

Protection of Personal Information in the Era of Big Data

Cuicui Hu

School of Law, Anhui University of Finance and Economics, Bengbu, Anhui, China

Abstract

In recent years, cloud computing and big data technologies have been widely used in China in the fields of public security, medical and health care, intelligent transportation, telecommunications and education, etc. The quality of life of the people has been improved and the digital industry has gained tremendous development, but at the same time, a series of personal information infringement disputes have arisen and the protection of personal information has attracted much attention. At present, insufficient protection of personal information under public law, the shortcomings of traditional informed consent rules, imperfect regulatory mechanism for personal information, and weak awareness of personal information protection have become major obstacles to balance the protection and utilization of personal information. Accordingly, it is necessary to adhere to the personal information protection path that combines public law protection and private law protection, to apply informed consent in the handling of personal information, and to improve the comprehensive supervision mechanism that unifies administrative supervision, industry association supervision, corporate internal supervision, and public opinion supervision, and on this basis, to improve the personal information infringement remedy mechanism that combines judicial remedy and private remedy.

Keywords

Personal Information; Personal Data; Privacy; Informed Consent.

1. Introduction

In the era of big data, personal information is continuously circulated and shared in the field of private and public rights, contributing to the rapid development of the digital economy. However, in the process of collecting and utilizing personal information, the protection of personal information often faces challenges due to the lack of remedies, the lack of special regulatory mechanisms, and the weak awareness of citizens' personal information protection. First, there is a risk of personal information leakage in the field of public power. Some scholars point out that "governments around the world are gradually trying to overcome the phenomenon of 'information silos' and carry out the integration of government data".[1] However, the fusion of government data will inevitably sacrifice or disclose more people's personal information, and the rights and interests of personal information are threatened; in addition, personal information infringement often occurs in big data investigation. Some scholars point out that big data investigation is usually applied in the field of network remote investigation, retrieval or freezing of electronic data, and has the characteristics of high technology and concealment.[2] This means of investigation in reducing the cost of investigation, improve the efficiency of investigation at the same time, often because of the lack of awareness of investigators to protect personal information, personal information is also increasing the risk of infringement. Second, in the field of private rights, automated decision-making is abused. The abuse of automated decision-making is mainly manifested in "big data", "user profiling" and "face recognition", in which information processors abuse the power of algorithms to collect and use consumers' personal information against their true will. The

information processor abuses the power of the algorithm to collect and use personal information against the consumer's true will, resulting in the leakage of personal data information. Therefore, in order to reduce the risk of infringement of personal information, it is necessary to study the protection of personal information in depth. Based on this, this paper aims to propose some specific suggestions to improve the protection of personal information, taking into account the legislative experience of foreign countries.

2. Definition of Personal Information

Currently, Article 76(5) of the Law of the People's Republic of China on Network Security (hereinafter referred to as the "Network Security Law"), Article 104 of the Civil Code of the People's Republic of China (hereinafter referred to as the "Civil Code") and Article 4 of the Law of the People's Republic of China on the Protection of Personal Information (hereinafter referred to as the "Personal Information Protection Law") all define "Personal information" is defined in Article 104 of the Civil Code and Article 4 of the Law of the People's Republic of China on the Protection of Personal Information (hereinafter referred to as the "Personal Information Protection Law"), but with some differences. The Cybersecurity Law defines personal information as all kinds of information that can identify an individual; the Civil Code, based on the legislative experience of the Cybersecurity Law, removes the restriction of "identity" and extends the scope of personal information to all kinds of information that can be identified; and the Personal Information Protection Law fully draws on the EU General Data Protection Regulation (GDPR). The Personal Information Protection Law, however, fully draws on the legislative experience of the General Data Protection Regulation (GDPR) of the European Union and stipulates that personal information includes not only identified or identifiable information, but also excludes anonymized information, further broadening the scope of personal information and helping to guide judicial practice in locating personal information more accurately.

2.1. Relationship between Personal Information and Personal Data

Table 1. The relationship between personal data and personal information and the reasons

Perspective Show	Reason
Viewpoint 1: The two have the same nature	Information is the content of data, and data is the form of information. In the era of big data, it is impossible to separate data from information and discuss the rights on data abstractly. [5]
Viewpoint 2: There are differences between the two	Personal information and personal data are the embodiment of concrete and abstract legal interests, respectively.

Regarding the relationship between personal information and personal data, there are different views in our theoretical circles. Some scholars advocate that the relationship between information and data is actually one of content and form, the connotation of personal data contains personal information, personal data is not only closely related to personal interests, but also involves economic interests, and in the era of big data, personal information and personal data are the same thing, and the two are a unified and inseparable whole.[3] Other scholars argue that there is a difference between personal information and personal data, and that the content of personal information and the specific legal interests that the content points to are determined, while personal data is obtained through processing, and the content points to an abstract possibility of legal interests.[4] The author prefers the former view. Firstly, the terms "personal information" and "personal data" both originate from the translation of "personal data", and there are only some differences in their titles, while their Secondly, if we support the latter view, in the era of Internet and big data, as the boundary between personal

information and personal data is gradually blurred and complicated, it will be more difficult to protect them in practice. Therefore, personal data and personal information are essentially the same, and personal data processing activities, conflicts and disputes can refer to the relevant provisions of the Personal Information Protection Law, the Civil Code and other laws.

2.2. Relationship between Personal Information and Privacy

The relationship between personal information and privacy has been full of controversy in our academic circles. Some scholars believe that personal privacy is included in personal information, and in the complicated network environment, it is difficult to distinguish between the two, so there is no clear boundary between them.[6] On the other hand, some scholars believe that "although personal information may contain private content, after de-identification, personal information no longer has privacy characteristics, and there is no possibility of overlap between the two." [7] Thus, it seems that there is no consensus in academic circles on the relationship between the two.

After the promulgation of the Civil Code, the concepts of "privacy" and "personal information" were defined in the title of personality rights, indicating that there is indeed a distinction between the two, but at the same time, it was also proposed that "the private information in personal information shall be subject to the provisions on the right to privacy; if there are no provisions, the provisions on the protection of personal information shall apply. If there is no provision, the provisions on the protection of personal information shall apply." This legal provision indicates that there is a link between personal information and privacy. In general, there is a certain intersection between personal information and privacy, but there is a great difference between the two, and the difference between the two is mainly: First, personal information emphasizes "identification", while privacy emphasizes "privacy". Second, personal information usually has both moral and property interests, while privacy mainly involves moral interests.[8] Third, personal information involves not only private interests, but also public interests, and therefore needs to be protected by civil law, criminal law, administrative law and other departments, while privacy mainly involves the private sphere, and the rights are mainly protected by civil law.

Table 2. The difference between personal information and privacy

Differentiation	personal information	privacy
Judgment basis	Identifiability	Privateness
Content of Rights	A combination of spiritual and property interests	Spiritual Benefits
Protection path	Civil law, criminal law, administrative law, etc.	Civil law

3. China's Personal Information Protection Facing the Reality of the Dilemma

3.1. Personal Information Inconsistency between Private Law Protection and Public Law Protection

Regarding the protection of personal information in private law, although laws and regulations such as the Civil Code, the Law on the Protection of Consumer Rights and Interests, and the Provisions on the Protection of Personal Information of Telecommunications and Internet Users in China are all covered, they are mostly in principle and are not very operable in practice.

In contrast, the formal adoption of the Personal Information Protection Law on August 20, 2021 will be more helpful for individuals to protect their personal information rights and interests in a timely and accurate manner in accordance with the law, and at the same time play a practical role in regulating the utilization of personal information.

Compared with the private law protection of personal information, the protection of public law such as administrative law and criminal law is relatively weak. At present, the provisions of the administrative law on the protection of personal information are mainly concentrated in the Personal Information Protection Law, but these provisions are rather abstract. Specifically, one is that the "relevant departments" for personal information protection are not clearly defined in the law. Although the "Personal Information Protection Law" provides that the State Internet Information Department, the relevant departments of the State Council and the relevant departments of local governments at or above the county level perform the duties of personal information protection, the designation of "relevant departments" is not clear, and it is likely that administrative organs will not act or "favorably compete for control" when administrative enforcement. The situation is that the administrative authorities may not act or "compete for control" in administrative enforcement. Second, the discretionary power of judges to impose administrative penalties is not limited. The Personal Information Protection Law for the illegal handling of personal information, set a large range of fines and a high amount, and there is no supporting administrative penalty discretion benchmark system, the discretion of judges is not constrained, is likely to lead to "different penalties in the same case". Third, the administrative organ can be the subject of personal information protection, but also the collection and use of personal information, when the administrative organ does not perform the protection duties or abuse, leakage of personal information, the law does not provide the corresponding means of relief. In addition, in terms of criminal law protection of personal information, there are individual articles in the Criminal Law concerning personal information protection, such as "the crime of infringing personal information", "the crime of illegally acquiring state secrets" and "the crime of infringing commercial secrets". In order to strengthen the protection of personal information, the Amendment to the Criminal Law (IX) regulates the use of personal information by expanding the scope of criminal subjects and infringement of personal information. It can be seen that the criminal law protection mechanism of personal information is gradually improving but not sound.

In conclusion, there are inadequacies in the protection of personal information in both private and public law. In order to truly protect the rights and interests of personal information without impeding the normal use of personal information, it is necessary to continue to improve the civil legal regulation of personal information and to strengthen the legislation on personal information in public law such as administrative law and criminal law.

3.2. The Principle of Informed Consent for Personal Information is Difficult to Fully Implement

Currently, the application of the principle of informed consent is mainly concentrated in the Personal Information Protection Law. The Personal Information Protection Law provides graded and classified protection for personal information, on the basis of which the application of informed consent is distinguished. According to the Law, in general, the processing of personal information shall comply with the principle of informed consent, and the personal information processor shall fulfill the obligation to inform the individual before processing, and the personal information processor shall not use the personal information until the individual is fully informed and the individual's consent is obtained; however, there are also exceptions, and if the personal information processor falls into one of the circumstances in Article 13(2) to (7) of the Law, the personal information processor shall only fulfill the obligation to inform the individual without obtaining the individual's consent. In addition, sensitive personal

information, because it is closely related to the personal and property interests of individuals, is different from general information and is subject to strict informed consent.

It can be seen that the application of the informed consent rule in the Personal Information Protection Law has largely protected the rights and interests of personal information, but there are still many obstacles in the specific application in practice. Specifically, first, information processing activities are becoming more and more complex. Along with the development of the big data industry, the processing of information often involves the collection, storage, use, processing, transmission, provision of personal information and other links, the application of the principle of informed consent has become more difficult, and the application of informed consent in each link will also affect the normal use of personal information. Second, personal information processing activities have become more virtual and hidden. The subject of personal information processing often begins to use personal information without obtaining the true intention of the individual, and the individual has no way to know about the infringement of personal information. Third, the amount of personal information is huge, and there are many different kinds of personal information. If all personal information is required to apply the principle of informed consent, it will affect the normal use of personal information and is not conducive to the realization of the data rights of personal information processors, mainly in the following ways: Internet enterprises and network operation platforms may have to invest more labor costs and material strength, and operators are less motivated to innovate in the industry; the difficulty of government supervision increases, which is not conducive to the optimization of the level of government supervision; enterprises The level of service of enterprises, government and other subjects is affected, and it is difficult to improve people's sense of well-being and access.

Therefore, following the current principle of informed consent does not really achieve the protection of personal information, and at the same time the normal use of personal information will be restricted, so it is necessary to put certain restrictions on the application of the principle of informed consent.

3.3. Inadequate Monitoring Mechanism for Personal Information

At present, the administrative supervision of personal information, the internal supervision of enterprises, the supervision of industry associations and the supervision of public opinion are inadequate. First, administrative supervision is limited. As mentioned earlier, the information protection department of government agencies has not been clearly defined, and the government not only undertakes the responsibility of personal information protection, but also is the subject of personal information collection and utilization, so it is inevitable that some staff members will abuse their power to violate the personal information of citizens. Secondly, the internal supervision of enterprises is not strong enough. There are inevitably some people among the staff of enterprises who are not highly professional, and they may negligently disclose or intentionally abuse personal information when collecting and utilizing personal information; coupled with the fact that enterprises have not set up special data supervision institutions or have set up but are not sound, resulting in serious problems of personal information infringement. Third, industry associations do not have adequate supervision of personal information processors. In practice, the supervision and management provisions of the industry autonomy code for personal information utilization behavior need to be improved, and the personal information utilization behavior lacks the regulation of industry self-regulatory organizations. Fourth, the supervision of public opinion needs to be strengthened. On the one hand, personal information subjects' own awareness of information protection is lacking; on the other hand, the personal information protection department is unknown, and it is difficult to realize the right of social subjects to complain and report against personal information infringement chaos.

3.4. Inadequate Remedies for Personal Information Infringement

For a long time, in order to resolve disputes over personal information infringement, personal information is usually included in the adjustment of intellectual property rights, copyright, competition law, privacy rights and claims, but it is ultimately an indirect protection of personal information and cannot truly achieve a balance between the protection and utilization of personal information; and the promulgation and implementation of the Personal Information Protection Law provides legal compliance for the realization of direct protection of personal information and further clarifies that individuals The promulgation and implementation of the Personal Information Protection Law provides legal guidelines for the direct protection of personal information, and further clarifies the right of individuals to safeguard the rights and interests of personal information through civil judicial channels.

However, for the infringement of personal information, the Personal Information Protection Law only provides that the right subject can file a private lawsuit or civil public interest litigation, but in practice, there are indeed personal information protection departments illegally handle personal information or do not perform the supervision of personal information, then whether individuals can use the administrative remedy of administrative litigation or administrative reconsideration to achieve the purpose of protecting personal information, the law has not been clarified. The law has not yet been clarified. It can be seen that the remedy for personal information infringement is relatively single, and civil remedies alone are not sufficient to resolve personal information infringement disputes.

4. Extraterritorial Legislative Experience of Personal Information Protection

In the context of big data, the issue of personal information legislation has received widespread attention globally, especially in developed countries or regions such as the European Union and the United States, which have considerable experience in personal information legislation, mainly in the form of unified legislation in the European Union to implement strict protection of personal information, which has promulgated legal norms such as the Charter of Fundamental Rights of the European Union, the Personal Data Protection Directive and the General Data Protection Regulation. Compared with the EU, the US mainly adopts a decentralized legislative model, among which the more famous laws include the Privacy Act, the California Privacy Act and the Children's Online Privacy Protection Act.[9] Accordingly, this part focuses on a comparative analysis of the legislation of the EU and the US in terms of the path of personal information protection, the application of the principle of informed consent and the supervision of personal information, in order to seek ways and means suitable for solving the problem of personal information in China.

In terms of the path of personal information protection, the EU and the US both adopt a combination of public and private law paths to protect personal information, while differing in the specific application. The EU has long attached great importance to human rights and insisted on the strict protection of personal information, and set personal information as a fundamental right through its charter, and strictly stipulated the rights enjoyed by personal data subjects and the administrative responsibilities of personal information regulators in the General Data Protection Regulation to realize the protection in public law.[10] In addition, when personal information infringement involves privacy content, it is clear that individuals have the right to seek private remedies. In contrast, the United States has always adhered to the concept of prioritizing economic development and preferring the use of personal information, although its protection mechanism for personal information is also more robust. It mainly includes personal information into the scope of privacy protection to achieve private law protection, and also helps to protect personal information through industry self-regulation and

market regulation; while in the public law remedy of personal information is mainly achieved through competition law, in addition, it also determines that government agencies are responsible for the supervision of personal information. In conclusion, the protection path of personal information in Europe and the United States is diversified, which is enlightening to the relevant legislation in China.

The application of the principle of informed consent is reflected in the personal information legislation of both the EU and the US, but there are differences in the degree of application. As mentioned earlier, the EU attaches great importance to the protection of individual rights and interests, and therefore, in the processing of personal information, the EU law requires the relevant subjects to fulfill the obligation to inform and strictly comply with the principle of informed consent; at the same time, in order to implement informed consent, the legislation also provides the rights related to the principle of informed consent for the subjects of personal information. In contrast, the U.S. applies informed consent mainly by specifying in its legislation the "right to withdraw consent" or "right to opt out" for the subject of personal information.[11] As mentioned above, the U.S. prefers the use of personal information, and accordingly, the U.S. values the commercial value of personal information, and its application of the principle of informed consent to personal information in practice is more flexible, which is very beneficial to the development of the data industry.

On the supervision of personal information, the EU and the US generally advocate the establishment of a comprehensive personal information supervision mechanism. Specifically, the EU has legislated a strict responsibility for personal information supervision by administrative subjects, and "regulation increases the cost of collecting consumer data".[12] In order to strengthen the protection of personal information, the EU has also set up a special personal information regulator, that is, "a special criminal justice agency to regulate the collection and use of data and set up a special data protection framework".[13] In contrast, "the U.S. is not just a criminal court. In contrast, "the U.S. relies not only on legal regulation, but also on a system of industry self-regulation, built from recommended industry guidelines, online privacy certification programs, and technology protection and safe harbor agreements." [14]

There are significant differences between the EU and the U.S. when it comes to post-facto remedies for personal information. First, in the EU, "under the GDPR, data controllers who fail to comply with their data breach notification obligations are subject to fines of up to €10 million or 2% of their global annual turnover." [15] Second, the difference in the way the U.S. deals with personal information breach is that many U.S. states have enacted special data breach notification laws, and "some states provide that individuals may sue the subject responsible for the damage caused by the failure to comply with the notification obligation or directly against the breaching party for damages under the state's consumer protection laws." [16] Accordingly, personal information infringement disputes in the United States are generally resolved through civil litigation.

In summary, the EU and the United States have similarities in the concept of personal information legislation, but due to the different national conditions of each country, there are major differences in the specific legal provisions. Therefore, when our legislation draws on the beneficial results of these countries or regions, we need to solve the problem of personal information protection by combining our practical experience .

5. Improvement of Personal Information Protection in China Path

5.1. Sound Parallel Model of Private Law Protection and Public Law Protection of Personal Information

In terms of administrative law protection of personal information, first of all, the legislation needs to clarify which departments the "relevant departments" refer to, and on this basis, the

division of powers and responsibilities within the department should be clarified to prevent unclear authority and mutual shirking of responsibilities; and the obligation of confidentiality should be added to the supervisory department, when the relevant organization or individual's complaint or report on Personal information infringement to the supervisory authority complaints, reports, the relevant departments must promptly complain about the identity of the complainant or whistleblower and other private information confidential, to prevent their legitimate rights and interests are infringed. Secondly, the establishment of a benchmark system for the discretionary power of administrative penalties for personal information should be accelerated so that the discretionary power of judges can be controlled within a reasonable range. Finally, it is recommended to introduce administrative reconsideration and administrative litigation, so as to achieve the purpose of preventing administrative inaction of government agencies as the main body of personal information protection and regulating the illegal use of personal information by the government as the processor of information.

In terms of the criminal law protection of personal information, since China's Criminal Law sets fewer crimes against personal information, which is not conducive to combating crimes and safeguarding human rights, it is necessary to "create new data crime crimes by adding new crimes"[17] To strengthen the protection of personal information. In addition, it is also necessary to "establish an independent information supervisory body for criminal proceedings" to strengthen the supervision of personal information in criminal law.[18] In addition, it is necessary to "establish an independent criminal lawsuit information regulator" to strengthen the responsibility of regulating personal information in the field of criminal law. In conclusion, we insist on constructing a personal information protection system with the synergy of public and private laws, which can balance the interests of information processors and information subjects more effectively.

5.2. Moderate Relaxation of the Application of the Principle of Informed Consent

First, informed consent is strictly applied to sensitive personal information. As mentioned above, sensitive personal information is closely related to the personal and property rights and interests of individuals, and as long as the processing of personal information involves the scope of sensitive personal information as stipulated in the Personal Information Law, the subject of the information processing must comply with the principle of informed consent. Second, the application of informed consent is relaxed for general personal information. Compared with sensitive personal information, the collection and use of general personal information usually has less impact on the privacy, life and property security of individuals, and is also conducive to operators providing better personalized services to individuals, thereby promoting the innovation and development of the digital industry. Therefore, the general personal information processing activities can be utilized without the consent of the individual after the information processing subject fulfills the obligation to inform. Of course, if a citizen's moral or property interests or other interests suffer as a result, he or she still has the right to seek public or private remedies. In short, the principle of informed consent can be applied in an adapted manner to better meet the development needs of modern society.

5.3. Establishment of a Comprehensive Personal Information Monitoring Mechanism

To regulate the information utilization behavior of personal information handlers, internal supervision and external supervision should be unified. First, the administrative internal supervision system must be continuously optimized. Specifically, efforts should be made to improve the supervision level of administrative supervisory departments and their staff on the basis of a clear personal information protection department, for which a group of high-tech talents needs to be actively cultivated; information protection departments should also

strengthen communication and collaboration with other departments to improve supervision efficiency; in addition, there is a need to "establish a data security risk assessment mechanism" [19]. In addition, there is a need to "establish a data security risk assessment mechanism. Second, improve the internal supervision system of enterprises. First, focus on cultivating the professionalism of internal personnel to prevent information misuse and reduce the risk of information leakage; second, establish and improve the standard of supervision by establishing a special information supervisory body within the enterprise. Third, strengthen the supervisory responsibility of industry associations. While safeguarding the interests of the industry, it should also improve the rules of industry autonomy for the protection of personal information and assist the government in regulating the market order. Fourth, strengthen the supervision of public opinion in multiple ways. First of all, the complaints and reporting department should be clarified from legislation, and a perfect personal information network supervision platform should be established to broaden the channels for citizens' complaints and reports. In addition, a reporting reward mechanism can be set up to improve the enthusiasm of social subjects to protect personal information. In short, administrative supervision, supervision of public opinion, supervision of industry associations, internal supervision of enterprises and supervision of public opinion should be carried out throughout the process of personal information protection.

5.4. Establishment of a Diversified Personal Information Infringement Remedy Mechanism

Firstly, it is suggested that the personal information legislation should be improved in the future by adding administrative remedies of administrative reconsideration and administrative litigation, in order to deal with the situation where administrative subjects collect and use personal information illegally or refuse to fulfill their personal information protection duties; secondly, it is suggested that judicial remedies and private remedies for personal information infringement should be coordinated and developed. Since personal information is characterized by a wide variety and huge quantity, there are numerous cases of infringement disputes related to the continuous circulation and sharing of personal information. Relying on judicial remedies alone not only increases the workload of the court, but also is not conducive to saving judicial costs, and the trial period of the court is generally long, and the damages suffered by the subject of personal information cannot be compensated in a timely manner. Accordingly, judicial remedies should be the main means of personal information infringement disputes, supplemented by private remedies such as negotiation, regulation and arbitration, so as to make up for the inadequacy of the current personal information infringement remedy mechanism.

6. Conclusion

In the era of big data, the economic benefits of personal information are becoming more and more important. The use of personal information has created valuable wealth for individuals and market players, but at the same time, the security risk of personal information is increasing day by day. Although there has been a great breakthrough in how to achieve a balance between the protection of personal information and the use of China's legislation, but still needs to be improved and perfected. 2021, September 14, the General Office of the CPC Central Committee, the General Office of the State Council issued the "Opinions on Strengthening the Construction of Network Civilization" pointed out that "to strengthen the protection of personal information law, data security law implementation "Accordingly, the practice needs to actively seek solutions to improve the protection of personal information in terms of the protection path of personal information, the application of the principle of informed consent, supervision and management, as well as infringement remedies, and to protect the vital interests of citizens in

conjunction with the Personal Information Protection Law, while promoting the scientific development of China's digital economy.

References

- [1] Wang Xiaoniu, Deng Shunyi, Li Mengying, Chen Renjie: Research on China's personal information rights-based protection system in the era of big data - based on the background of government data integration (Information Security Research, China 2020), p.1088-1100.
- [2] Deng YJ. Research on the balance between big data investigation and personal privacy protection (Journal of Guangxi Police Academy, China 2020), p.58-63.
- [3] Cheng Xiao. On the rights of personal data in the era of big data (China Social Science, China 2018), p.102-122+207-208.
- [4] Tian Gang. Reasonable Boundaries of the Expansion of Criminal Law Protection for Data Security (Law Forum, China 2021), p.66-75.
- [5] Cheng Xiao. On the rights of personal data in the era of big data (China Social Science, China 2018), p.102-122+207-208.
- [6] Zhu Yang, Li Xintian. An analytical framework for personal data privacy security protection in the era of big data (Journal of Intelligence, China 2021), p.165-170.
- [7] Shi Mingtao. The dilemma and the way out of personal information protection in the era of big data - a review and reflection based on the current research status (Technology and Law, China 2020), p.66-74.
- [8] Wang Liming. On the legal protection of the right to personal information - centering on the boundary between the right to personal information and the right to privacy (China Prosecutor, China 2013), p. 76.
- [9] Gao Rongwei. Foreign personal information protection mechanism (Journal of Property Rights, China 2020), p.15-17.
- [10] Yang Fan, Liu Ye. The "public-private parallel" path of personal information protection: China's legal practice and European and American inspiration (Journal of International Economic Law, China 2021), p.48-70.
- [11] Wan Fang. Consent" and "withdrawal of consent" in personal information processing (China Law, China 2021), p.167-188.
- [12] Sun Y, Luo W. Lin. From the protection of personal data to the maintenance of the personality rights of data subjects--and a review of the implementation of the Regulations on the Protection of Personal Information Network of Children (E-Government, China 2020), p.52-58.
- [13] Cheng Wenwen. Reconsideration of personal data protection in the era of big data: A perspective of industrial development (Journal of Fuyang Normal University (Social Science Edition), China 2020), p.107-111.
- [14] Cheng Wenwen. Reconsideration of personal data protection in the era of big data - from the perspective of industrial development (Journal of Fuyang Normal University (Social Science Edition), China 2020), p.107-111.
- [15] Fang Yu. Personal information protection under the evolution of data value: rethinking and reconstructing (Economic and Trade Law Review, China 2020), p.95-110.
- [16] Fang Yu. Personal information protection under the evolution of data value: rethinking and reconstructing (Economic and Trade Law Review, China 2020), p.95-110.
- [17] Tian Gang. Reasonable Boundaries of the Expansion of Criminal Law Protection for Data Security (Law Forum, China 2021), p.66-75.
- [18] Zheng Xi. An Outline of the Protection of Personal Information in Criminal Proceedings (Contemporary Jurisprudence, China 2021), p.115-124.
- [19] Ma Haiqun, Zhang Tao. Interpreting the construction of China's data security protection system from the Data Security Law (Draft) (Digital Library Forum, China 2020), p.44-51.