Process-based Risk Control of Crawler Behavior in the Field of E-commerce Live Broadcast

Zihe Ji

Civil Law Institute, Southwest University of Political Science and Law, Huixing Street, Chongqing Municipality, PRC

2252967678@qq.com

Abstract. Crawler technology has important value in the field of e-commerce live broadcasting, which can mine and release the potential economic value of e-commerce live broadcasting data. However, currently in China's judicial practice, crawler technology is mostly regarded as illegal behavior, which not only has an impact on the balance of data control and circulation, but also may bring adverse consequences to the development of e-commerce live broadcasting industry. Therefore, it is necessary to reasonably guide the application of crawler technology in the field of e-commerce live broadcasting from the perspective of risk control, so as to maximize the utilization of data. From the perspective of the circulation chain of data elements, this paper aims to deeply analyze the key nodes of data circulation in the field of e-commerce live broadcasting, so as to evaluate the crawling risk and build an operable crawling risk control scheme. The process control of crawling risk should be divided into the following four stages: data access stage, data collection stage, data use stage, data post-processing stage.

Keywords: e-commerce live broadcast; A reptile; Risk control; Data element flow

1 INTRODUCTION

Data is the lifeblood of the information age, and unlocking its value has become a crucial business objective for internet companies. In China's legal framework, the concept of 'risk control theory' has been incorporated and affirmed by laws such as the Network Security Law, Data Security Law, Personal Information Protection Law, and Network Data Security Management Regulations (Draft for Comment). This demonstrates that traditional illegality assessments struggle to address the unique characteristics of data flow.

Currently, much of the data used in e-commerce live streaming is obtained through web crawling technology, which is often perceived as unlawful by judges and scholars. Rather than simply categorizing it as either legal or illegal on a binary scale, a more nuanced discussion about the degree of unlawfulness associated with web crawling behavior would better serve enterprise risk management. Therefore, from an enterprise

R. Magdalena et al. (eds.), *Proceedings of the 2024 9th International Conference on Social Sciences and Economic Development (ICSSED 2024)*, Advances in Economics, Business and Management Research 289,
https://doi.org/10.2991/978-94-6463-459-4_106

management perspective, how can litigation risks arising from web crawling be mitigated? This paper proposes dividing the data circulation chain into four stages - data access, data collection, data utilization and subsequent processing - to identify specific risk points at each stage and provide practical solutions.

2 THE QUESTION

Crawler technology (web scraping) is essentially a technology that automates the acquisition and storage of data in a specific server, and itself has a neutral nature.[1] crawler behavior by natural persons or units for a wide range of data object (such as user data, studio operating data and commodity sales management data), in the form of various states (such as data site consent or violation of data site authorization will climb, and deliberately avoid or forced breakthrough data site security protection measures to climb, etc.) data capture.[2]

The utilization of crawler technology holds significant value in the realm of e-commerce live broadcasting. It enables the extraction and conversion of e-commerce live broadcast data into analytical materials, facilitating targeted services on the platform, empowering anchors and MCN companies with a comprehensive understanding of live broadcasting regulations, and guiding consumers towards rational consumption patterns. Furthermore, crawler technology expands the scope of data analysis from isolated fragments to encompassing market dynamics as a whole. It also refines social division of labor, compensates for platform deficiencies in terms of power and computing capabilities, while preventing data monopolies and wastage.[3]

However, in judicial practice, crawler behavior is often identified as illegal, such as "The case of illegally obtaining computer information system".Data itself is characterized by replication and non-exclusion, which is particularly obvious in the field of e-commerce live broadcasting. It is easy to produce the situation of "one number of multiple rights", that is, a certain data generated in the process of live broadcasting may carry the data rights of multiple subjects. At present, some courts believe that live broadcast data has the characteristics of "sharing", and they all enjoy the use of the data to a certain extent without violating the principle of "legal, necessary and user consent". Other courts believe that enterprise platforms only enjoy legitimate rights and interests in the non-original data sets formed by the collection, storage, processing and transmission of data, and that a single original data individual is separated from them. The judgment thinking is different and the legislation is not comprehensive. The discretion of judges in the application of Article 2,12 and 17 of the Anti-Unfair Competition Law has been unable to solve the increasingly complex problem of data crawling and affect the balance between data control and circulation.

3 SITUATION ANALYSIS

3.1 Theoretical level: crawler behavior in the field of e-commerce live broadcasting, from legitimacy judgment to risk control

In the data controversy of crawler behavior, the traditional department law is difficult to provide a solution. Criminal regulation does not distinguish between crawler mode, crawler object, crawler purpose, etc., and only takes the economic loss caused by the crawler and the amount of personal information infringement as the criminal standard.[4] The relatively gentle way is the anti-unfair competition law, but the legal norms are more general.[5] Due to the particularity of data, the influence of the data monopoly and malicious competition are not simply enterprise competition and monopoly, but may threaten data security, public privacy and the real physical world, and the supervision and governance of data cannot be realized through the Anti-Unfair Competition Law.

In the academic discussion, many scholars tend to preset the crawler behavior as illegal behavior, and regard the contexalized positive factors as "reasons for exemption" or "reasons for illegal exclusion". From the perspective of criminal law, the illegality of crawler behavior is mainly reflected in the objective aspects and objects, such as the invasive behavior and whether the crawler object involves the personal information of citizens. Once the criminal conditions are met, they can be severely punished.[6] Researchers in the field of anti-unfair competition law have supplemented this issue by taking into account the purpose of data use, whether the crawler subject is involved in unfair competition or monopoly, and the data type of the crawler. In the field of digital law, the technical factors caused by the pressure of access to the server, the severity of the intrusion means, and the types of agreements that violate the authorization of the data party have gradually attracted the attention of the academic circle.

As can be seen from the above scene, it is inappropriate to judge the legitimacy of crawler behavior according to traditional standards, because the crawler behavior presents multiple forms. As the risk of companies touching on legal risks increases, China draws lessons from foreign legislation and takes risk management as a key means to ensure data processing and security.[7] This paper will study the risk control of crawler behavior in the field of e-commerce live broadcasting.

3.2 Practical level: Risk points and analysis of all links of crawler behavior in the field of e-commerce live broadcasting

3.2.1 Risk point at data access

The first is whether the crawler object is specially protected. According to the degree of data openness, it can be divided into open data and non-open data. Open data is a data that is voluntarily disclosed by enterprises and freely obtained and used by the public. In the field of e-commerce live broadcasting, open data is the main type of data frequently obtained by crawlers, such as user viewing data, interactive data, transaction data, etc. About climb take open data is legal, article 127 of the civil code stipulates the data network virtual property, framework to protect open data attached rights, but because the data has not yet confirmed, open data limited in acquisition, trading, ownership, the judicial practice to labor input data ownership, and then deny the rationality of the climb to the public data.[8] In addition, protected but not publicly available data can be classified into three categories: violations of crawler technical restrictions, protocol restrictions, and crawler prohibition data. According to the criminal law expansion interpretation, non-open data is regarded as "unauthorized" access and use, and any unauthorized data acquisition behavior is regarded as an illegal crawler.[9]

The second is whether the scope of climbing exceeds the scope of authorized. When crawling network data, they must abide by relevant laws and regulations, and must not infringe others' privacy rights and intellectual property rights. If the scope of climbing exceeds the scope of authorization, it may lead to legal disputes, and even face legal liability. For example, in the No.36 guidance case of the Supreme People's Procuratorate, the defendant Gong was found to be beyond the authorization scope of the company for providing the login account information of the company's internal management and development system. Although Gong did not take technical means to destroy the system protection, but was still identified as illegal.

Finally, whether the data access causes too much pressure on the server. If the crawler interferes with the normal operation of the visited website or system, it may be suspected of destroying the computer information system. Whether data access puts excessive pressure on the server depends on multiple factors, including server performance, frequency of data access, quantity, time, and security. If the data is accessed too frequently and too often, it may overload the server, which may affect its performance. Similarly, if the data access time is too concentrated, it may cause the server to bear great pressure in a short time.

3.2.2 Risk points at data collection

In the field of e-commerce live broadcasting, the classification and classification of data collection objects is the key risk link of crawler behavior, covering data classification and data classification. In terms of data classification, state secrets, business secrets, personal information and intellectual property data prohibited by the Criminal Law, Personal Information Protection Law and Anti-Unfair Competition Law should be avoided.

At the same time, collecting and using too much open data may result in downstream crimes, so the risk level is considered medium. Open data can be freely accessed by users and is a public resource, even with code barriers. The usage of web crawlers to obtain public data is debated in academic and practical circles, with questions of whether it constitutes computer information system crimes or unfair competition. The US has moved from denying unauthorized crawlers to supporting free access to public data. China's industry is not against collecting public data, and judicial attitudes have changed. Therefore, accessing general open data is less risky.

Moreover, the degree of damage caused to the server caused by the data acquisition method determines the value of risk. Without appropriate control of the use of network crawler technology, resulting in the disorderly emergence of large-scale access, beyond the server load limit, and then cause the collapse of the website, such behavior may violate the "Network data Security Management Regulations" article 17, "Network Security Law" Article 27, "Criminal Law" Article 286 and other provisions. Common data collection behaviors include destructive behavior, breakthrough behavior and evasive behavior. In addition, the technical means that violate the will of the data website.

3.2.3 Risk point when the data is used

First of all, the use of crawler data illegal crime may involve illegal use of information network crime, help information network criminal activities crime, is prohibited behavior. In addition, it may also involve violations of users' privacy, intellectual property rights, trade secrets and other illegal acts.[10]

Secondly, insufficient innovative use of obtained information poses a greater risk, such as the inability to create new data products. If such behavior infringes on the rights and interests of the data controller, it amounts to unfair competition and may lead to legal disputes. In contrast, the crawler behavior for the purpose of integrating and enumerating data is less innovative, but the integration of information helps to improve the efficiency and accuracy of social decision-making. For example, the commodity price comparison software provides users with the whole network price comparison service of the same products by capturing the massive commodity prices on multiple platforms. Crawler websites that provide data analysis, trend prediction and other services are the most innovative, which are significantly different from the above-mentioned enterprises. The data captured by them is used for research and development of innovative products.

Finally, there is a great debate about the legality of the use of crawler data, and there is no conclusion. Rao suggested using the "rational use" system in the field of personal information protection. As long as the use of data does not harm national security and public interests, and does not harm the legitimate rights and interests of citizens and organizations, such as personal study and scientific research. From the perspective of anti-unfair competition, some believe that the "rational" use of open data should be conducive to improving efficiency and promoting innovation, such as filling the market gaps and providing multiple channels to the society.[11]In general, the academic community tends to set the legal situation for the use of data, but there is no consensus on what is a "reasonable" use.[12]

3.2.4 Risk points for the subsequent processing of the data

Data storage, data transaction and data exit are the common risk points of subsequent data processing.

First, data storage problems are widespread but pay low attention, leading to frequent large-scale data leakage incidents. The data leakage scene of e-commerce live streaming platforms is more complex. Because of user data for MCN company and live the main has commercial value, some sites such as new shake, shaking check using crawler technology grab user data, form a huge database, but if the technical protection measures does not reach the designated position, will cause serious data security problems, including data leakage, tampering, delete, etc., affect the integrity and availability of the database.

Second, after ensuring data compliance, the most important step in data trading is reviewing the qualifications of the transaction object and the purpose of data use. If a user knowingly provides data for illegal activities, it may result in criminal penalties, such as violating personal information laws. Therefore, it's crucial to verify trading object qualifications and data use purposes. The data provider must ensure the legitimacy and integrity of the data user, avoiding providing data to those who may misuse it. Additionally, the provider must clarify its data use purposes to comply with legal requirements.

Third, data exit risks mostly appear in enterprises with frequent foreign transactions. With the expansion of overseas territory, enterprise data and user data go overseas together with enterprises. The risk of data exit is not only the risk of external data compliance, but also the scope of legal obligations of enterprises due to the jurisdiction of "digital sovereignty" in the digital field.[13] However, the damage degree of data exit can be classified as endangering the national "digital sovereignty", causing or may cause damage and causing or may cause ethical problems, thus dividing the behavior risk level. As show in table 1.

Table 1. Risk point control of crawler behavior of e-commerce.[1]

Behavioral form				forbidding act	highrisk	Medium risk	Low-risk or no-risk		
During the data access	access object			Dislegally accessible data	With anti-crawler technology Limit the number of visits occupy	Data that limits access with a protocol	Open data	1. Only the qualified users and applications can access the data. 2. Monitor, control and audit the access behavior	Data security protection
	Access scope			The crawl scope is beyond the authorized scope			The crawl scope does not exceed the authorized scope		
	Access limit			Seriously affect the website Run	Did not seriously affect the website operation (automatic access collection traffic does not exceed One-third of the average daily traffic on the website)				
When the data were collected	Collect at the object level	data classification	User data	State secrets; business Industry secrets, individuals Information, knowledge Property right data + plot serious	Personal information, related Intellectual property data Involving unfair competition Fight for data + not The plot is serious	1. Open the non-open number occupy 2. Raw data / base data	General open data	1. Follow the phase Pass the law instrument 2. Respect for knowledge Right and choice 3. Use desensitization	
			Broadcast room operation data						
			Sales management data						
		data staging		Core data	Important data	general data			

[1] The above points of view in this paper are sorted into a table

						and other technical methods	
	technological means	act of sabotage	Forced breakthrough data, website security measures	Avoid behavior	Get the consent or authorization		
When the data is used		1. For illegal use crime 2. Substantial substitution Generation method damage number According to the interests of the controller	Use of data Less innovative	For the data analysis, Create data products , to promote innovation, increase of efficiency	Personal study, scientific research, etc	1. Follow the phase Pass the law instrument for drawing circles 2. Respect for use Privacy of households	
			For specific data (state secrets, business secrets				
When the data is subsequently processed	data storage	Deliberate disclosure of personal information and other data	For important databases No protection	For important databases Protective measures are weak	The database protection measures	Pay attention to data, exit problems, data leakage, exposure, data, and transaction risks	
	Data trading	Know that the other side uses Data offenders Sin,still provide the number occupy	To have a criminal record Or the more suspicious right	Provide data to more reputable objects	Using public data Easy platform data delivery Easy, and the other party's reputation higher		
	Data exit	State secrets and other Heart data exit, The harm to our country " data sovereignty"	Important public data Social data out Environment, cause or can can cause the country, organizational and personal damage	More important to the public data Social data out Environment	General data exit		

4 RISK CONTROL OF KEY NODES OF CRAWLER BEHAVIOR IN THE FIELD OF E-COMMERCE LIVE BROADCASTING

From the perspective of the data element circulation chain, this paper will assess the key nodes of the data circulation in the field of e-commerce live broadcasting, and discuss how to build an operational scheme of crawler risk control. After 203 questionnaires and 3 interviews with practitioners, it is found that it is feasible to streamline the risk control of crawler behavior at key nodes.In this paper, the process control of crawler risk is divided into four stages: data access, data collection, data use, and data post-processing.

4.1 Key node of crawler risk control in the data access stage

First, the openness of the data access objects should be the basis for judging the legitimacy of the crawler behavior. Modern computer systems such as "a mixture of castle and public places", where data from "inside the castle" are accessible with permission, and data from "public places" can be viewed freely.[14] Open data implies the consent of data subjects to others' access to data. Widly disclosed data can attract more users, earn more trading opportunities, and have low risk.[15] Relatively speaking, the judicial issue of private data needs to be addressed by guiding cases and interpretations to activate the data trading market and reduce corporate compliance costs.

Second, compliance with the data party Robots agreement as an important basis for obtaining "authorization" is generally recognized. The crawler shall respect the access time, access data scope, access method and access purpose, etc. agreed in the Robots agreement, and shall not violate the climbing restriction of the website. Therefore, the Robots agreement can be regarded as a valid contract clause, with the intention of the contract.[16] Enterprises should understand the server performance and capacity, frequency and quantity of data access, and improve efficiency by optimizing data access policies, such as using caching, reducing unnecessary requests, or optimizing queries. According to the Data Security Management Measures, the bottom line of data access is not to hinder the normal operation of the website, and the traffic collected by automatic access should not exceed one third of the average daily traffic of the website.

4.2 Key nodes of crawler risk control in the data collection stage

First, enterprises with data as the core productivity in the field of e-commerce live broadcasting should conduct data classification and classification. Enterprises should refer to the "Data Safety Law", "Network Security Standards practice guide", "Information Security Technology personal Information Security norms" and other relevant provisions, using the general guiding principles. At present, the industry usually grades the core competitiveness and production value of enterprises according to the data.

However, the formulation of data standards should follow the market logic. As the market demand for data transactions changes, enterprises should adjust dynamically. As show in table 2.

Table 2. Classification list of e-commerce live broadcast data.[2]

E-commerce live streaming data classification list		
First class subclass	Secondary subclass	Example data
User data for users	Personal data	Such as user ID number, user tag, user IP, etc
	Watch and interaction data	Watching data includes browsing records, viewing time, etc.; interactive data includes gift records, barrage data, thumb up records, etc
	transaction data	Such as participating in the lottery situation, order information, logistics information, etc
	User-supervised data	Supervise the reporting records and the follow-up processing results, etc
Broadcast room operation data studio operator	Anchor personal data	Such as anchor personal data, anchor with the total amount of goods, total revenue of goods, reputation of goods, etc
	sales statistics	Such as the duration of the live broadcast, GMV, the proportion of fans in the transaction, the amount of thousands of views, the return rate in the sale, etc

Secondly, when evaluating the behavior of breaking through the anti-crawler mechanism, it should be judged on the basis of the computer information system and data security, and considered in essence. It should be clarified that a simple violation of the Robots protocol does not amount to an intrusion. Robots The purpose of the protocol is to guide the web crawler to grab useful information more effectively, unless to maintain the normal operation of the website, protect the public interest and other legitimate reasons, otherwise shall not prohibit the web crawler access, so it is called the "gentleman's agreement", does not have the effect of technical measures.[17]

Finally, enterprises need to reduce the burden of data source servers when they crawl through the live broadcast data of e-commerce companies. First, communicate with the data party and obtain the consent or authorization to enjoy more preferential policies.

[2] This paper refers to the relevant provisions of the "Network Security Standard Practice Guide" and "Information Security Technology Personal Information Security Code", and adopts a hierarchical classification method. In first-level classification, data types are divided into three categories according to the original data source: user data, broadcast room operation data and commodity sales management data. In the second-level classification, by examining the business habits of data analysis on large e-commerce live streaming platforms, such as NetEase Data, Shake check, new shake and other platforms, the circulation of data between institutions and industries is promoted.

Secondly, the climbing speed is controlled to avoid the server overload from affecting the data quality. Moreover, follow the protocol, such as using the specified API interface, meet the data use range, etc. In addition, the crawler algorithms are optimized to improve efficiency and reduce invalid requests. Finally, reasonable data storage and processing, such as compression storage, weight removal, cleaning, to improve the efficiency of data processing.

4.3 Key nodes of crawler risk control in the data use stage

First, from the innovative perspective of anti-unfair competition law, the risk management of data use needs to consider: establishing a professional data team with data mining, analysis and product development skills; Invest sufficient resources, including hardware and software, to meet the demand; Develop scientific data innovation process to ensure continuous product optimization.

Second, for special data, such as state secrets, trade secrets, personal information and intellectual property data, enterprises need to implement special technical processing. If a state secret is discovered, it shall promptly communicate with the relevant departments and report it; For trade secrets, unauthorized access will bear legal responsibility; Personal information needs to be desensitized, anonymized, encrypted and restricted. Data enterprises should comply with regulations and avoid legal risks when applying e-commerce live data.

4.4 Key nodes of crawler risk control in the subsequent processing stage of the data

The risk control level of data storage, data transaction and data exit behavior is different.

First, large data controllers are legally responsible to implement technical protection and reinforcement of the existing database. According to the completeness of the protection measures, the database protection intensity can be divided into several levels, and the risk assessment level can be set step by step. Therefore, it is very necessary to protect the database effectively and technically. In terms of technical measures, security components such as authorized access, terminal data leakage prevention, core data encryption, data security exchange, Internet digital asset protection, watermark anti-diffusion and so on can be used. [18]At the same time, in order to ensure the security of transactions, buyers and sellers can use standardized and efficient data trading places to avoid the risk of OTC black market trading. Since December 2022, the Opinions of the CPC Central Committee and The State Council on Building a Data Basic System to Better Play the Role of Data Elements have formally proposed the construction of a national data trading platform, the people's data service platform, the national intellectual property data, Shanghai Data Exchange and other escort for data security. The review of the trading party's criminal record is also an important part of compliance.

Second, in order to ensure the security of transactions, all participants can rely on formal and efficient data trading venues to avoid the risks brought by the over-thecounter black market exchanges. Since December 2022, the Opinions of the CPC Central Committee and The State Council on Building a Data Basic System to Better Play the Role of Data Elements clearly proposed to build a national data trading platform, a people's data service platform, as well as the Shenzhen Data Exchange, Shanghai Data Exchange, etc., to provide a solid guarantee for data security. Data trading can also rely on the blockchain marketing tag trading mechanism (decentralized data security transaction system, DSTS) of the E-commerce Alliance, and realize a secure and complete data trading ecology by building the decentralized upper-level consensus incentive mechanism and combining with the trusted execution environment.[19]

Third, in terms of foreign-related data security supervision, China's public security organs, state security organs and other relevant departments perform their duties according to law to supervise the massive outflow of data. At the same time, enterprises also need to lead themselves to the "forced self-discipline model" to bear the consequences of the risk of losing control of their own data.

5 EPILOGUE

E-commerce live broadcasting's data circulation risk assessment and Crawler risk control are crucial for enterprise data security and business stability. Managing access rights, considering special protection, authorization scope, and restrictions are vital in data access. Enterprises must classify collected objects and use methods that minimize server damage in data collection. Rational and compliant data use, with focus on privacy protection and product innovation, is essential. Data exit, leakage, and transaction risks must be addressed in follow-up processing. Comprehensive data security protection ensures data security and reliability. In summary, enterprises must develop targeted risk control strategies for each data circulation link, ensuring data safety, compliance, and efficient use.

ACKNOWLEDGEMENT

Supported by: Innovation and Entrepreneurship Project for College students in Chongqing

REFERENCE

1. Iggena Thorben;Bin Ilyas Eushay;Fischer Marten;Tönjes Ralf;Elsaleh Tarek;Rezvani Roonak;Pourshahrokhi Narges;Bischof Stefan;Fernbach Andreas;Parreira Josiane Xavier;Schneider Patrik;Smirnov Pavel;Strohbach Martin;Truong Hien;Gonzɑ́lezVidal Aurora;Skarmeta Antonio F.;Singh Parwinder;Beliatis Michail J.;Presser Mirko;Martinez Juan A.;GonzalezGil Pedro;Krogbæk Marianne;Christophersen Sebastian Holmgård. IoT-Crawler: Challenges and Solutions for Searching the Internet of Things. [J] Sensors. Volume 21 , Issue 5 . 2021. PP 1559-1559
2. Yang Zhiqiong. The punishment regulation of web crawler in the data era [J]. Comparative method study, 2020 (4).

3. He Yun can. Data ownership theory scenario selection —— based on dualism [J]. Information Security Research, 2020 (10).
4. Yang Zhiqiong. The punishment regulation of web crawler in the data era [J]. Comparative method study, 2020 (4).
5. Liu Jifeng. The "unbearable light" —— theory is based on the absence of general provisions and the improvement of limited principles [J]. Journal of Beijing University of Chemical Technology (Social Science Edition), 2010 (3).
6. Yang Zhiqiong. The judicial dilemma and outlet of data crime in China: taking the benefit of data security Law as the center [J]. Global Law Review, 2019,41 (6).
7. Rao Chuanping. On the process management of data capture and legal risk [J]. Oriental Law, 2023 (6).
8. Wen Qingmei. On the protection scope of enterprise data property rights [J]. Jingchu Law, 2024 (1).
9. Li-ping hu. The punishment law system of web-crawler behavior [J]. People's Procuratorate, 2022 (11).
10. Liu Jifeng, Zeng Xiaomei. On the competition method protection path of user data [J]. Price Theory and Practice, 2018 (3).
11. Zhai Wei, Liu Yinuo. The legitimacy boundary of open data crawling in the perspective of anti-unfair competition law [J]. Price Theory and Practice, 2021 (8).
12. Shehu Vlona Pollozhani;Shehu Visar.Human rights in the technology era ‑ Protection of data rights[J]. European Journal of Economics, Law and Social Sciences. Volume 7 , Issue 2 . 2023. PP 1-10
13. Liu Lingxia. The theoretical connotation, practical challenge and coping path of digital sovereignty security [J]. Journal of Shaanxi Normal University (Philosophy and Social Sciences Edition), 2024.
14. Xuejian Li. In the era of big data, the standard of crawling enterprise data in the crime and its judicial restriction [J]. Journal of Dalian University of Technology (Social Science Edition), 2023,44 (5).
15. Liu Jifeng, Zeng Xiaomei. On the competition method protection path of user data [J]. Price Theory and Practice, 2018 (3).
16. Manu Narula; Jasraj Meena; Dinesh Kumar Vishwakarma.A comprehensive review on Federated Learning for Data-Sensitive Application: Open issues & challenges[J].Engineering Applications of Artificial Intelligence
17. Yang Huajian, Qu Sanqiang. On the legal nature of the crawler agreement [J]. Law applicable 2013 (4).
18. Li-ping cao. The crawler agreement as a dimension of the legitimacy of business ethics —— Case of unfair competition dispute between Beijing ByteDance Technology Co., Ltd. and Beijing Weimeng Network Technology Co., Ltd. [J]. Law is applicable, 2023 (5).
19. Dai Wei Qi, et al. Blockchain marketing label trading system for e-commerce alliance [J]. Computer Research and Development, 2024.