Research on Personal Information Protection System of E-commerce Platform Users

Haoyuan Sun

Asia-Australia Business College, Liaoning University, Shenyang, China

1220170784@qq.com

Abstract. With the rapid development of information technology, E-commerce has gradually become an important way for people to obtain needed goods and services. At the same time, the operation mode of E-commerce platform determines that it will have access to a large number of users' personal information. If such information is leaked, it will have a great impact on users' property rights and personal rights. This paper focuses on improving the compliance work of E-commerce platform enterprises, and puts forward detailed suggestions on the compliance work of E-commerce platform operators' personal information from the perspective of system construction and compliance operation, which is conducive to E-commerce platforms' compliance work in the era of personal information protection.

Keywords: E-commerce Platform; Personal Information Protection; Information Security; Information Disclosure.

1. Introduction

In the information age, E-commerce, a new business model begins to rise, and online transactions attract more and more market elements into the E-commerce platform. The development of electronic commerce has profoundly changed the traditional business model. Consumers are no longer constrained by geographical factors, and merchants can offer goods and services to more consumers. However, different from the traditional consumption mode, the consumption process of E-commerce is mainly dominated by E-commerce platforms. If users want to purchase goods through E-commerce platforms, they must register their accounts on E-commerce platforms and provide valid personal information when purchasing. The business activities of E-commerce platforms greatly depend on users' personal information. Therefore, E-commerce platforms often use information technology to store large amounts of users' personal information for a long time. The application of information technology makes the storage time and storage method of the users' personal information obtained by the operators of E-commerce platforms different from that of the traditional commercial trade, which inevitably enhances the legal risk of information disclosure and improper use, and also increases the possibility of harm increasing and spreading.

In practice, with the development of E-commerce platforms, cases related to the leakage of users' personal information on E-commerce platforms are common. In 2017, Shen was blackmailed 120,000 yuan after her personal information was leaked when she bought a plane ticket through an online ticketing service. In 2020, a large E-commerce platform in China reported that hackers accessed a large amount of user information through web crawlers. According to a police investigation, criminals accessed nearly 1.2 billion pieces of users' personal information on the E-commerce platform and used them for their own improper business.

In recent ten years, the research of personal information protection is at its peak. Some scholars pointed out that the protection of sensitive personal privacy information should be strengthened [1], and special provisions and classified protection should be made for it [2]. However, some scholars believe that in the information age, any personal data on the Internet can lead to special types of personal information [3], so the dimension of protection should be more comprehensive. At the same time, some scholars pointed out that although the protection status of personal information is guaranteed in the existing laws, the corresponding provisions are relatively general [4].

The consequences caused by the disclosure of user's personal information are very serious. If personal information is leaked, it will bring unnecessary troubles to users and affect their personal

property rights and even personal rights. In this regard, from the perspective of platform enterprise compliance, this paper will carry out legal and operational analysis on the protection system of E-commerce platform users' personal information, and put forward detailed suggestions to promote it, so as to provide useful insights for practice.

2. The Internal Logic of E-commerce Platform to Protect Users' Personal Information

2.1 The Commercial Characteristics of E-commerce Platform

2.1.1 Overview of E-commerce Platform

E-commerce platform is an important place for enterprises or individuals to negotiate online transactions, a virtual network space for business activities built on the Internet and a management environment to ensure smooth business operation, and an important place to coordinate and integrate information flow, goods flow and capital flow in an orderly, related and efficient way. Its original intention is to build a profit-oriented online platform, convenient for users to trade. Users can post information, match trades, sell or buy products and services on the E-commerce platform. But it has also led to E-commerce platforms being able to access users' personal information, use that information to make decisions, and keep a record of that information. But when the E-commerce platform is set up, its main business doesn't include providing data security services. As E-commerce platforms are closely related to users' personal information, they should be given the legal obligation to protect users' personal information.

2.1.2 Main Types of E-commerce Platforms

According to the business types of E-commerce platforms, they can be roughly divided into three categories:

2.1.2.1 Pure Proprietary E-commerce Platform

Pure proprietary E-commerce platforms refer to those that only provide sales channels for their own branded goods or services, such as Midea, Haier and other electrical brands online shopping malls. Brands apply for their brand name consistent with the network domain name to open online mall. The essence of this kind of E-commerce platform is to simply combine offline sales mode with online sales, so as to expand their sales channels.

2.1.2.2 Pure Intermediary E-commerce Platform

Pure intermediary E-commerce platform means that platform enterprises do not sell products and provide services on this platform, but provide a virtual platform for the third-party operators to carry out trade. Third-party operators sell products and provide services. For example, Taobao is a type of E-commerce platform, and the self-operated stores on Taobao website are all opened by major brands or individuals. Its main characteristic is that the personal information of both operators and users will pass through the intermediary E-commerce platform, so this kind of E-commerce platform has the function of information aggregator.

2.1.2.3 An E-commerce Platform with both Proprietary Nature and Intermediary Nature

An E-commerce platform with both proprietary and intermediary nature means that the E-commerce platform not only sells its own brand of goods and services on the E-commerce platform, but also acts as an intermediary to provide a trading place for other brands of goods and services. For example, Suning Tesco is such a platform. It sells Suning's own products as well as products of other brands. Compared with pure intermediary E-commerce platform, information has a greater use value for this type of E-commerce platform. On the basis of pure intermediary E-commerce platform, the personal information of users it collects can also provide decision-making information for its own participation and sales business. Gathering users' personal information can not only help such E-

commerce platforms build an ecosystem in the online market, but also assist them improving their advantages when competing with other brands.

2.1.3 The Relationship between Business Characteristics and Personal Information Protection

E-commerce is defined as a commercial organization and a commercial subject stipulated by commercial law. Its basic feature is profit. Such profitability makes E-commerce platforms collect and use personal information for the purpose of achieving greater commercial profits. But in the past, users' personal information did not have independent commercial value, so it was not used for other commercial activities. However, for E-commerce platforms now, users' personal information can help them make decisions in many cases, and therefore has become an important factor of production [5]. Collecting and using personal information is no longer a simple tool or means, but for the purpose of further expanding the business territory of E-commerce platforms. This leads to a higher risk of abuse. Accordingly, the increased risk of abuse increases the necessity of legal regulation. By increasing the cost of breaking the law, a legal protection system is constructed to make the benefits of protection exceed the benefits of not protecting, and promote enterprises to consciously implement personal information protection.

2.2 Legal Characterization of E-commerce Platforms

2.2.1 With Technology Empowerment and Industrial Ecological Expansion, E-commerce Platforms Become Online Public Living Space

The rapid development of Internet technology, big data, cloud computing and other information technologies provide technical support for business activities from offline to online. Technology empowerment causes E-commerce platform and traditional sales mode become an important way for people to obtain needed products and services. The industrial ecological expansion of E-commerce makes E-commerce platform no longer a simple enterprise, but a path of ecological diversification. The business scope of E-commerce platform is becoming wider and wider, and the degree of integration between businesses is turning into higher and higher. For example, a large number of new E-commerce operators emerged, which were led by we-chat business, generating the socialization of E-commerce [6]. E-commerce platform has become an important place for users to carry out daily communication and personal life. At the same time, the intensity is also deepening, and the breadth is gradually getting more and more extensive. E-commerce has been deeply involved with all aspects into the life of individuals, becoming the online public life space of E-commerce users.

2.2.2 The Effect of Direct Government Regulation is Weakened

From the technical level, government agencies are not professional Internet companies, so they have a relatively macro understanding of the E-commerce industry. Their understanding of grasping the specific operation process and details may be lagged behind and indirect. This is reflected in the fact that administrative subjects often need to inquire and collect evidence for specific E-commerce platform operators and related subjects after the occurrence of specific events to master the operation status of relevant business lines in detail. At the same time, compared with the operators of E-commerce platforms, the Internet technical support available to government agencies is limited. Therefore, it is necessary to pay large administrative resources and economic costs to clearly point out the loopholes in the technical security of E-commerce platforms. In terms of links, the users of E-commerce platform are extensive and complex. However, the regulatory role of the government is global. In order to realize the regulatory path, the decree needs to be passed layer by layer in the system, which will weaken the regulatory effect. In order to enhance the effect of regulation, it will be a more effective governance path to realize direct management by entrusting E-commerce platforms with certain legal obligations.

2.3 Through Legislation, E-commerce Platforms are Endowed with Certain Public Management Functions

As the government has limited ability of regulation and effect on the E-commerce industry, it has become an important channel to realize good governance effect and maintain the competition order of the E-commerce industry by enacting certain public management functions on the E-commerce platform through legislation. To be specific, the public management attribute functions of E-commerce platforms in traditional businesses are mainly reflected in the qualification audit function and rule-making function. First of all, according to the article 27 of the E-commerce law, E-commerce platform operators should be required to apply to sell goods or provide services of business operators to submit their identity, address, contact information, such as the administrative licensing real information, check, registration, set up registration files, and regularly check update. As can be seen from this article, the legislation enforces E-commerce platforms with the supervision function of qualification examination before third-party operators enter the platform business, which, to some extent, enables E-commerce platform operators to determine the entry threshold of the platform market. In addition, the article 36 of the E-commerce law stipulates that E-commerce platform operators shall timely publicize measures such as warning, suspension or termination of services of operators within the platform for violating laws and regulations in accordance with the platform service agreement and transaction rules. The management measures mentioned in the above article have a distinct color of public law, confirming that E-commerce platform operators can formulate platform service agreements and relevant transaction rules according to the operating conditions of the platform. E-commerce platforms also evaluates, adjudicates and imposes penalties on the specific business activities of the third-party operators according to the content of the service agreement and transaction rules. It can be seen that E-commerce platforms have begun to undertake certain public law review obligations and have the statutory duty to maintain the order of online business environment.

2.4 Personal Information Protection is an Important Part of E-commerce Platform to Fulfill Public Functions

The article 58 stipulates that personal information processors that provide important internet platform services with a large number of users and complex business types shall fulfill the following obligations: (a) establish and improve the compliance system for personal information protection in accordance with national regulations, setting up independent institutions mainly composed of external members to supervise the protection of personal information; (2) formulate rules of the Platform in accordance with the principles of openness, fairness and justice, clarifying the standards for product or service providers on the Platform in handling personal information and the obligations to protect personal information; (3) Stop providing services to product or service providers on platforms that seriously violate laws and administrative regulations in handling personal information; (4) Regularly release social responsibility reports on personal information protection and accept social supervision. In the personal Information Protection Law recently issued, E-commerce platform operators, as one of the important types of Internet platforms, are given the legal obligation of personal information protection. Besides the typical functions of formulating platform rules related to personal information protection and stopping providing personal information products and services, the public management function of establishing compliance system of personal information protection and issuing social responsibility report of personal information protection has been added, which has a strong color of front-end risk control.

Protecting users' personal information that plays an important role in E-commerce business is an important embodiment and effective way for E-commerce platforms to perform public functions instead of the government. In this regard, it is necessary to guide E-commerce platforms to perform the obligation of protecting personal information through legislation.

3. Key Points of System for Protecting Users' Personal Information on E-commerce Platforms

3.1 Collecting Step

3.1.1 Defining Principles

According to the Personal Information Protection Law (second draft), E-commerce platforms should inform users of the scope of information they collect and the scope of usage. This requires E-commerce platform operators to inform users of the types and scope of information collected in business activities in a clear way. If the method is not clear, it will cause information asymmetry between E-commerce platform and users. If users do not know what scenarios the platform will use their information for, it may bring risks of information insecurity to users. From the point of view of users, users also need to convey to the E-commerce platform whether they agree with the scope of collection or use of a clear expression of meaning. Otherwise, unclear information disclosure will make users and E-commerce platforms lose the binding mechanism based on commitment. Therefore, whether from the perspective of users or from the perspective of self-restraint of the platform, unclear information types and scope of use will cause practical risks that harm the influence of personal information protection.

3.1.2 Principles of Authenticity

When formulating and releasing statements about users' personal information, E-commerce platform operators should ensure the authenticity and accuracy of relevant contents. For example, the collection scope and usage scenarios of users' personal information should be consistent with the actual situation, without any substantive differences or conflicts. If the content stated or informed is untrue, the decision made by the user based on the untrue statement is not the true expression of the user's personal intention and cannot represent the true consent of the user. At the same time, within the foreseeable scope, the service content of the platform should be relatively certain. This requirement is mainly to prevent illegal elements from setting up E-commerce platforms for the purpose of illegally collecting personal information rather than selling products and services. In practice, some illegals will set up a fake E-commerce platform to attract users to register. After collecting enough information, they will cancel the enterprise and use the collected personal information for other ways of profit. Therefore, the stability of the service content of the platform within a certain time range is an inevitable requirement to avoid the false operation risk of the platform.

3.1.3 Principle of Voluntary Authorization

E-commerce platforms should not abuse the dominant position of enterprises to coerce users into making choices. When users want to use a specific E-commerce platform to participate in online commerce and trade activities, and the E-commerce platform is in a monopoly position in the industry, the E-commerce platform should not abuse its dominant position and arbitrarily formulate user information authorization rules. The E-commerce platform should enact personal information authorization rules on the basis of reasonable practices in the industry, otherwise users are not authorized out of voluntary principle, but out of fear under coercion.

At the same time, the form of user's consent should also reflect the principle of voluntariness. At present, it is common for E-commerce platform operators to require users to check the consent box when obtaining user authorization. Users can choose whether to check the consent box voluntarily. At the same time, there are other forms of non-compliance, for example, after the user has read the statement, it is deemed that the user has agreed, and the system automatically jumps to the next interface. In the context of obtaining user's authorization and consent in this way, although the user did not check the "no" box, it could not directly prove that the subjective state of mind of users is "yes". This behavior is unfair and the form of silence cannot be considered voluntary. This is because personal information is of great importance to the property rights and personal rights of users.

Therefore, in the protection mechanism of personal information, the requirement of voluntary principle needs to reach a relatively high degree.

3.1.4 Principle of De-identification

After collecting users' personal information, platforms should erase the sensitive information as much as possible. The main goal of E-commerce platforms to collect the required user personal information is providing target portraits of commercial services based on the common characteristics of one or more groups, so as to better understand the precise needs of users, rather than to identify the differences between individuals with accurate information. Therefore, for specific users' personal information, especially sensitive information related to users' privacy, such as physical health, interpersonal communication, activity track and other personal information types, E-commerce platform operators should carry out maximum de-labeling on the premise of following the minimum necessary principle. Meanwhile, this measure is also a necessary step to prevent information leakage after inducing major information security risks or even leading to major information security events. After E-commerce platform operators have processed users' personal information to the maximum extent, the user information after fuzzy processing is difficult to be used as a clue to accurately judge the specific situation of users even if information leakage occurs.

3.2 Using Step

3.2.1 Principle of Purpose Limitation

The purpose in the principle of purpose limitation should have two attributes: legitimacy and rationality. From the perspective of legality, E-commerce platforms cannot engage in industries prohibited by law. From the perspective of rationality, since users' authorization comes first and business activities of E-commerce platforms will develop over time, their business scope may change. When it is too late to obtain users' re-authorization consent, E-commerce platform operators should follow reasonable principles to use the personal information they have obtained without using information beyond the reasonable limits that can be foreseen at the time of user authorization.

The principle of purpose limitation is based on the commercial use of personal information. If personal information is used for academic research, public security and other activities necessary for public welfare, the purpose is legitimate and reasonable and will not be used for other activities. Only in the commercial use of personal information, the purpose of use may change with the development of the E-commerce industry and the overall operation of the E-commerce platform. There is a broad space for use, so it is necessary to limit the purpose of using personal information.

3.2.2 Principle of Disclosure

E-commerce platform operators must disclose the collection and use of users' personal information. From the perspective of the objects and scope of disclosure, E-commerce platforms should disclose to users the types, scope and purposes before collecting users' personal information. In addition, during personal information processing, the use of personal information involved in the E-commerce platform should be disclosed twice according to the changes in the business activities of platforms. At the same time, according to the relevant provisions of the Personal Information Protection Law, E-commerce platform operators are required to regularly release social responsibility reports on personal information protection in the form of reports and accept public supervision. From this perspective, the objects of the personal information processing activities disclosed by E-commerce platform operators not only include the existing user groups themselves, but also include the public that may be transformed into potential users.

3.3 Transmission Step

3.3.1 Principle of Safety

In terms of technical protection, users' personal information obtained by E-commerce platforms is stored and preserved in the form of electronic data, so advanced technology is the basis for the

realization of the principle of personal information protection and security. In this regard, E-commerce platforms need to build special firewalls, hire professional information security technology experts, and encrypt users' personal data processing activities. Through the above protection approaches, the purpose of protecting the personal information delivered to the E-commerce platform by users is realized.

When users' personal information is no longer used, E-commerce platforms must delete it. If the information gathered by the early stage of the electric business platforms accompanied by losing its timeliness, along with the development of the time, for example, originally collected information is no longer applicable to the business development direction of electric business platforms, the original user personal information no longer has commercial value, right now it's necessary for electric business platforms to timely delete users' personal information. Although this part of information has no commercial value for E-commerce platform operators, it is still the condensation of users' personal dignity value. Once leaked, it will bring troubles to users' daily life and freedom of action. Therefore, when information is no longer in use, E-commerce platforms need to delete information to protect the rights and interests of individuals.

In the process of information reauthorization, the transmission path must be secure and users must know about it. The security of transmission path still belongs to the scope of technical protection, but the user's knowledge needs to be implemented through legal system. For example, when the E-commerce platform is upgraded and its business scope is expanded, if the E-commerce platform transmits the user's information to others without the notification of reauthorization, it may be suspected of illegal use activities beyond the purpose limit of the usage scope and in violation of relevant personal information protection laws and regulations.

At the same time, in the case of cross-border transmission of users' personal information, it is necessary to ensure information security. User personal information may contain a lot of important security information, such as biological genetic information. This type of user's personal information needs to be prohibited from leaving the country when it is transmitted across borders. In this regard, E-commerce platforms should comply with the cross-border transmission of personal information. Once cross-border transmission of personal information is involved, they must report to government departments in accordance with laws and regulations. Key infrastructures storing users' personal information, such as cloud servers and large memory, should not be densely distributed abroad, but should be distributed in China as far as possible, so as to prevent information leakage of users' personal information abroad.

3.3.2 Principle of Approval

As the collection of personal information is complex and the use of multiple channels, it needs to involve the internal and external multi-link approval process. A specialized information technology department shall be set up within an E-commerce platform operator. When an enterprise needs to use personal information internally, it first needs to review the technical risk of using personal information through the specialized information technology department, so as to do a good job in the internal approval process. Secondly, when E-commerce platform operators use personal information for cross-platform information transmission, the internal technical departments of both parties need to communicate and connect. Thirdly, when the personal information processed by E-commerce platform operators is sensitive, it needs to be approved after security review and can only be transmitted after obtaining approval from relevant departments.

4. Suggestions on the Development of E-commerce Platform from the Perspective of Personal Information Protection

4.1 Improve the Construction of Internal Compliance System

First, E-commerce platforms should train their employees. After the promulgation of new laws, existing employees should be trained so that they can systematically understand the latest laws. At

the same time, these training activities should be held on a regular basis, to be followed up with the continued promulgation of future legal regulations and implementation guidelines.

In addition, in terms of cultural building of the company, cultural awareness and cultural atmosphere should be formed to protect users' personal information. Employees are individuals in a company. The company's business philosophy will influence employees' behavior and make them pay more attention to information security when accessing and using users' personal information. To create such an atmosphere, the company should set up a special department responsible for this matter.

Collaboration between different parts of the company also needs to be emphasized. The transfer and succession between different departments need to form a fixed process, and establish a set of user personal information protection paradigm. This can not only ensure reasonable and compliant use of personal information, but also promote the overall management of the company.

In addition, supervision mechanism should be introduced, as well as reward and punishment system should be established to assist the operation of supervision mechanism. Any person in the company has an effective channel to report to the company about staff members or departments who violate the information protection rules and regulations. If the report is accurate, the whistle-blower should receive incentives, such as bonuses or honorary titles. Meanwhile, the informant should also receive corresponding punishment, such as notice of criticism, fine bonus and even bear legal responsibility.

4.2 Improve Compliance Awareness and Ability of Staffs

First of all, the managers should vote on the implementation of user personal information protection and set relevant examples, such as encouraging employees who have made contributions to personal information protection to be commended. At the same time, the spirit of user personal information protection can be conveyed from top to bottom through internal speeches or meetings.

Secondly, the compliance department should coordinate the work related to personal information protection and provide systematic document support. At work, the compliance department shall take the initiative to assist the management in formulating the compliance management system for the protection of user personal information and drafting the compliance management plan for the protection of personal information. For newly developed businesses, the company shall assess the risk of disclosure of users' personal information, and coordinate the cooperation of all relevant departments to deal with the risk. At the same time, it is necessary to track the changes and development of relevant laws and regulations and the industry itself, and according to the relevant requirements, put forward or formulate rules and regulations of the company on the protection of user personal information.

The technical department shall provide technical support for personal information protection, coordinate the construction of personal information protection for relevant users, improve the existing protection technology, and reduce technical loopholes. At the same time, we should protect ourselves against possible technical risks, such as virus attacks, and formulate countermeasures and backup plans.

Other business departments in the company should actively cooperate with the above-mentioned departments. In daily work, other departments should implement the spirit of user personal information protection, in strict accordance with the rules and regulations. If such departments encounter the problems related to user personal information, they not only provide timely feedback with the corresponding departments, but also do a good record of the work with convenient follow-up management and accountability.

4.3 Increase Investment in Information Security Technology

The openness of the network determines that even if the user's personal information is only stored inside the enterprise of E-commerce platforms, it may be stolen by criminals. The main business of E-commerce platforms is E-commerce, and it is not a professional information technology company. When it is equipped with information security technology, it will consider the cost of input. Therefore,

the information security technology equipped by general E-commerce companies often results in limited investment based on the economic considerations of cost and efficiency, which will bring objective obstacles to the prevention of users' personal information leakage risk. Therefore, in order to effectively protect users' personal information, it is necessary to increase the input of E-commerce platform operators in information security technology.

Based on the necessity and urgency of information input, E-commerce platform operators should increase information security technology input at the current stage. First of all, E-commerce platform operators need to consider budget planning in terms of finance. New information security technology often needs enough capital as the foundation, so the company should combine its own economic strength, reserve enough capital for information security technology, in order to ensure the subsequent development. Secondly, E-commerce platform operators should purchase some advanced technologies. Taking blockchain technology as an example, its application in the field of E-commerce can effectively protect users from fraud [7].

At the same time, E-commerce platform operators should hire professional information technology personnel to guide information protection compliance work. According to the article 57 of the Personal Information Protection Act, it also includes the establishment of a third-party independent supervision agency and systematic supervision and regulation with improving its security and reducing its risk loopholes through internal and external integration. Finally, E-commerce platform operators should regularly review and give feedback, and enterprises receiving feedback should carry out internal rectification and system improvement in a timely manner.

5. Conclusion

The current economic development has gradually entered the era of data, and the rapid development of E-commerce platforms enables users' personal information to achieve extensive and centralized aggregation in the online business world. At the same time, the characteristics of E-commerce platform itself, such as releasing information and matching transactions, make users' personal information with legal value become a very important factor of production for E-commerce platform. The lack of compliance construction on E-commerce platforms will increase the risk of users' personal information being abused. Therefore, it is increasingly necessary to restrict the collection and use of users' personal information by laws on E-commerce platforms.

At present, legislation has endowed E-commerce platforms with certain functions of public information protection, among which personal information protection is a specific requirement for E-commerce platforms to perform public functions in the future. In today's business environment and legislation environment, the system construction of E-commerce platform operators to protect users' personal information should start from the collection, use, transmission and other aspects, pay attention to the principles of clarity, authenticity, voluntary authorization and other principles, through means such as de-labeling, so that personal information can be used legally and reasonably. At the same time, in the process of information transmission, E-commerce platform operators should follow the principle of security and approval. Based on these principles, E-commerce platforms should pay attention to the establishment of a sound internal compliance process, improve the compliance awareness and work ability of internal staff, and increase input in information security technology while specifically building relevant protection systems. At present, platform enterprises in the booming E-commerce industry consciously undertake legal obligations and social responsibilities for personal information protection, which is conducive to promoting the benign integration of industry development and social governance and realizing a good cycle of the entire E-commerce ecological environment.

References

- [1] Zhang. From Privacy to Personal Information: Theory and Institutional Arrangement of Benefit Remeasurement [J]. Chinese Law, 2015(03):38-59.

- [2] Ju and Wang. Legal Protection of European Union Consumers' Personal Sensitive Data in the Context of Cloud Computing [J]. Journal of Law,2014,35(08):79-85.
- [3] Hu. Conception of The Definition of Personal Sensitive Information in China [J]. Chinese Law, 2018 (05): 235-254.
- [4] Yan and Wang. Analysis of Personal Information Protection Strategy under the Background of Civil Code Compilation [J]. Legal Expo,2021(10):65-66.
- [5] Zhang. Personal Information Protection in E-commerce Platforms from Constitutional Perspective [J]. Market Weekly, 2021,34(04):175-177.
- [6] Wang. The Definition of E-commerce Platform Operators: An Analysis based on The Article 9 of E-commerce Law [J]. The People of the Rule of Law,2018(20):23-27.
- [7] Zhang. Application Analysis of Blockchain Technology in Network Security [J]. Network Security Technology and Application,2021(08):12-13.