

E-Commerce Platform Data Ownership and Legal Protection

Changjun Wu, Xinhui Zhang

School of Law, Beijing Wuzi University, Beijing, China

ABSTRACT

In order to better distinguish the issues of data ownership in e-commerce platforms, this article starts with the basic theory of data rights on e-commerce platforms, studies the current status of e-commerce legal regulations, and explains relevant data rights regulations from the aspects of legislation, law enforcement, and justice Practice and analyze how to scientifically allocate rights, obligations and responsibilities in practice based on classic cases of data rights protection on e-commerce platforms. Through the research on the existing data of e-commerce platform data rights, the comparative analysis method is used to analyze the main problems in the development. The e-commerce platform data rights protection legal system, law enforcement protection methods, and judicial relief systems still need to be improved. Finally, corresponding perfect countermeasures are proposed for the above problems. China should further improve the e-commerce platform data rights legal system, law enforcement mechanism, and judicial relief channels, improve the self-discipline mechanism of industry associations, improve the internal data governance capabilities and levels of e-commerce platform enterprises, and provide a comprehensive and systematic legal protection for the protection of e-commerce platform data rights.

KEYWORDS: E-commerce platform; Data ownership; Data rights; Legal protection; Legal responsibility

I. INTRODUCTION

In recent years, e-commerce platforms represented by Taobao, JD, and Pinduoduo have occupied China's main e-commerce market. From cities to rural areas, Chinese people use e-commerce platforms to conduct transactions more and more frequently. In the process of people increasingly transforming from traditional transactions to online transactions, information networks not only play a huge role, but also have security threats. In the era of big data, it is easy for people to leak personal data in the process of trading on the platform. With the promulgation of the E-commerce Law in 2018, many scholars have begun to study the intellectual property rights, infringement liability, and information protection of e-commerce platforms. Since this article studies the data ownership issues of e-commerce platforms, it needs to consider issues such as tort liability and personal information rights protection, so this type of research has certain reference significance for this thesis.

II. Current status of legal regulations for data rights protection on e-commerce platforms

At present, China has been deepening research on data rights on e-commerce platforms, striving to make greater breakthroughs in legislation, law enforcement, and judicial levels. This section summarizes the current status of data rights legislation in China. Since China's current legislation is relatively fragmented, In the "Electronic Commerce Law", "General Principles of Civil Law", and "Tort Liability Law", they will explore and summarize the relevant law enforcement and judicial status, and analyze with classic cases.

How to cite this paper: Changjun Wu | Xinhui Zhang "E-Commerce Platform Data Ownership and Legal Protection" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.680-686, URL: www.ijtsrd.com/papers/ijtsrd32983.pdf



IJTSRD32983

Copyright © 2020 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (<http://creativecommons.org/licenses/by/4.0>)



A. Current status of legislation for data rights protection on e-commerce platforms

Legal systems such as the General Provisions of the Civil Law, the Tort Liability Law, the Electronic Commerce Law, and the Contract Law provide legal protection for the protection of data rights on e-commerce platforms and promote the healthy development of data rights transactions. However, China's protection of data rights has not reached the level of other mature protection systems. There are still a large number of disputes over data ownership, and they are all typical cases with greater impact. For example, data disputes between Tencent and Huawei, major e-commerce platforms have data ownership disputes, and the consequence is often that both parties have losses. Moreover, looking at the current law popularization activities in society, there are few legal popularization topics with the protection of data rights, and there is also a lack of formal official platforms for popularizing knowledge of data rights protection. [1] In China, the personal data protection norms are scattered in different laws such as the "General Principles of Civil Law" and "E-commerce Law". For example, Article 111 of the General Provisions of the Civil Law stipulates that the personal information of natural persons is protected by law. [2]

1. Relevant regulations of the E-Commerce Law

After using comparative analysis to find the regulations on data rights in the "Electronic Commerce Law" and other laws, I summarized and sorted them out. During the legislative process, the legislators started to consider from the perspective of data protection. Some laws already

involve data. Protected content. Starting from the first spread of personal data on e-commerce platforms, it must be based on law. Operators and e-commerce platforms collect personal data through formal methods, rather than other illegal means.

There will be mediation procedures before normal litigation procedures in China, and mediation procedures are also adopted for data ownership disputes. In the e-commerce platform, if there is a dispute between the buyer and the seller, there is a page for submitting personal evidence inside the platform. After the evidence is submitted and the reasons are explained, the staff responsible for resolving the dispute will review the evidence provided by both parties and give both parties time to proceed. Negotiation. If the negotiation fails, the responsibility will be determined based on the evidence submitted by both parties. Since China added the Hangzhou Internet Court under the court system, online operations have improved the efficiency of case handling. Both parties do not need to go to the court of litigation. However, there are also some shortcomings. When data ownership disputes occur, it is difficult to obtain complete evidence. One party is not fair.

2. Relevant provisions of the "General Principles of Civil Law"

In the "General Principles of Civil Law", the concept of data rights can be summarized from the part of personality rights, including privacy rights. In the process of codification of the civil law, the protection system for personal data rights has been infiltrated and strengthened. Individuals can file infringement suits. After the revision of the general rules of the civil law, provisions on personal information rights have been added. The personal information right is mentioned here because the draft research on the personal information right in the civil law is more comprehensive than the personal data right. In addition, the civil law does not specify the scope of data and network virtual property in detail, but it mentions the protection of data and network virtual accounts. From the perspective of legislators, it is more to consider other special legislation, which will also become the focus of legislation.

3. Relevant provisions of the Tort Liability Law

The "Tort Liability Law" provides relevant provisions on the protection of e-commerce data rights, such as Article 38 of online infringement liability, from the perspective of the legislator to protect the interests of individuals. When the infringer realizes that his data rights may be threatened by the infringer, he can ask the infringer to take measures against the infringed rights, which is undoubtedly a way of relief. When an e-commerce platform user infringes on other users, whether as an operator or an e-commerce platform, if the infringement is known to have occurred and no measures are taken to stop it, the infringement shall also be liable for the infringement. Therefore, it is recommended that the Ministry of Industry and Information Technology of the People's Republic of China take the lead to organize the drafting of well-known experts and scholars across the country, listen to opinions widely online and offline, and make contributions to China's e-commerce data rights protection law. [3]

B. Current status of data rights protection law enforcement on e-commerce platforms

In May 2019, the State Cyberspace Administration of China issued the "Data Security Management Measures (Draft for

Comment)", in which detailed regulations have been made on the processing and use of data, and a large amount of relevant content of the GDPR has been borrowed. The GDPR "General Data Protection Regulation" issued by the European Union in 2018 can be regarded as the most severe and strictest regulation currently. The regulations are mainly aimed at enterprises with heavy penalties, and minor behaviors are also penalties. Relatively speaking, users can better protect their rights through the regulations. Companies wanting to obtain user data must obtain their own permission. For small businesses, it is easier to touch the penalty edge of this regulation. After the introduction of this regulation, many companies closed their open platforms to the EU or changed it to the simplest page. Because the profit is far less than the amount of a fine paid here.

So, can China enforce such strict regulations on companies like the EU? This is worth thinking about. First of all, disputes about data ownership are no longer confined to the country. It is common to leak data from China to foreign countries or steal data from foreign countries. China is currently not only trying to increase the intensity of data rights management in legislation, but also making many efforts in law enforcement. Although China is learning from mature foreign legal systems in legislation, the legislation still has the disadvantages of being scattered and vague. In order to better protect data rights, companies should be aware that the purpose of data rights protection is to protect their own interest. As there is currently no clear basis for law enforcement, relevant authorities cannot easily impose legal sanctions on companies. It is necessary to increase the regulations for business operators on the basis of the regulation of business operators in the "E-Commerce Law" to reduce implementation difficulties, save legislative costs, and increase enforceability. [4]

C. Current judicial status of data rights protection on e-commerce platforms

From previous academic seminars, it can be found that experts and scholars have a need to improve the current status of judicial protection of data rights, and specifically analyze from the following aspects. In terms of judicial regulation, the criminal law is the last resort to protect data rights. In e-commerce platforms, the problem of data rights violations is very concentrated. However, when data is illegally used, there is no accurate motive to report crimes. Therefore, there are fewer criminal cases involving data rights. In addition, the criminal law's description of combating data rights infringement is not accurate enough. Some scholars believe that crimes on the Internet require criminal law to play its role, but they need to accurately crack down on illegal acts. Secondly, in the relevant data rights protection legislation, it is necessary to focus on how to balance personal data protection and rational use of data. The combination of economic incentives and rights protection can be introduced to enable users to have a higher level of experience in e-commerce platforms. Status to protect their rights, so as to protect the data rights from infringement while ensuring the full flow of data. Analysis of typical judicial cases—Taobao sued Meijing Company for unfair competition. This case is the first case in the Internet court regarding data ownership disputes, which serves as a warning and standardization in the e-commerce industry. Although this case judged the dispute to be unfair competition, it has promoted progress in improving data protection. The first instance of the case pointed out that

"the practical value of the original data lies in the content of the network user information it contains, not in its form." It can be seen that the missing data basically includes the category. [5]

III. The main issues of legal protection of data ownership on e-commerce platforms

A. The legal system still needs improvement

1. Lack of entitlement norms

At present, China's laws and regulations on the protection of e-commerce data rights are scattered in different departmental laws. Although most of them exist in the civil law as a whole, there are some important terms defined in the regulations. Moreover, the reason why it is difficult for most scholars to grasp the concept of data in academics is that data belongs to the content that is constantly flowing in the Internet information network and its coverage is relatively large. In the event of rights and obligations, the "Network Security Law" can be invoked to regulate, but in its obligatory regulations, there is no stipulation on the rights that operators can enjoy. [6] The "Network Security Law" as a whole only constitutes a system for the protection of personal data and information, and it still lacks operability. Previously, other representative countries have made relevant regulations on data rights, including rights and obligations, distribution of responsibilities, remedies, etc. At the same time, under the impact of traditional transaction models, China will also form multiple uses of the Internet in the future. Therefore, it is necessary to formulate laws and regulations that suit and promote China's e-commerce data protection based on China's national conditions and the current e-commerce development status.

2. Easily lead to data leakage

In the transaction of e-commerce platform, whether as an operator or a platform, the user's data is collected legally in accordance with the agreement signed by the user when using the platform. Although this data includes some basic personal data, such as personal name, phone number, contact addresses, etc., but these data are sufficient to enable them to achieve illegal purposes. Generally, the content filled in when mailing express delivery includes name, phone number, etc., which can be mailed to the other party, and the mailing party can choose to conceal data about itself. [7] But in fact, contrary to the original intention set, in the e-commerce platform, the user, the operator, and the e-commerce platform are equal subjects. Considering that the civil law is cited above to resolve the data rights case, because the civil law resolves. It is the personal and property issues between equal subjects. In combination with the problem of data collection, when users want to collect data about operators and e-commerce platforms, the only way they can take is to use search engines to find relevant data, which is obviously not accurate and complete compared to the collected data, which puts it in an unequal position with the platform. After collecting personal data in accordance with the law, operators have the right to the nature and content of the collected and stored personal data, and what kind of civil law relief they can obtain when others infringe such rights. These issues are important to data technology and industry. The development is very important.

3. Legal use of data rights

Data rights are of a constitutional nature. When state agencies collect personal data in accordance with laws and

regulations, all parties should provide them in accordance with the requirements of the administrative department. The competent authority here refers to the competent authority responsible for managing the database in the country. In the work of national data management agencies, it is often necessary to collect personal data of citizens and attribute them to the database under the premise of ensuring that personal data is not leaked to enterprises or other countries. Most citizens did not respond when their data was collected. This act of providing their data to relevant state departments can be regarded as a citizen's obligation to the state. Under normal circumstances, what the state does has not caused any loss to citizens, and it is more for the country's daily work. In comparison, when an individual provides data to an operator, the operator needs to fulfill the obligation of protecting the individual's data and ensuring that it is not leaked. As a third party other than the buyer and the seller, the platform must handle all the data of both parties in this process. Therefore, when competing or conducting transactions between platforms, the first purpose should be to protect the data of all subjects on the platform. In the era of big data, the focus of competition has shifted to competition for big data. Therefore, it is necessary not only to protect data from being leaked in China, but also to protect data from leaking to other countries.

B. Law enforcement protection methods still need to be improved

1. Data infringement is difficult to obtain evidence

After the user's data is infringed, the user is relatively in a weak position. When it comes to obtaining evidence against the process of its data being leaked and infringed, the actual operation is difficult. In the age when the e-commerce industry is developed, the content displayed on the Internet is always changing in real time. The content browsed in the previous second cannot be verified in the next second, so for users, it is not good for them in most cases. And from the perspective of law enforcement, how to protect the interests of the three parties in the first place still needs to be improved.

2. Lack of law enforcement protection methods

During the operation of e-commerce platforms, personal data is becoming more and more likely to be leaked. The collection, storage, transmission, processing, and generation of data in the information network cause different security threats. Once the data is collected maliciously, the subject will completely lose control over who or how the data is used. After personal data is collected by the operator or used by the platform, it is disseminated at high speed without any risk warning. The consequences are unimaginable. In addition, if e-commerce platform data rights do not have a complete law enforcement protection system, the data owned by operators may be maliciously stolen and spread by criminals. Only when a complete e-commerce platform data rights protection system is established can the possibility of illegal cases be reduced. There was a case in China in 2015. Three employees on a certain platform who did not have permission to log in to the customer information system exported their customer data into a table after logging in to the account and password of the authorized supervisor, and then each piece of data was sold to fraud at a different price. This has caused a large number of customers to encounter fraudulent calls in a short period of time. At present, there are still some deficiencies in China's law enforcement

protection methods. The original party of the data and the party holding the data are in an unequal position, resulting in an imbalance between the two parties. In most ownership disputes, it is the defendant who is responsible for the burden of proof, not the plaintiff in civil disputes, and it is only in this case that the two are substantially equal. In addition, a universal strict liability system should be established to reduce the infringer's defense to a minimum. [8]

C. The judicial relief mechanism still needs improvement

1. Victims have difficulty seeking relief

There is a lack of clear, specific and highly operable provisions on remedies such as claims and prosecution after infringements in the "E-Commerce Law", which leads to the fact that when the victim is defending his rights, he does not know which agency to look for to protect his data rights. Moreover, when people are faced with data infringement, their ignorance of the prosecution procedures and the materials that need to be prepared will cause people to ignore the importance of maintaining their data rights in a timely manner and choose not to prosecute. The victim may also consider whether the time and cost required are comparable to the damage caused by the infringement. Therefore, when there is less reward for maintaining data rights than ignoring the infringement, people will choose the latter.

2. The compensation amount is not clear

As mentioned above, the current legislation is not perfect, and there is no specific measure of the amount of compensation related to the prosecution. For example, in the case of Sina Weibo's sued Maimai, the amount of the appeal was 10.3 million yuan. The actual amount of compensation is only 200,000 yuan. Compared with data infringement cases of the same type, the amount of compensation is smaller, and it is also a case of data infringement that has occurred earlier in China, so there is no clearer compensation amount to refer to. In most cases, the decision is made based on comparing the amount of compensation awarded in similar cases, which will take into account the value of the data involved or the degree of damage to the victim and the length of time.

3. Inaction by relevant law enforcement agencies

In China's e-commerce industry, consumers' personal data security faces the risk of being illegally collected, used, leaked, and traded. The protection system for personal data security is relatively incomplete. [9] Relevant departments are prone to management omissions or management overwhelming problems in e-commerce platform data ownership cases. When facing the same dispute, all parties have the power to manage or supervise, the law enforcement department may cause Inaction. Moreover, most users do not know whether they are being tracked. For example, mobile phone software will share the user's name, password and other data with partners, which may cause unrestricted use of data by third parties. One of the factors for the continued success of the e-commerce platforms we know today is personalization, which is mainly due to their tools to keep track of what users browse. Moreover, the scope of data collectors will become larger and larger, and a large amount of dizzying data will be collected continuously. The relief mechanism needs to be more complete and systematic to protect the rights of users, operators, and e-commerce

platforms, so that when faced with difficult cases, all parties will have more relief channels.

IV. Perfect countermeasures for legal regulation and protection of data rights on e-commerce platforms

By summarizing China's current legislative, law enforcement, judicial and other aspects that need to be perfected, it is found that scholars' views are focused on the legal regulation of e-commerce platform data rights, and they also have sufficient reasons to support their views. Regarding legislation, there should be special laws to regulate, in order to clarify China's emphasis on the protection of data rights on e-commerce platforms; for law enforcement, China's existing basic principles should be used to promote the improvement of law enforcement mechanisms; for justice, it should be targeted at Improve judicial remedies and put forward reasonable suggestions.

A. Improve the legal system of e-commerce platform data rights

1. Determine the rights and obligations of the subject

Regarding the above-mentioned "Cyber Security Law" that stipulates the obligations of operators but not the norms of rights, I believe that any party in the e-commerce platform should be given equal rights and obligations, because the e-commerce platform, Operators and users are relatively equal. In the process of revising civil rights, the relevant provisions of personal information rights can be used as a reference. Since it belongs to the rights enjoyed by civil subjects, it is necessary to follow the principle of equality. When it comes to data ownership disputes, only when the civil entities of both parties enjoy equal rights and obligations can data rights be better protected. In terms of legislation, it is inappropriate for China to adopt industry self-discipline to regulate the collection and transmission of personal data by network operators. [10] In the EU's "Uniform Data Protection Regulations" regulations, the two parties are given equal legal status and the establishment of a dual system that combines the self-discipline of data controllers and the supervision and management of regulatory agencies to promote the implementation and implementation of data protection related laws. Implement.

2. Centralized data rights legislation

Regarding the legal protection system for data rights of China's e-commerce platforms, the shortcomings of fragmentation and fragmentation should be discarded and a special "Data Law" should be formulated. And to improve the "E-commerce Law", because currently the most closely related to the e-commerce industry is this law, its promulgation also guides more legislators to think about improving the e-commerce legal system, making them aware of the importance of the legal protection system for business data rights. In addition, the data rights were legislated based on the development status at the time, but now the Internet has gradually evolved into a big data background, so it is necessary to update the data protection rules. Decentralized legal regulations are not conducive to the development of the legal protection system for data rights on e-commerce platforms in the future. Only when the system is clear can legislators more clearly improve relevant legislation. I suggest that the "E-Commerce Law" regulates the distribution of rights and responsibilities in response to the issue of data ownership in different situations, and what

China really needs is to improve the law on data infringement-related crimes from the source, so multiple departments can be adopted for joint governance Way to protect the data rights of e-commerce industry entities. The US Federal Trade Commission has proposed that the management platform enable it to take measures to counter-identify data. China can specify the operating range of the platform in legislation to reduce the possibility of data abuse.

3. Protect citizens' data rights

China's "Decision on Strengthening the Protection of Online Information" clearly stipulates that "Internet service providers shall abide by the principle of lawfulness and obtain the consent of the collected persons...", when data rights are regarded as civil rights, equal civil subjects must of course not engage in illegal acts. In order to highlight the protection of data rights, it should be embodied into the right of informed consent, the right to delete, etc., so that the data subject can obtain sufficient self-determination rights in the actual process, and provide sufficient material protection for data rights.

In the Chinese Civil Code, the infringement liability section focuses on punitive damages for infringement of intellectual property rights. It can be seen from this that the protection of individual legal rights by legislators is no longer limited to the losses caused by the infringement of rights, but should also include damages to the infringer punishment. Moreover, in order to strengthen the protection of intellectual property rights, some committee members proposed that the cost of violations must be increased so that the infringers will be more awed by the law. In addition, in terms of tort liability, it is stipulated that the network user provider shall be liable for damages caused by wrong notification. Both of the above two amendments have further strengthened the protection of the aggrieved party and brought the direction of Chinese legislators closer to the development of the times. In the future related rights protection legislation, the protection of citizens' data rights should be strengthened.

B. Improve the enforcement mechanism for data rights protection on e-commerce platforms

1. Clarify the distribution of powers of each department

Legislators formulate relevant regulations to clarify the distribution of powers of various departments, so that when any dispute arises, there are targets for seeking relief, and at the same time, it is also to solve the hidden problems existing between the previous departments. At present, there is no special regulatory agency in the legislation. When problems arise, the public security departments and management departments have the power to solve them. When the departments at the same level have the power to regulate, it is impossible to clarify the department to which such problems belong, or when the case is complicated and there are interests entangled, there may be prevarication between different departments, which may make the case unable to be resolved in time. Therefore, it is necessary to advocate the principle of high efficiency and convenience in the administrative law. After adopting the above suggestions to set up the supervisory department, the responsibilities of the supervisory department and other departments should be clarified, and all entities must abide by the laws of the country, and the relevant departments must serve the people. , Make it play its true role.

Under the above-mentioned circumstances, we should first focus on legislation to make each department clarify how to exercise power to deal with data ownership disputes, so that power can be used on the cutting edge, and China's supervision and management system should be improved as soon as possible. It is possible to set up a special data supervisory agency that mainly protects data rights, and at the same time legalize its supervisory authority and scope to make its internal personnel more professional. In addition, the establishment of a third-party agency authorized by law to be responsible for data ownership disputes, and its auxiliary nature can make up for the omissions of other departments in data ownership disputes, and the purpose is to make the e-commerce industry better develop. Legislation makes law enforcement more maneuverable, laying a good foundation for judicial relief.

2. Improve the burden of proof system

Based on the above-explained differences in the legal status of users, operators and e-commerce platforms, it is recommended to establish a burden of proof system. Here, according to China's provisions on the principle of the inversion of the burden of proof, for example, in tort litigation related to high-risk work causing damage to the person, the infringer is responsible for the proof of the damage fact. The original intention of the establishment of this principle is that in such infringement litigation, the victim has difficulty in presumption of fault, presumption of causation, and evidence collection, etc., and this principle is conducive to timely protection of the rights of the victim.

But in fact, due to the complexity of the inversion of the burden of proof, this principle may also be abused. Because the victim is at a disadvantage in terms of human and financial resources. In the case of the inversion of the burden of proof, other situations that actually have difficulty in producing proof for the victim are not fully included in the legal provisions, so irregular operation and incorrect understanding have further appeared, which directly affects the justice of justice. It runs counter to the prestige of the law in people's minds. In spite of the above circumstances, it is still recommended to adopt the principle of inversion of the burden of proof in data ownership disputes on e-commerce platforms, so that users do not have to bear the burden of proof when suing the operator or e-commerce platform after being infringed, but one of them Undertake the burden of proof to protect users' data rights, and at the same time, we need to pay attention to avoiding situations that affect judicial justice.

3. Give full play to the supervisory function of consumer associations

The concept of multiple co-governance requires that the consumer association's legal protection of user data rights and interests should be fully utilized. The Consumer Association is a statutory body authorized by the Consumer Rights Protection Law to supervise the operation of operators in accordance with the law and protect the legitimate rights and interests of consumers. Its main tasks are to exercise supervision duties, protect consumer rights, and do a good job in mediating data rights disputes and supervision Businesses who publish false information, but the Consumer Association mainly manages offline transactions, and there should be institutions specifically for Internet transactions to monitor e-commerce platform

disputes, so as to ensure the normal conduct of offline transactions while also ensuring online transactions. Security of online transactions. In addition, the consumer association can investigate the relevant issues of consumer complaints and respond to the administrative department. If the relevant behavior of the operator or the platform does cause losses to consumers, the administrative department should promptly resolve it.

Severe penalties should be imposed on acts of illegally obtaining original data that endanger the privacy of data subjects. The administrative department should increase the penalties for such behaviors, so as to make the supervisory role played by the consumer associations more clear, so that the victim can increase the trust in such supervisory institutions, and serve as a warning to other relevant subjects. , So that it will give priority to its security issues in future data processing. In addition, supervisory agencies should also take the initiative to take measures to ensure data security, and try to enable data controllers to eliminate private personal information in the original data to avoid distressing consumers.

C. Improving the judicial relief mechanism for data rights on e-commerce platforms

1. Play the active role of judicial relief guarantee

Justice is the last line of defense to safeguard social fairness and justice. The reason for this interpretation of the judicial status can be corroborated by the case of Jiao Zhigang. Jiao Zhigang was fined two hundred Yuan by the public security agency after reporting the false police report. After that, the public security agency thought that Jiao Zhigang's punishment was less severe, so he revoked the original punishment and changed it to detention for ten days. He refused to accept the punishment of the administrative agency and filed an administrative review. Detained for fifteen days. Regarding the result of this reconsideration, he applied to the court for an administrative lawsuit, and the court finally revoked the administrative agency's punishment. Similar cases abound in practice, and the judiciary plays a key role at the last moment. As the law stipulates that judicial, administrative, and supervisory agencies are equal in the national institutional system, they can exercise judicial, administrative, and supervisory rights more clearly.

In addition, similar to the actions of the parties in this case that are less harmful to society, they should be sentenced to punishments corresponding to their actions. At present, the Chinese judicial organs can only compare the amount of judgment in a typical case to get the amount of punishment corresponding to the case. From a long-term perspective, China should specifically legislate on the amount of penalties. It can refer to the amount of penalties in intellectual property disputes and formulate a detailed and specific compensation system, which may include compensation for personal and property damage. For example, when a user trades on an e-commerce platform, the property loss caused by his own data leakage and the indirect loss to the right holder after the data right is violated. In addition, after data leakage has caused mental harm to e-commerce platforms, operators, or users, reasonable compensation should also be made based on the actual situation. When encountering data ownership

disputes, citizens must first think of seeking relief from the judicial organs in order to enable the judicial organs to give full play to their role, and then according to the court's judgment of the corresponding compensation amount, so that the rights of the infringed are protected.

2. Give the victim the right to confront

The basis for perfecting the reliance of judicial channels is the national laws and regulations. Therefore, only after the legislation on the protection of data rights reaches a certain level of perfection, the infringed can effectively seek remedies. In China's legislation on data rights on e-commerce platforms, the law clearly stipulates that the rights of victims are scattered, which makes it impossible to play the role of justice more effectively. As mentioned above, the suggestion that China should enact special legislation to protect the data rights of e-commerce platforms and improve the "E-commerce Law" in a timely manner are paving the way for future ownership disputes.

In the transaction process, it is difficult for users to take some measures to ensure that their data rights are not infringed in time, and there are certain difficulties in operation. When users find that their data rights have been violated, they should be given rights in order to protect their rights to the greatest extent. To fight against the infringement, because users cannot turn to the e-commerce platform for help at this time, and the operation of the operator is not controlled by the platform, and can only help the user to negotiate with the operator. Only by giving the victim the right to stop the infringement against the infringer can the disputes over the ownership of data within the e-commerce platform be resolved more timely and accurately.

D. Improve the self-discipline mechanism of industry associations

Promote the establishment of industry associations in key areas such as e-commerce and artificial intelligence, and expand the scope of participants in the industry as much as possible by using leading companies to take the lead and encouraging SMEs to join. [11] Among Chinese e-commerce companies, several well-developed e-commerce platforms play an important role in the entire e-commerce industry, such as Taobao, JD, Pinduoduo, etc., and the e-commerce industry is now a key field in China. In the future, more subjects will participate in this field. Therefore, it is necessary to establish an industry association to enable the e-commerce industry to reach an agreement on the protection of data rights, so as to promote better resolution of data ownership disputes on e-commerce platforms. China's existing e-commerce industry associations have established self-regulatory treaties on the protection of data rights in the Internet, which will stimulate the development of industry associations in the future, such as the "China Internet Industry Self-Regulation Convention" promulgated by the Internet Society of China. Internationally authoritative legal documents on data protection indicate that data rights can be protected by compulsory regulations such as industry standards and technical standards through the national public power. China can also strengthen the self-discipline of industry associations and improve the system of regulatory agencies. Promote the implementation of data rights laws. Industry associations should play the role of commanding the overall situation and regularly organize the enterprises

within the association to study laws and regulations, including formulating industry norms and regulations, and understanding the latest developments in Chinese laws.

E. Enhance the internal data governance capability and level of e-commerce platform enterprises

Leading e-commerce platform companies need to continue to play their own role in the protection of data rights on e-commerce platforms, including strengthening corporate internal governance, attaching importance to the protection of data ownership, and formulating data rights protection systems so that the data of platform users can be used legally. This will set a good example for future development of e-commerce platforms, and make the entire e-commerce industry pay more attention to the protection of data rights. The era of big data has higher requirements for the comprehensive level of talents, so we must pay attention to the training of internal data talents in the enterprise, and need to master the knowledge of law and data applications. E-commerce platform companies need to pay attention to the training of data ownership protection laws and regulations to improve data governance capabilities and levels. E-commerce platform companies can, in accordance with the needs of the e-commerce industry for the protection of data rights, make reasonable and legal formulations and improvements in terms of how to protect data rights, the definition of data rights between different subjects, and the processing rules after data rights infringement. Data rights protection rule system.

When users and operators conduct transactions within the e-commerce platform, data is also flowing between the three parties, and data disputes may arise between each other, and any entity will first protect its own data rights in the face of disputes. Therefore, once user data rights are violated, dispute resolution within the e-commerce platform has the lowest cost and the highest efficiency. Platforms and other data control and processing entities can set up data supervision specialists to improve data governance capabilities and be independently responsible for the internal supervision of the platform. When users (consumers) have disputes with merchants on the platform, the first remedy that comes to mind is to seek the help of the e-commerce platform. Although the e-commerce platform, operators and users are on an equal footing, the e-commerce platform can follow The "Business Law" and other laws provide necessary supervision to the operators on the platform in accordance with the law.

V. Conclusion

In summary, with the continuous change of information network technology, the e-commerce industry will increasingly become an indispensable part of people's lives. People use technology to change their lives and improve the quality of life through technology. E-commerce platform, as a model with a faster development speed and a higher utilization rate of people in the information network, will definitely have more problems that need to be improved in

future legislation. As the most frequent content of the e-commerce platform, data should be more responsive. Provide more adequate protection and take reasonable measures to ensure real-time data rights. However, the first purpose of the data protection law is still to promote the free flow of data. Only by solving the problem from the source can the e-commerce platform develop better and the transaction process will proceed more smoothly. At the same time, we must also pay attention to protecting the data rights of the weak, so that the legal protection system for e-commerce data rights can be used, and more people believe that e-commerce platforms can bring convenience to them and increase users' awareness of e-commerce. The trust of the platform is expected to develop faster and more quality in the e-commerce industry.

References:

- [1] Li Jianfen, Gong Weiqi. Legal protection of personal data rights in the context of big data [J]. *Legal Expo*, 2019(10): 165+167.
- [2] Chu Hongli. Research on the Legal Issues of the Utilization and Protection of Personal Data [J]. *Journal of Ningbo Radio and TV University*, 2019, 17(04): 58-64.
- [3] Meng Yuping. Legal regulations on illegal collection and processing of personal consumption data [D]. *Guangxi University*, 2019.
- [4] Meng Yuping. Legal regulations on illegal collection and processing of personal consumption data [D]. *Guangxi University*, 2019.
- [5] Han Xuzhi. The dilemma of data right confirmation and the solution [J]. *Eastern Methodology*, 2020(01): 97-107.
- [6] Zhang Shurong. Legal protection of e-commerce data information in China [J]. *Communication and Copyright*, 2018(10):164-166.
- [7] Cheng Xiao. On personal data rights in the era of big data [J]. *Chinese Social Sciences*, 2018(03): 102-122+207-208.
- [8] Zhang Shurong. Legal protection of e-commerce data information in China [J]. *Communication and Copyright*, 2018(10):164-166.
- [9] Yang Hong, Zhong Xiaofei. Research on the Countermeasures of E-commerce Consumers' Personal Data Security Crisis [J]. *Library and Information Service Guide*, 2017, 2(03): 61-67.
- [10] Xiang Liling, Wang Jinghui. Comparison of Chinese and foreign legal norms for the collection and transmission of personal data by network operators[J]. *Library and Information Service*, 2016, 60(04): 21-28.
- [11] Lin Limin. The construction of China's personal data security system under the background of big data [J]. *Straits Law*, 2019, 21(04): 38-443