

## Legal regulation of big data killing

-- From the perspective of "Personal Information Protection Law"

Yanbing Cao<sup>†</sup>, Mengze Yang<sup>†</sup>

Department of Law, Northwest Normal University, Gansu, 730070, China

<sup>†</sup>These authors contributed equally

**Abstract.** As a new problem arising from algorithm and information abuse in the data age, big data killing is difficult to be regulated by law before the promulgation of the Personal Information Protection Law, and the relevant judicial practice is not mature enough. The implementation of the Personal Information Protection Law clearly prohibits the killing of big data from the perspective of protecting personal information, and makes comprehensive provisions from the three stages of personal information collection, processing and application. However, the relevant regulations are not perfect, and the right to carry personal information and the impact assessment system of personal information protection still need to be clarified. In terms of information compliance, the government and enterprises should build a multi governance mechanism to improve personal information protection and governance capabilities.

**Keywords:** Big data killing; Personal Information Protection Law; Algorithm personalized pricing.

### 1. Introduction

With the advent of the information society and the rapid development of the digital economy, data has been used more and more widely in the field of Internet platform economy. However, a series of data related issues have emerged, among which big data killing is a hot and influential issue in recent years. In 2020, Professor Sun Jinyun from the School of Management of Fudan University led a team to conduct field research on taxi hailing software, and found that the proportion of Apple mobile phone users who were ordered by drivers of high-priced vehicles was three times that of non-Apple mobile phone users, and the platform discount enjoyed by Apple mobile phone users was significantly lower than that enjoyed by non-Apple mobile phone users. In April 2021, the Internet platform enterprise administrative guidance meeting jointly convened by the General Administration of Market Supervision and other three departments pointed out that the problem of big data killing must be seriously addressed. Data is the core factor of production in the development of digital economy, so it is difficult to fundamentally eliminate big data killing, but this does not mean that we are "helpless". For example, we can promote top-level design and regulate it by modifying and interpreting laws.

For the problem of big data killing, the academic community, from the perspective of consumer rights protection, advocates to use the E-commerce Law of the People's Republic of China, the Price Law of the People's Republic of China, the Consumer Rights Protection Law of the People's Republic of China and other relevant laws to regulate, but in legal practice, the above laws are difficult to apply. However, the implementation of the Personal Information Protection Law of the People's Republic of China clearly prohibits the killing of big data from the perspective of protecting personal information, and is expected to regulate the killing of big data. Therefore, this paper studies the regulatory role of the Personal Information Protection Law of the People's Republic of China on big data killing, discusses its problems in practical application and puts forward optimization suggestions.

## **2. Definition of big data killing**

### **2.1 Concept**

At present, the academic community has not yet formed a unified conclusion on "what is big data killing", and each has its own views. For example, Zou Kailiang and Peng Rongjie in the article "Legal characterization and regulation of big data" killing "- a two-dimensional perspective based on" algorithm "regulation and consumer rights and interests protection" think that big data killing is a betrayal of business ethics and commercial civilization, and a substantial violation of the obligation of "clearly marking prices", It belongs to negative price fraud; Jiang Ye believed in the article "Algorithm training and algorithm training: legal regulation of algorithms in the age of artificial intelligence" that big data killing is a differentiated pricing behavior caused by businesses by collecting information about user consumption behavior, forming user portraits and using algorithm bias; In the article "Research on the Typology of Algorithm Infringement and Legal Response - An Extension of Algorithm Regulation Based on the Personal Information Protection Law", Wang Ying believed that big data killing is an algorithm that collects user data for user portraits, provides different pricing according to user preferences, and achieves precision marketing and maximizes revenue. In fact, it is a kind of "price discrimination".

### **2.2 Origin**

#### **2.2.1 Technical conditions provided by algorithm**

In terms of technical conditions, the "black box" feature of the algorithm makes it easy to fall into discrimination. First of all, the algorithm itself has a technical threshold. Without professional learning, it is difficult for the general public to understand its operating mechanism, such as the background, elements and procedures of the algorithm. Secondly, the algorithm is covert. In order to protect trade secrets, platform operators generally do not disclose the process of algorithm processing users' personal information. Moreover, the algorithm has poor interpretability, and developers cannot explain or even know every logical relationship behind the algorithm, which makes it difficult to realize the user's "right to be explained". In addition, algorithm designers have the idea of pursuing profits, which makes it difficult to reasonably use the algorithm in a neutral manner. They often provide better conditions to attract users with higher potential value, which will undoubtedly make other users suffer unfair treatment. With the help of technology, some platform operators make use of their information asymmetry advantages with users to analyze and portray personal data related to consumers' consumption habits, purchasing power, etc.

#### **2.2.2 Users are at a disadvantage**

Platform operators often use "long" and obscure "package" agreements, such as Privacy Policy and User Agreement, to generally describe the user's personal information that may be collected by the platform and the way to use it. However, they are often unable to accurately locate the specific personal information and explain how to use it. Users are often unwilling to read or cannot understand these "lengthy" agreements, so users may not know the specific content and purpose of their personal information collected and used. The relevant data and pricing algorithm of personal information are in the hands of operators, while users cannot know when their information is collected and where it is used, or whether their personal information is used illegally. On the one hand, users cannot compare costs, and can only accept the commodity information presented on the platform page in a one-way manner. On the other hand, due to the limited number of platforms, the prices of each platform are similar, resulting in a small space for users to choose. Therefore, although users are the main body of personal information, they are trapped in an information blind spot and are at a disadvantage of information asymmetry. The platform and users present a stock game state of "the strong are always strong, and the weak are always weak".

### 2.2.3 Supervision faces many difficulties

The continuous development of the information age is impacting the original order of the market operation, bringing multiple challenges to the government's supervision of the platform economy. First of all, different types of platforms, such as e-commerce platforms, online car hailing platforms, and search platforms, have different business operation models, and different platforms have different problems and regulatory priorities. The diversity of platform models makes it difficult to fully apply the current single regulatory model. Secondly, as the big data killing involves multiple regulatory fields and is jointly supervised by the Ministry of Industry and Information Technology, the Internet Information Office, the Market Supervision Bureau and other departments, it is easy to have unclear rights and responsibilities, multiple management and other situations in judicial practice, resulting in low regulatory efficiency of big data killing and even the absence of a regulatory vacuum. In addition, the supervision mode of big data is relatively backward. At present, the development of big data technology is ahead of the innovation of regulatory methods. In the face of the problem of big data killing caused by algorithmic discrimination, the innovative application of new regulatory methods by the government is still in the exploratory, pilot and screening stages. The technical supervision coverage is not complete, and the cost of investigation and punishment is high. In addition, the relevant regulators have insufficient knowledge of big data technology and legal related expertise, and cannot effectively address the regulatory challenges brought by big data killing.

### 2.3 Form

The main forms of big data killing are as follows:

(1) According to the device model of the mobile phone held by the consumer, analyze the income level and payment ability of the consumer, so as to make differentiated pricing. For example, Meituan and other platforms classify consumers using Apple devices as groups with higher income and payment ability, and Apple users of some goods display higher prices than Android users.

(2) According to the consumer's consumption records and browsing records, analyze the consumer's consumption habits and preferences, so as to carry out differential pricing. If consumers consume a certain commodity frequently, it indicates that they have a high degree of preference for it and a strong tolerance for its price changes. The price displayed by the platform to such consumers may be higher than that of consumers with low consumption frequency.

(3) According to whether consumers have opened members and member levels, analyze the degree of trust and dependence of consumers on the platform, so as to make differentiated pricing. For example, Meituan member users may face rising delivery fees while enjoying red envelope of orders; The price of air tickets and hotels booked by Ctrip users with high membership may be higher.

(4) According to the geographical location of consumers, analyze the space and price tolerance that consumers can choose, so as to make differentiated pricing. If users have few peripheral consumption options and the platform has few competitors, the platform may increase its pricing.

In the above ways, for goods or services with high customer price, the platform has a large profit space, and the corresponding cooking space is also large. The phenomenon of big data cooking is more obvious.

## 3. Legal application of big data killing in the view of Personal Information Protection Law

### 3.1 Legal regulation status of big data killing

#### 3.1.1 Legislative level

At present, there are many laws and regulations related to big data killing in the international legal community. Relevant foreign legislation, such as the EU's General Data Protection Regulation, is based on the position of external regulators, mainly committed to protecting personal data and giving individuals many rights; The California Consumer Privacy Act of the United States has effectively

improved the degree of information transparency and enhanced consumers' control over their personal information; The Personal Data Protection Act of Singapore aims to regulate the collection, use and disclosure of personal data by market operators.

At the legislative level, China mainly regulates big data from three directions:

First, from the perspective of consumer protection, the Law on the Protection of Consumer Rights and Interests, the Electronic Commerce Law and the Shanghai Municipal Regulations on the Protection of Consumer Rights and Interests (Revised) issued by the local government emphasize the protection of consumers' right to know and their right to choose. For example, Article 10 of the Law on the Protection of Consumers' Rights and Interests stipulates that "consumers have the right to fair trade. When purchasing goods or receiving services, consumers have the right to obtain fair trade conditions such as quality assurance, reasonable price and correct measurement."

Second, from the perspective of competition protection, the Anti-monopoly Law, the Anti-monopoly Guide of the Anti-monopoly Committee of the State Council on Platform Economy in the Field of Platform Economy, etc., emphasize the maintenance of market fairness and oppose the implementation of monopoly by operators, For example, Article 17 of the Anti-monopoly Guide for Platform Economy stipulates that "operators in the platform economy field who have a dominant market position may abuse their dominant market position, apply differential treatment to counterparties with the same trading conditions without justified reasons, and eliminate and restrict market competition."

Third, from the perspective of data protection, the Network Security Law, the Data Security Law, the Shanghai Data Regulations, and the Personal Information Protection Law emphasize the restriction of personal data collection and the protection of users' data security. For example, Article 41 of the Network Security Law stipulates that "network operators shall follow the principles of legality, legitimacy and necessity in collecting and using personal information, make public the rules for collecting and using information, and clearly indicate the purpose, method and scope of collecting and using information, and obtain the consent of the recipient."

### 3.1.2 Judicial level

As of October 18, 2022, the author has searched on the China Judicial Documents Network with the keyword "big data killing", and can retrieve 6 cases. In the case of "Liu Quan v. Meituan", the court held that Meituan's dynamic adjustment of distribution fees according to the transaction volume of the platform was its own business behavior and did not constitute an infringement of Liu Quan. In the case of "Zheng Yugao v. Ctrip", the court held that the price fluctuation of air tickets affected by market factors conforms to general trading practices and the public's perception. Zheng Yugao's time to query the air ticket price has a certain interval, and the change range of the air ticket price is also within a reasonable range. It cannot be deemed as big data killing because of the fluctuation of the air ticket price in different time periods. In the case of "Hu Hongfang v. Ctrip", the court did not find that Ctrip had big data killing behavior, but found that Ctrip had improperly handled Hu Hongfang's personal information.

By sorting out "Liu Quan v. Meituan", "Zheng Yugao v. Ctrip", "Hu Hongfang v. Ctrip" and other cases, the author believes that the current judicial practice of big data killing in China is not mature enough. At present, there are two problems in China's judicial practice related to big data killing. First, there is less experience in related cases, and there is no precedent to be based on and compared with traditional cases; Second, it is difficult for judicial authorities to identify relevant evidence of big data killing, and consumers are often required to provide evidence, which is extremely difficult for consumers.

### 3.2 New ideas of legal regulation from the perspective of the Personal Information Protection Law

Operators implement big data killing behavior, involving three stages of personal information collection, personal information processing and personal information application. This paper explores the regulatory role of the Personal Information Protection Law in the above three stages.

### 3.2.1 Personal information collection stage

Collection is the beginning of illegal use of personal information. The personal information collected by Internet platform operators should only meet the minimum demand for providing users with basic services. If the minimum demand is exceeded, operators may use the excessively collected personal information for big data killing and other illegal acts. For example, online shopping platforms provide users with shopping services. The information they need to collect is the mobile phone number of the registered user, payment information and the contact information of the consignee, instead of collecting the user's login location information, address book, biometric information, etc.

Article 6 of the Personal Information Protection Law stipulates that "the collection of personal information shall be limited to the minimum range of processing purposes, and excessive collection of personal information shall not be allowed.", The "minimum principle" of personal information collection has been established. This provision is the basic action guide for Internet platform operators to collect and process information, intended to balance the relationship between the information collection of Internet platform operators and the protection of citizens' personal information rights, and effectively responded to the social problem of excessive collection of users' personal information by some applications in recent years.

In December 2021, the China Cyberspace Security Association and the National Computer Network Emergency Technology Processing and Coordination Center jointly released the Monitoring and Analysis Report on the Collection and Use of Personal Information by App in Violation of Laws and Regulations. The report pointed out that the introduction of the Personal Information Protection Law has optimized the legal environment for the protection of personal information on App. The governance of the behavior of collecting personal information beyond the scope has achieved results, but some App are for business purposes such as accurate user portraits, promotion and marketing. The collection of personal information is still beyond the necessary scope to realize the function, mainly including seven kinds of situations, such as having the right to ask beyond the necessary scope, the specific content of data collection beyond the necessary scope, and the collection method beyond the necessary scope.

### 3.2.2 Personal information processing stage

Article 7 of the Personal Information Protection Law stipulates that "the principles of openness and transparency shall be followed in the processing of personal information, the rules for processing personal information shall be made public, and the purpose, method and scope of processing shall be clearly stated.", The "principle of openness and transparency" for personal information processing has been established. Platform operators shall handle their personal information in a manner of open rules and transparent processes, and individuals have the right to know their personal information. In practice, operators generally inform users of their personal information processing rules through user agreements and other texts, and process personal information based on users' consent.

#### (1) Notification and consent rules

Informing and consent is the core rule of personal information protection. The Personal Information Protection Law stipulates the platform's obligation to inform and the individual's authorization to consent, requiring the information processor to fully inform the information subject and obtain consent before processing personal information. An important reason why it is difficult to regulate big data killing is that the operator takes the user's consent as the exemption. The operator's objective infringement behavior after obtaining the consent to handle the user's personal information rights and interests does not constitute an infringement for the user.

Notification is the basis of consent. Article 17 of the Personal Information Protection Law stipulates the general notification rules for personal information processors, requiring that notification should be "in a conspicuous manner", "in a clear and understandable language", and "true, accurate, and complete". The user agreement and privacy policy are often thousands of words, which are filled with a lot of miscellaneous information. In practice, some APPs have too small fonts and sections are

not segmented, which brings users a huge reading burden. Users often check their consent without reading, creating conditions for platform operators to add unreasonable clauses, mislead users to agree, and avoid legal liability. In view of this, the Personal Information Protection Law requires that the platform should inform users of the purpose and method of personal information processing and other related matters in a significant way. The language of user agreements and privacy policies of some platforms is obscure and difficult. There are too many professional terms, even missing words and sentences, which make users unable to understand, even if they want to read, they can only check the agreement of consent and confirmation. After the promulgation of the Personal Information Protection Law, the language of the platform agreement is required to be clear and understandable, and ordinary consumers without professional ability can also understand it. In practice, some platform agreements do not tell the purpose of applying for permission or the expression is ambiguous, or even plagiarize other platforms, and there is no relevant operation path and function mentioned in the agreement in their own platforms. The Personal Information Protection Law requires that the language of the platform agreement be true, accurate and complete, which can effectively curb the occurrence of the above situations.

#### (2) Portability of personal information

Article 45 of the Personal Information Protection Law stipulates the right to carry personal information, that is, individuals have the right to transfer their personal information to designated information processors. If a user is not satisfied with the service of one platform and meets the conditions specified by the national network information department, he/she can carry personal information to another platform. The user's personal information is in the hands of the platform, so that the platform can kill the familiar. The portability improves the flexibility of users' control over personal information, empowers users to acquire and transfer personal information, enhances users' control over personal information, and helps to narrow the status gap between the platform and users. In order to promote fair competition in the market, protect the rights and interests of users, and curb the platform killing behavior.

### 3.2.3 Personal information application stage

Automatic decision-making is an algorithm mechanism that uses computer programs to automatically analyze and make decisions. If it is not run properly, it will damage the rights and interests of users. The typical performance is that big data is cooked, which makes users suffer unreasonable differential treatment. The Personal Information Protection Law has written automated decision-making into law for the first time, and it is also the first time to directly regulate big data killing at the legal level. Article 24 of the law requires that "when making automated decisions using personal information, transparency and fair and just results shall be guaranteed, and unreasonable differential treatment shall not be applied to individuals on transaction terms such as transaction prices". The "black box" of the algorithm makes it difficult to detect the big data killing, and the transparency of the algorithm is an important measure to regulate the "black box" of the algorithm. Ensuring the transparency of the algorithm is conducive to verifying the problem of the algorithm mechanism and reducing the difficulty of proving the rights of users. The platform uses big data to kill acquaintances and set unreasonable transaction conditions for users, which obviously violates the "fairness and justice of results" required by the Personal Information Protection Law, and damages consumers' right to fair transactions. The platform should be responsible for the results of automated decision-making, and can no longer use the "technology neutrality" as a defense.

## **4. Personal Information Protection Law" from the perspective of large data to kill the legal regulation approach**

### **4.1 Clarifying and refining the implementation norms of the Personal Information Protection Law**

The introduction of the Personal Information Protection Law refers to big data killing, but the relevant regulations are relatively broad, and the implementation rules need to be clarified. In this regard, the author suggests that the legal interpretation should be carried out in a timely manner, and the supporting legal measures should be improved as soon as possible, so as to promote the real implementation of the law and better application in practice.

#### **4.1.1 Portability of personal information**

The Personal Information Protection Law has formally established the right to carry personal information, improved the self-determination of personal information, and helped to curb the arrogance of the platform. However, the relevant statements are broad and unclear, and there is still room for further improvement of specific implementation specifications. The object of the right of portability stipulated in this law is personal information, but the category of personal information is not clear. If we simply take personal information as the dividing standard, the scope of portable data information will be ambiguous and judicial practice will be at a loss. For example, data such as consumer reputation is obviously not identifiable and is not within the scope of personal information defined in the Personal Information Protection Law, but it affects consumers' shopping experience and vital interests. Therefore, if the boundary of portability is too narrow, the data information that users really care about cannot be transferred. However, if the boundary of portability is too wide, it may infringe the information security of third parties and the business secrets of platform enterprises. Therefore, the author suggests to delimit a reasonable object scope of portability, improve the certainty of the object, and strictly limit the scope of application of the right, so as to build a specific application path of the portability of personal information in China, and better regulate the big data killing behavior of the platform.

#### **4.1.2 Personal Information Protection Impact Assessment System**

The Personal Information Protection Law has established a personal information protection impact assessment system. One of the applicable situations of this system is "using personal information for automated decision-making", which is conducive to reducing the occurrence of improper algorithm operation through prior compliance assessment and risk assessment, so as to curb the phenomenon of big data killing. However, the terms of this system are still relatively broad and need to be further refined. The Personal Information Protection Law does not specify whether the process and results of personal information protection impact assessment should be made public, but only requires that "the assessment report and processing records should be kept for at least three years". Transparency has increasingly important value for the healthy and sustainable development of the digital economy. On the premise of not seriously affecting business efficiency and not damaging trade secrets, personal information processors should make necessary disclosure of the process and results of personal information protection impact assessment, such as the time, frequency, main conclusions and number of participants of the public assessment. In order to improve the public participation in the personal information protection impact assessment system, reduce the black box operation and avoid the system becoming a mere formality. It also reduces the information gap between users and the platform to a certain extent, which is conducive to users fighting against the big data killing behavior of the platform.

## 4.2 Establish a multi-dimensional governance mechanism for information compliance

### 4.2.1 Government

The Personal Information Protection Law stipulates the departments that perform personal information protection responsibilities, including the national network information department responsible for overall planning and coordination, other relevant departments of the State Council and relevant departments of local people's governments at or above the county level, and establishes a departmental framework for personal information protection and supervision. At present, big data killing occurs frequently, but it is difficult to be effectively supervised. All departments need to cooperate with each other, regulate big data killing respectively from their own regulatory perspective, and coordinate under the specifications of the Office. We should not only strengthen supervision, but also provide reasonable guidance to avoid curbing the autonomy and innovation of enterprises, adhere to the principle of inclusive and prudent supervision, and achieve legal, scientific, and active and effective supervision. As the big data killing involves massive data, the regulatory authorities should also actively apply big data technology to the daily supervision of Internet operators, improve the business level and working ability of regulators, and improve the ability to investigate and deal with illegal acts of using hidden big data, so as to address the law enforcement challenges brought by technological development with regulatory innovation.

### 4.2.2 Enterprise

Industry autonomy has incomparable advantages over government regulation, such as flexibility and negotiability. The author suggests that the application of Personal Information Protection Law should be supported by industry autonomy. Big data killing is ineffective for a long time, but at present, the field of industry self-discipline conventions on data compliance and algorithm governance is still blank. In order to improve the public's trust in the platform, it is recommended that the Internet platform form an industry convention from the bottom to the top to reasonably collect and use big data and algorithm technology, encourage each platform to supervise each other, form a joint force to comply with regulations, and maintain market order. In particular, head Internet platforms, such as Meituan and Gaode, should shoulder their responsibilities, improve self-restraint, actively explore and practice compliance, promote the establishment of industry standards, and reduce the risk of big data killing.

## Acknowledgment

This work was supported in part by Special cultivation project of "National Innovation and Entrepreneurship Training Plan for College Students"CXCYKT20222.

## References

- [1] Sun Jinyun: 2020 Taxi Report (Part 1): 800 Taxi for Fudan Professor's Team, Is Delay a Time Game, On Sina Finance <http://finance.sina.com.cn/jjxw/2021-02-20/doc ikftssap7632791.shtml>, February 20, 2021.
- [2] Three Departments Jointly Convened the Internet Platform Enterprise Administrative Guidance Meeting, published in China Youth Daily <https://baijiahao.baidu.com/s?id=1697077716522451722&wfr=spider&for=pc>, April 15, 2021.
- [3] Zou Kailiang, Peng Rongjie Legal characterization and regulation of big data "killing" -- based on the two-dimensional perspective of "algorithm" regulation and consumer rights protection [J] Financial Economy, 2020, (07): 51-57.
- [4] Jiang Ye. Algorithm Training and Algorithm Training: Legal Regulation of Algorithms in the Age of Artificial Intelligence [J] Hebei Law Journal, 2018,36 (12): 142-153.
- [5] Wang Ying Research on the typology of algorithm infringement and legal response -- the idea of expanding algorithm regulation based on the Personal Information Protection Law [J] Legal System and Social Development, 2021,27 (06): 133-153.

- [6] Liu Chao The manifestations, causes and governance strategies of algorithm discrimination [J] People's Forum, 2022, (02): 64-68.
- [7] Liang Zheng, Zeng Xiong Policy response to "big data killing": behavior characterization, regulatory dilemma and governance outlet [J] Science, Technology and Law (Chinese and English), 2021, (02): 8-14.
- [8] Zhu Jianhai. The legal regulation dilemma of "big data killing" and its solution path [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2021,33 (01): 64-72.
- [9] Liu Quan v. Meituan, Civil Judgment of Changsha Intermediate People's Court, Hunan Province (2019) Xiang 01 Min Zhong No. 9501.
- [10] Zheng Yugao v. Ctrip, Civil Judgment of Shanghai Changning District People's Court (2020) Hu 0105 Min Chu No. 9010.
- [11] Hu Hongfang v. Ctrip, Civil Judgment of Shaoxing Intermediate People's Court, Zhejiang Province (2022) Zhe 06 Min Zhong 3129.
- [12] The National Computer Network Emergency Technology Processing Coordination Center and the China Cyberspace Security Association released<Monitoring and Analysis Report on the Collection and Use of Personal Information about Illegal Apps>, which was posted on China Netcom [http://www.cac.gov.cn/2021-12/09/c\\_1640647038708751.htm](http://www.cac.gov.cn/2021-12/09/c_1640647038708751.htm), December 9, 2021.
- [13] Sun Yueyuan Research on the Right Object of Data Portability: Structure, Effect and Localization in China [J] Journal of Henan University of Economics and Law, 2022,37 (03): 78-90.
- [14] Liu Quan On the Impact Assessment of Personal Information Protection -- Centering on Articles 55 and 56 of the Personal Information Protection Law [J] Journal of Shanghai Jiaotong University (Philosophy and Social Sciences Edition), 2022,30 (05): 39-50.
- [15] Reich On Deconstruction and Regulation of Algorithm Personalized Pricing -- Disenchanted Big Data [J] Financial Law, 2022, (02): 146-162.
- [16] Zhu Jianhai the legal regulation dilemma of "big data killing" and its solution path [J] Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2021,33 (01): 64-72.
- [17] Liang Zheng, Zeng Xiong Policy response to "big data killing": behavior characterization, regulatory dilemma and governance outlet [J] Science, Technology and Law (Chinese and English), 2021, (02): 8-14.