traditional investigation is dominated by causality, and big data investigation is dominated by correlation. In traditional investigation activities, the direct and ultimate purpose of investigation is to meet the investigative needs of collecting evidence, fixing evidence, and apprehending suspects to pursue crimes (Xingyi 2021), a necessarily cause-and-effect thinking. In traditional investigation activities, its theoretical basis is causality (Chunle *et al.* 2021), deducing a unique conclusion based on the evidence obtained, and its results have uniqueness and certainty. In big data investigation activities, the purpose pursued by the traditional investigation is only part of it. In crime prevention and crime fighting activities, big data investigation uses more correlation thinking to prevent and detect crime, and it uses the correlation between the collected data to describe the correlation between individual data and the facts of the case, and the result obtained is a higher degree of correlation and possibility.

2.2 Big Data Investigation Moves from Reactive to Active Detection

According to Article 151 of the Chinese Criminal Procedure Law, traditional investigation activities are generally carried out only after the victim has reported the crime and the public security authorities have opened a case. Under the traditional crime investigation model, investigation activities are only initiated after the public security authorities have opened a case, which is a passive mode of investigation by the investigating authorities. Usually, traditional crime investigation is based on the objective existence of criminal acts and facts of the case, based on the collected criminal evidence, according to the investigative experience and investigative techniques to identify suspects (Zhiyuan 2019). In the big data investigation activities, most of the investigation activities are not opened based on the victim reporting the crime and the public security organs opening a case, mostly a proactive investigation mode. In judicial practice, based on the concealment of big data crime cases and the timeliness of big data crime evidence collection, the opening of many big data investigation activities rely on the initiative of the staff of the investigating authorities to open, and there may not be a specific victim reporting at the time of opening, a proactive mode of prevention of possible criminal acts.

2.3 Big Data Investigation is an Expansion from Post-Investigation to Pre-Investigation

Traditional investigation is a single-track operation of the interrogation model, which is dominated by the pursuit of the value of crime control, belongs to a retrospective mode of investigation, is after the crime occurred, according to the clues provided by the informant to carry out a series of investigative activities (Zhiyuan 2019). Big data investigation is a kind of ex-ante preventive measures, its criminal investigation activities to advance to the case have not been fully formed, that is, big data investigation to intervene in the process of crime implementation, when there is no clear victim, is a kind of ex-ante investigation. In criminal activities involving big data types, there is a long time lag between the act and the harmful result, if the traditional ex post facto investigation model is adopted, it will encounter considerable challenges in fixing the criminal evidence in a timely and effective manner. In current judicial practice, big data investigation has been extended to ex-ante in the process of investigating cases such as cybercrime and telecom fraud.

3. Legal Dilemmas Encountered in the Judicial Practice of Big Data Investigation in China

In Chinese judicial practice, there are still many difficult legal control points for big data investigation that have not yet been resolved, mainly the legal attributes of big data investigation, the issue of cross-border jurisdiction of data, the issue of big data investigation procedures, the issue of interference with privacy and personal information, and the issue of technical bias of big data investigation technology itself.

3.1 Unclear Whether the Legal Attributes of Big Data Investigation are Arbitrary or Mandatory Investigative Measures

At present, it is widely believed that the purpose pursued by big data investigation is focused on both predicting crime and fighting crime (Gang 2020). However, the theoretical and practical circles do not have a uniform understanding of the legal attributes of big data investigation. Many scholars consider big data investigation as a compulsory investigative measure from different perspectives. Some Chinese scholars compare big data investigation with the technical investigation measures recognised by China's Criminal Procedure Law. In China, technical investigative measures usually refer to specialized technical means such as electronic eavesdropping, telephone tapping, electronic surveillance, secret photography or secret acquisition of certain physical evidence,

and mail inspection (Jianlin & Chen 2022). They argue that big data investigation is similar to technical investigation in terms of technicality, secrecy and time of investigation, and therefore, it should also be identified as compulsory investigation in terms of characterization (Junbin 2021). Some scholars do not recognise the caste relationship between big data investigation and technical investigation, but see them as a juxtaposition, and consider that big data investigation measures involve citizens' privacy in terms of the degree of interference with citizens' rights, and should be included in compulsory investigation measures (Ke 2019).

In judicial practice, it is believed that the law does not explicitly stipulate the specific attributes of big data investigation, nor does it include it in the scope of technical investigation, and big data investigation is mainly used to prevent crime and combat crime, so it can be considered as an arbitrary investigative measure. If it is classified as a mandatory investigative measure, it will be bound by the layers of mandatory investigative measures, which will affect the efficiency of investigation and case handling. Moreover, some special types of crime, such as cross-border crime, cybercrime and telecoms fraud, would be extremely disadvantageous if they were investigated after the occurrence of the crime and would make it extremely difficult to save people's losses at a later stage.

3.2 Ambiguity in Cross-Border Jurisdiction over Data in Big Data Investigations

To some extent, the flow of data renders jurisdiction, traditionally characterised by geographical boundaries, ineffective. Chinese judicial practice often adopts the principle of "tangential" jurisdiction over big data crime cases, i.e. jurisdiction is available wherever there is some connection with big data crime. According to China's Criminal Procedure Law, the Interpretation of the Criminal Procedure Law and other laws and regulations and judicial interpretations, the places with jurisdiction include the location of the server used for the network service during the stage of committing the crime, the location of the network service provider, the location of the infringed information network system and its administrator, as well as the location of the information network system used by the defendant and the victim in the process of committing the crime, the location of the victim at the time of the infringement, and the place where the victim's property was damaged. the place where the victim's property was damaged. Although Chinese law provides detailed provisions on big data jurisdiction and basically establishes the principle of relevance of data jurisdiction, there is still controversy as to whether there is jurisdiction over data stored outside of China. For example, if a company from country A in China holds a large amount of service data of Chinese citizens and enterprises based on various services, but the data it obtains is not stored in China, can China's investigative authorities freely access the data and analyse it, and what are the specific procedures for accessing it? For example, in the famous case of Microsoft v. Ireland, Microsoft refused to hand over the user information stored in its cloud servers in Ireland to US law enforcement officials on the grounds that the data was stored outside of the country and was not under US jurisdiction (Bin & Minxian 2021). Currently, many countries are faced with the paradox of strongly supporting open data as a catalyst for technological development, while at the same time calling for comprehensive data protection to defend digital sovereignty as an integral part of national sovereignty (Shin-Yi *et al.* 2021).

3.3 Lack of a Clear and Complete Legal Regulatory Process for Big Data Investigations

At this stage, the legal procedures involving big data investigation in Chinese law are not yet perfect. People still have certain doubts about the legitimacy of big data investigation. The imperfect legal procedures of big data investigation are mainly reflected in some of the following aspects: the initiation time of big data investigation, initiation subject, the scope of application, application period, approval method, approval procedure, supervisory body and remedy channels.

With regard to the time of initiation, according to Article 115 of China's Criminal Procedure Law, the public security organs can only initiate investigation procedures for criminal cases that have already been filed, and there is no possibility of investigative intervention in cases that have not been criminally filed or that involve administrative or civil matters. Moreover, in order to prevent arbitrary initiation of investigative powers and arbitrary interference with citizens' rights, China's criminal procedure law sets the filing of a case as a prerequisite for the initiation of investigative powers (Lei 2018). In practice, big data investigation does not strictly adhere to the standard that investigation activities should be initiated by criminal filing and often breaks through the boundary of the Chinese Criminal Procedure Law which stipulates that investigation can only be conducted after criminal filing, and expands to a broader pre-filing stage. In terms of initiating subjects, it is unclear whether big data investigation should only give the public security authorities the right to initiate it, and whether the procuratorate and the supervisory committee can be the subject of initiating big data investigation. The scope of application, mainly including the object and type of application of two aspects. At this stage, the object of application of big data investigation is not clear. In terms of the applicable period, Article 151 of China's Criminal Procedure Law limits technical investigation measures to a single three-month period, but the law does not have any regulation on the duration or number of big data investigations. In terms of approval methods, there is no unified form of regulation for the approval of big data investigations. In terms of approval

procedures, there is a great deal of discretion as to which department of the public security organs or procuratorial organs will decide to initiate big data investigation activities. In terms of supervisory bodies, the law has not yet identified a specific supervisory body to specifically supervise big data investigation activities. In terms of remedies, the remedies and procedures related to big data investigation are also in a state of absence for the time being. There is no specific procedure to remedy judicial infringement related to big data.

3.4 Interference with Privacy and Personal Information in Big Data Investigations

Big data investigations have had a number of negative effects while significantly increasing the efficiency of investigators, the most prominent of which is the interference with privacy and personal information.

In big data investigations, the processing of fragmented data may not pose a threat to the privacy or personal information of individuals. However, according to the "mosaic theory", when cross-collision of big data is carried out, some relatively complete personal information is often obtained from it, causing infringement on the privacy and personal information of individuals. In Chinese judicial practice, big data technologies have a high potential to infringe on citizens' privacy and personal information. In the big data collection phase, huge amounts of personal data information need to be collected to construct the scope of the data search. Moreover, investigators in most cases do not inform citizens in advance when collecting personal data information, and on some occasions do not accurately inform citizens of the purpose of use and the scope and duration of application when collecting personal data. Data subjects also do not have the right to delete irrelevant information collected by the investigative authorities. In short, while big data investigations provide investigating authorities with more efficient crime control tools, they also interfere with citizens' privacy and personal information beyond what is acceptable in traditional investigations.

3.5 The Technical Bias Inherent in Big Data Technology

By its very nature, big data detection is an act of processing massive amounts of data. The act benefits from the computer algorithms behind it, which are developed and designed by real human individuals in the real world. The creators and designers of Big Data algorithms invariably mix in personal value judgements and value choices when formulating them. The historian of technology Melvin Kranzberg also argues that technology and social ecology interact, with the same technology producing different results in different contexts (Hydén 2020). Big data investigation relying on computer algorithms is not a truly objective analysis and is inevitably influenced by the subjective values of the algorithm's creator or designer, creating a "black box of data power" (Hongtao & Xiyue 2020) that leads to technological bias and injustice in terms of gender, colour, race, religion, geography and other aspects of discrimination. Similarly, from a social science perspective, the values and biases of those who provide the data and code design for an algorithm can influence its construction, even when the best intentions are to create algorithms that make people's lives better (Hydén 2020). Moreover, from a normative perspective, a computer algorithm is a technical instruction designed to perform a certain service (Hydén 2020), and it is implicitly a purpose-oriented value judgment or value choice. In judicial practice, big data investigation has a clear assumption of investigative tasks before it is applied, i.e., the detection of various possible crimes as its service value.

4. Some Suggestions for Enhancing the Science of Judicial Practice of Big Data Investigation in China

In China's judicial practice, there are mainly five outstanding problems with big data investigation as mentioned above. In order to promote more scientific and standardised big data investigation in judicial practice in China, targeted improvements can be made in the following aspects to better utilise the value of big data investigation in preventing crime and fighting crime.

4.1 Phased Clarification of the Legal Attributes of Big Data Investigations

Some Chinese scholars believe that big data investigation is a kind of compulsory technical investigation (Jie 2016). There are also scholars who hold the opposite view that the scope of application of big data investigation does not conform to the scope of application of technical investigation as stipulated in Article 148 of the Criminal Procedure Law, and therefore does not recognize its legal status of technical investigation (Yang & Junbin 2018) and deny that all big data investigation is compulsory. Chinese scholar Ran W. also believes that there are certain differences between big data investigation and technical investigation in terms of application scope, application procedures and specific contents (Ran 2017). This paper argues that in order to clarify whether big data investigation belongs to mandatory investigation or arbitrary measures, it should be determined from the act of big data investigation and the stage it is in. In terms of big data investigation behavior, it is mainly data collection, data mining, and data analysis. The different acts of big data investigation should also be identified separately. From the big data investigation in the stage, big data investigation can be divided into two stages based on whether there is a clear object of investigation. The former stage does not have the exact object of investigation, and the latter stage generally has a clear object of investigation. In the former stage, there is no

clear target for investigation, the main task is to prevent crime and the damage caused to the individual is relatively minor or even insignificant, so it can be considered as an arbitrary measure. In the latter stage, when there is a clear target, the examination standard should be raised in time to give more attention to the protection of human rights, to prevent the alienation of big data technology from causing irreparable harm to individuals, and to gradually shift to the examination of higher-level mandatory investigation measures, so as to promote a better balance between the protection of human rights and the punishment of crime.

4.2 Treating Data Sovereignty as a Form of Sovereignty Breaks Down the Difficulties of Cross-Border Big Data Jurisdiction

In Chinese judicial practice, the regulation of transnational data jurisdiction is not perfect. In practice, it mostly adheres to the data storage jurisdiction model, i.e. strict data storage laws and regulations are in place to restrict data to the territory. Article 37 of China's Network Security Law, Article 31 of the Data Security Law and Article 40 of the Personal Information Protection Law all provide that operators of critical information infrastructures shall store personal information and important data within China, and that when such data needs to be provided outside of China, it must be subject to a strict security assessment by the state's Internet information department beforehand. The issue of jurisdiction over personal data stored outside of China involving Chinese citizens is not clearly defined in Chinese law.

Articles 44 and 45 of the EU GDPR restrict the transfer of data outside the EU to ensure that all personal data of EU residents is processed in accordance with the highest data protection standards. Some scholars also claim that data is part of national sovereignty and that the state has the right to regulate, restrict or even prohibit the free flow of data (Shin-Yi *et al.* 2021). This paper argues that, in terms of offshore data jurisdiction, China can also draw on the "long-arm jurisdiction" of the US or the "data sovereignty" principle of the EU's GDPR, recognising to a certain extent that data is also part of a country's sovereignty, and that no country can No country may exercise jurisdiction in any form on the territory of another country. Therefore, Chinese investigative authorities should enjoy legal investigative powers over big data obtained in China, regardless of where it is stored. China should also view data as an intangible but valuable property, and as long as the data is generated in China, China should enjoy legal "data sovereignty" similar to territorial sovereignty, regardless of where it is stored.

4.3 Improving Procedural Laws Related to Big Data Investigation

In the different stages of big data investigation, the procedures can be adapted to them respectively. In terms of initiation time, big data investigations are mostly focused on data collection in the early stages, and are at the stage of arbitrary investigative measures, which interfere less with the individual's right to privacy and personal information, and can be set up with more relaxed procedures. In the later stage, big data investigation interferes with individual human rights to a deeper extent, and should be strictly limited, and can only be initiated after the case is filed, in order to maximize the protection of human rights. On the subject of initiation, the subject of big data investigation should not be completely restricted to the public security organs, the procuratorial organs and supervisory organs should also have the right to start big data investigation when there is a need to handle the case. In terms of scope of application, big data investigation can be applied to all citizens, including those without and with limited criminal responsibility. When applying to minors, care should be taken to protect their legitimate rights and interests. In terms of the types of applicable cases, a detailed catalogue of applicable criminal cases can be formulated according to the technical strengths and practical needs of big data investigation, so as to prevent the abuse of big data investigation. In terms of the period of application, the provisions of the Chinese Criminal Procedure Law on technical investigation measures can be borrowed, with a time limit of 3 months each time, and in case of difficult and complicated cases, an extension can be applied for, but each extension cannot exceed 3 months. In terms of approval methods, written approval may be implemented. In terms of approval procedures, corresponding approval authorities may be set up for the public security authorities, the procuratorial authorities and the supervisory authorities. In terms of supervisory bodies, a separate provincial big data supervisory body can be set up in the Chinese government agencies for regulation, to ensure that the big data supervisory body can manage and supervise the use of data in a more impartial and objective manner. In terms of remedies, a special remedy department can be set up at the provincial level to receive complaints and grievances regarding big data investigations. For the relevant investigation departments to implement big data investigation in violation of the law can be sent to their subjective organs administrative rectification or punishment recommendations. In serious cases, corresponding criminal responsibility can be pursued.

4.4 Balancing Big Data Detection with the Need for Privacy and Personal Information

Big data is generally regarded as the oil of the post-industrial era (Shin-Yi *et al.* 2021), and all areas of society are scrambling to grab various data resources. Big data investigation is also valued by investigative authorities

due to its prominence in judicial practice. However, it is not appropriate for criminal investigation power, as a highly compulsory public power of the state, to infringe too much on the private rights and interests of individuals (Mei & Yunan 2021). How to balance big data investigation with the protection of individual privacy and personal information is an issue that we need to address urgently. To this end, we can strike a balance in the following two aspects.

First, the relationship between big data investigation and the right to privacy and personal information should be correctly understood. The relationship between big data investigation and the protection of personal privacy and personal information is not an incompatible and irreconcilable contradiction. There is no essential value opposition between the two, and there is a high degree of consistency in the intrinsic values pursued.

Secondly, improve the mechanism for protecting the rights of big data investigation. According to the relationship between big data investigation and privacy and personal information, corresponding protection mechanisms can be introduced to strengthen the protection of individual rights in order to moderate the conflict between the rights and obligations of both parties. Specifically, an informed consent system, a correction and deletion system and a data hierarchy management system can be introduced. An informed consent system means that citizens should be informed of their rights and their consent should be obtained when interfering with their rights. In big data investigation, in the first stage, as there is no specific target and no interference with the individual rights of citizens, there is no need to inform, but in the later stage, as there is a clear target and it may cause damage to the individual rights of citizens, citizens should be informed in detail and their written consent should be obtained. The system of correction and deletion means that the right to correction and deletion is given to the data subject in the process of big data investigation. The data hierarchy management system means that a lower management threshold should be set for the analysis data in the early stage of big data investigation, and a relatively higher level of supervision system should be set for the analysis, mining and processing stages in the later stage of the investigative authorities.

4.5 Setting an Independent Data Regulator in China to Address the Technical Shortcomings of Big Data Detection

From a normative point of view, algorithms are inherently normative and are based on specific purposes, which are often not public or transparent (Hydén 2020). Data algorithms are not a form of "visible justice" in relation to the general public. In judicial practice, it is very easy for computer algorithms to rationally guide or even influence the value choices and value judgments of investigators. In the face of fairness and justice, people not only want to know the "what" of the result, but also the reason for the result in a visible way, i.e. the "why". Effective big data investigations in China cannot be carried out without the support of supervisory authorities. The EU Data Protection Act stipulates that each member state should establish an independent supervisory authority. To this end, China can learn from the EU GDPR's experience of big data regulation, set up a special big data supervisory body, establish an algorithmic regulatory mechanism, an ethical review mechanism and a supervisory and accountability mechanism.

Algorithm regulation mechanism, i.e. the establishment of a fair and rational algorithm operation model. Ethical review mechanism, i.e. an ethical review committee composed of people with multidisciplinary knowledge backgrounds in law, big data technology, ethics, etc. to evaluate the algorithms in big data investigation in terms of law, technology and ethics (Ran 2018). Illegal data destruction procedures should be initiated when the collected data violates the law or ethics, and the illegal data should be completely destroyed. Supervisory and accountability mechanisms, i.e., setting up a special accountability department within the big data supervisory body to receive complaints from individuals or units and to protect the rights of the subjects of big data investigation. When the complaint is found to be true, the unit or individual can be warned, fined and other measures, and the unit in violation of the relevant provisions can be put forward to the person in charge of the unit or the person directly responsible for the case certain warnings and recommendations for rectification, and the consequences or circumstances seriously violate the criminal law to pursue the corresponding criminal responsibility.

5. Conclusion

The new round of global technological revolution is still emerging, big data technology with its unique advantages to rapidly occupy the major areas of society and become the leading force of the new round of technological revolution. At present, big data is a national strategy for China's economic and social development. In the criminal justice field, China should give full play to data information to promote social harmony and stability, to better stimulate the vitality of big data, to more fairly and justly protect the legitimate rights and interests of the people, and to promote the growth of big data investigation in the criminal justice field. In the era of big data, Chinese police should also pay more attention to safeguarding and protecting human rights while preventing and combating crime, and pay more attention to procedural science when using big data investigation. Specifically, when using big data investigation, the police should take into account both the need to protect the

public interest and the protection of individual privacy and personal information. In terms of addressing the inherent technical shortcomings of big data investigations, Chinese judicial practice should focus on enhancing the supervision of data by third-party regulators and strengthening the objectivity of data. In terms of rights remedies, China should set up a more complete system of rights remedies for big data investigations in order to protect the rights of individual citizens.

References:

Bin, L., & Minxian, L. (2021). Research on the Cross-border Electronic Collection under the Conflict of Big Data Sovereignty Jurisdiction. *Law Science Magazine*, 42(08), 147-161.

Chunle, N., Guangqi, L., & Han, Z. (2021). Research on the Investigation Cognition from the Epistemology of Big Data. *Journal of People's Public Security University of China (Social Sciences Edition)*, 37(03), 33-43.

Gang, C. (2020). Explanation and Regulation: Big Data Investigation under the Principle of Legal Procedure. *Law Science Magazine*, 41(12), 1-17.

Hongkui, H. (2016). Big Data Era and Academic Innovation in Investigation. *Journal of People's Public Security University of China (Social Sciences Edition)*, 32(06), 38-43.

Hongtao, N., & Xinyue, H. (2020). Analysis on the Application of Big Data Detection Technology in Intellectual Property Crime. *Science Technology and Law*, (4), 57-64.

Hydén, H. (2020). AI, Norms, Big Data, and the Law. *Asian Journal of Law and Society*, 7(3), 409-436.

Jianlin, B., & Chen, Q. (2022). Limits of application and procedural regulation of big data investigations. *Guizhou Social Sciences*, (03), 78-86.

Jie, L. (2016). How the Criminal Law Protects Privacy: A Review on Personal Information Protection in the 9th Amendment of Criminal Law. *Jinan Journal (Philosophy & Social Sciences)*, 38(12), 118-125.

Junbin, W. (2021). Risk Prevention and "Consciousness" Correction of Big Data Investigation. *Journal of Dalian University of Technology (Social Sciences)*, 42(02), 89-97.

Jun, H. (2021). Study on the Legal Character and Regulatory Rules on the Act of Data Investigation. *Journal of People's Public Security University of China (Social Sciences Edition)*, 37(01), 78-85.

Ke, Z. (2019). Construction of a procedural control system for big data investigative measures: prerequisites, core and guarantees. *Oriental Law*, (06), 87-94.

Lei, C. (2018). Legal Control of Big Data Investigations. *Social Science in China*, (11), 156-180.

Mei, L., & Yunan, C. (2021). From Conflict to Integration: The Construction of Rules for the Protection of Citizens' Personal Information in Criminal Investigation. *Research on Rule of Law*, (05), 34-45.

Ran, W. (2017). Big Data Investigation. Beijing: Tsinghua University Press.

Ran, W. (2018). Research on the change of investigation model and its legal issues in the era of big data. *Law and Social Development*, 24(05), 110-129.

Shin-Yi, P., Ching-Fu, L., & Streinz, T. (2021). Artificial Intelligence and International Economic Law. New York: Cambridge University Press.

Xingyi, W. (2021). The Paradigm Shift in Criminal Investigation Statutes in China. *Nanjing University Law Journal*, (03), 41-56.

Yang, Y., & Junbin, W. (2018). Conflict and Bridging: Personal Information Protection under the Mode of Big Data Surveillance. *Journal of Intelligence*, 37(12), 147-155.

Zhiyuan, G. (2019). Transformation of Investigation Mode of Future Crimes in Context of Big Data. *Journal of Lanzhou University (Social Sciences)*, 47(02), 34-42.