ISSN: 2710-0170

Exploring the Path of Administrative Law and the Protection of Personal Information in the Era of Big Data.

Donghui Zhuo

Anhui University of Finance and Economics, Bengbu 233030, China

Abstract

In the era of big data, the value of personal information is becoming increasingly prominent, and the security threats it faces are becoming more and more severe. This paper focuses on the administrative law protection path of personal information, and through the analysis of the characteristics of personal information in the era of big data, the current situation and existing problems of administrative law protection, and proposes a specific path to improve the protection of personal information administrative law in China, aiming to build a more complete and effective personal information protection system, balance the relationship between personal information protection and data utilization, and protect the information rights and interests of citizens and the public interest of society.

Keywords

The era of big data; Personal Information; Administrative Law Protection; Path exploration.

1. Introduction：Background and significance of the research

1.1. Background of the research

1.1.1. Opportunities and Challenges for Personal Information in the Age of Big Data

With the rapid development of information technology, especially the wide application of big data technology in various fields, human society has stepped into the era of big data. Under the background of this era, personal information has shown explosive growth and unprecedented mobility. On the one hand, the collection, storage, analysis and utilization of personal information have brought many opportunities to the society. In the medical field, through the analysis of massive patients' medical records, genetic information and other data, it is possible to achieve precision medicine and improve the accuracy of disease diagnosis and treatment effect; in the financial field, with the help of big data technology to mine the user's consumption habits, credit records and other information, it is possible to more accurately assess the risk, provide personalized financial services for the user, and promote financial innovation and economic development. On the other hand, personal information faces serious security threats. Under the big data environment, the scope of collection of personal information is expanding, from traditional basic information such as name, age, and contact information to more sensitive and detailed information such as location information, browsing records, and social relationships, which, once leaked, will cause serious damage to personal rights and interests. In addition, the large-scale centralized storage and rapid dissemination of personal information also provides more possibilities for hacking and data leakage incidents, such as the frequent data leakage incidents of large enterprises and government agencies in recent years, which involved hundreds of millions of users' information and triggered widespread public concern about personal information security.

ISSN: 2710-0170

1.2. Importance and necessity of administrative law to protect personal information

In the face of the growing problem of personal information security, legal protection has become a key line of defense. Among the many branches of law, administrative law has a unique and important position and role in the protection of personal information.

1.2.1. Administrative law can provide preventive protection

By formulating and enforcing relevant regulations, standards and supervisory measures, administrative authorities can regulate and constrain the collection, processing and use of personal information in advance, so as to prevent the risk of abuse and leakage of personal information at the source. Existing administrative laws require enterprises to follow the principles of lawfulness, legitimacy and necessity when collecting personal information, and to clearly inform users of the purpose, manner, scope and storage period of the information collected, so as to avoid the excessive collection and unlawful use of personal information by enterprises.

1.2.2. Administrative law has a strong executive and supervisory character

With professional law enforcement teams and abundant law enforcement resources, administrative authorities are able to effectively supervise and inspect the protection of personal information, promptly discover and stop illegal acts, and impose administrative penalties on violators, thus creating a strong deterrent. Compared with civil law, which mainly relies on the parties to defend their rights through litigation after the fact, the active enforcement of administrative law can respond more quickly to personal information security incidents, protect the rights and interests of more people, and reduce the cost of individual rights defense and the risk of information security of the society as a whole.

1.2.3. Administrative law plays an important role in safeguarding the public interest

Personal information not only involves the privacy and rights of individuals, but is also closely related to social public interests. Government departments need to collect and use a large amount of personal information in the course of public affairs, such as public health management, social security maintenance and macroeconomic regulation. Administrative law can ensure that the government's handling of personal information meets the needs of the public interest, while preventing the government from abusing its power to infringe on the rights and interests of personal information, and realizing the balance between individual rights and interests and the public interest.

2. Characteristics and Value of Personal Information in the Age of Big Data

2.1. Characteristics of Personal Information in the Age of Big Data

2.1.1. Large volume and wide range of data sources

In the era of big data, the amount of personal information has exploded. This is mainly attributed to the popularization and application of information technology, which enables all kinds of behaviors in people's daily life and work to be digitally recorded and stored. From social platforms, e-commerce platforms, and search engines on the Internet to offline financial institutions, medical institutions, transportation hubs, and surveillance equipment in public places, every scenario is continuously generating massive amounts of personal information data. For example, the world-renowned social platform Facebook has billions of users, and every time each user likes, comments, shares, posts news and other behaviors on the platform, one or more data records will be generated, and these data converge to form an extremely large personal information data set.

ISSN: 2710-0170

The sources of personal information have also become more extensive than ever. In addition to traditional government departments, financial institutions, medical institutions and other organizations that hold large amounts of personal information, various emerging Internet companies, mobile application developers, and IoT device manufacturers have all become collectors of personal information. For example, an ordinary cell phone application may collect a variety of personal information such as a user's location information, address book information, call logs, text message content, browsing history, etc., during the use of the application; smart home devices, such as smart speakers, smart cameras, smart bracelets, etc., are able to collect users' voice commands, habits, health data, home environment information, etc., and personal information collected by these devices is transmitted and stored on cloud servers through the The personal information collected by these devices is transmitted over the network and stored on cloud servers, further enriching the data sources of personal information.

2.1.2. Variety of data types and complex structures

Personal information in the era of big data is no longer limited to traditional structured data, such as information stored in the form of tables in databases, but also includes a large amount of unstructured and semi-structured data. Structured data such as an individual's name, age, and contact information can be conveniently stored in relational databases and efficiently queried and analyzed through Structured Query Language (SQL). However, unstructured data such as images, videos, audios, and textual comments posted by individuals on social media, as well as email content and electronic documents do not follow a fixed structural pattern in terms of format and content, and are difficult to be processed using traditional database techniques. Semi-structured data, on the other hand, is between structured and unstructured, such as data in HTML or XML format in web pages, which has a certain markup structure but does not strictly follow a fixed table structure like relational databases.

These different types of personal information data intertwine with each other to form a complex data structure. A complete personal information dataset may contain both structured personal identification information and financial transaction records, as well as unstructured traces of an individual's activities on social media (e.g., photos, videos, etc.) and semi-structured records of an individual's postings and replies on online forums. The diversity of such data types and the complexity of their structure pose higher technical requirements and challenges for the storage, management, analysis and protection of personal information.

2.1.3. Highly dynamic and real time data

In the big data environment, personal information is in a state of continuous updating and change, and is highly dynamic. Information about an individual's living conditions, interests, social relationships, consumption habits, etc., will continue to change over time, and accordingly, the personal information data reflecting these conditions needs to be updated in real time. A person's location information may change in a few minutes, his/her shopping preferences on e-commerce platforms may change at any time with the change of seasons, fashion trends, and personal needs, and the relationship and interaction frequency of friends on social media are also in the process of dynamic adjustment.

Meanwhile, with the development of Internet of Things (IoT) technology, many devices are able to collect personal information in real time and transmit it to data centers for analysis and processing, which makes the real-time characteristics of personal information more significant. For example, smart wearable devices can monitor the user's heart rate, blood pressure, exercise steps and other health data in real time, and immediately upload these data to the cloud server so that the user or medical institutions can understand their health status in real time; traffic management departments collect real-time information about the vehicle's driving speed, location, driver behavior and other information through the sensors and cameras on the road,

ISSN: 2710-0170

which is used for traffic flow monitoring and violation of the law. Real-time warning. This dynamic and real-time nature requires personal information processing and protection mechanisms that can respond to changes in the data in a timely manner, ensure the accuracy and timeliness of the data, and also guard against the risk of information leakage due to real-time updating of the data.

2.2. The Value of Personal Information in the Age of Big Data

2.2.1. Individual-level values

For individuals, personal information has a multifaceted and important value in the era of big data. Personal information is the basis for individuals to participate in social life and economic activities. In modern society, individuals need to provide personal information to various organisations and platforms in order to obtain corresponding services and rights. In banking, individuals need to provide their identity and financial information to open bank accounts, apply for loans, and enjoy financial services; in using Internet platforms, the provision of personal information enables users to create personalised accounts, customise their browsing experience, and access content and services of interest, such as friend interaction on social media and course recommendations on online learning platforms.

At the same time, individuals can collect and analyse their personal information such as health information, study records, work performance data, etc. Individuals can better understand their own physical condition, knowledge level and ability strengths, so that they can make health plans, study plans and career development plans in a targeted manner. To a certain extent, personal information reflects an individual's social identity and image, and is of great significance to an individual's social and interpersonal relationships. Information such as hobbies, life photos and career achievements displayed by individuals on social media help to shape their image in social networks, attract like-minded friends, expand social circles, and enhance social interactions and interactions, thus satisfying individuals' social and emotional communication needs.

2.2.2. Value at the business level

In the business field, personal information has become an important production factor and competitive resource for enterprises, with great economic value. By collecting, analysing and utilising personal information, enterprises can gain a deeper understanding of consumers' needs, preferences and behavioural patterns, so as to achieve precision marketing and personalised services, and improve market competitiveness and economic benefits.

On the one hand, enterprises use personal information for market segmentation and target customer positioning. By analysing consumers' demographic information, consumer behaviour data, interest and hobby data, etc., enterprises can divide the huge market into segments with different characteristics and needs, and pinpoint their target customer groups. In daily life, cosmetic companies can segment the market into different cosmetic consumer groups based on information such as consumers' age, gender, skin texture, and purchasing history, develop and promote suitable products for each group's characteristics, and improve marketing effectiveness and product sales.

On the other hand, enterprises carry out personalised marketing and recommendation services based on personal information. Based on consumers‘ personal information and behavioural data, companies can tailor personalised advertisements, promotions and product recommendations to increase consumers’ purchase intention and loyalty. E-commerce platforms analyse users‘ browsing history, purchasing records and favourite information to recommend products that meet their interests and purchasing needs, and such personalised recommendations can not only improve users’ shopping experience, but also increase the platform's sales and user stickiness.

ISSN: 2710-0170

At the same time, personal information can also help companies optimise product design and service processes. Enterprises through the collection of user feedback on the use of products, evaluation information and customer service interaction records and other personal information, to understand the user in the process of product use problems and needs, so as to improve product design, optimise the service process in a timely manner, improve product quality and service level, and enhance the competitiveness of enterprises in the market.

3. Current situation and problems of administrative law protection of personal information in China

3.1. Status of administrative law protection of personal information

3.1.1. Administrative regulatory bodies and their responsibilities

At present, China's administrative and regulatory agencies involved in personal information protection show a diversified pattern. The Ministry of Industry and Information Technology (MIIT), as the competent authority of the information industry, has assumed important responsibilities in personal information protection, and is responsible for supervising and overseeing the collection, use, storage, and transmission of personal information by telecommunication business operators, Internet information service providers, and other subjects, supervising the implementation of personal information protection measures by enterprises through the formulation of relevant industry norms and technical standards, and interviewing enterprises in violation of the regulations, order rectification and administrative penalties for enterprises violating the regulations, etc., so as to maintain the order of personal information security in the telecommunication and Internet industries.

For its part, the State Internet Information Office is mainly responsible for coordinating cyberspace security and related supervisory and management work, and supervising the protection of personal information on online platforms, including reviewing whether the privacy policies of online platforms are compliant, supervising whether the platforms are guilty of over-collection of personal information, illegal trading of personal information and other violations of the law, and taking action in accordance with law against illegal online platforms by issuing warnings, imposing fines, suspending related businesses, suspending business rectification, shutting down websites, etc. , suspension and rectification, closure of websites and other punitive measures to strengthen the protection of personal information in cyberspace and create a safe, healthy and orderly online environment. In addition, the market supervision and administration authorities also play a role in the protection of personal information, especially in commercial activities involving the protection of consumers'personal information, and are responsible for supervising whether enterprises follow the principles of fair, just and lawful market competition, investigating and dealing with unfair competition and infringement of consumers'rights and interests in the process of collection and use of consumers'personal information, and safeguarding consumers'Personal information rights and interests are effectively protected in market trading activities through the maintenance of market order.

3.1.2. Administrative licensing and filing systems for information collection and processing

In a number of specific areas, China has implemented administrative licensing and filing systems for the collection and processing of personal information in order to strengthen the control of personal information at the source. In the credit-collection industry, the establishment of a credit-collection agency requires a licence from the People's Bank of China, and credit-collection agencies are required to operate in strict accordance with the relevant regulations in the course of collecting, collating, preserving and processing personal credit information, and to file with the People's Bank of China information on their business activities

ISSN: 2710-0170

and measures for the protection of personal information. Through this administrative licensing and filing system, it is ensured that credit bureaus have the appropriate qualifications and capabilities to protect the security and lawful use of personal credit information, prevent the leakage or abuse of personal credit information due to the misconduct of credit bureaus, and safeguard the stability of the financial credit system and the credit rights and interests of individuals.

In some big data application projects involving sensitive personal information, it may also be necessary to file a record with the relevant competent authorities, stating the purpose, manner, scope and security measures of the information collection of the project, so as to enable the competent authorities to supervise and review the personal information processing activities of the project to ensure that the project is carried out within the framework of lawfulness and compliance, to avoid the security of personal information triggered by the rapid development of the big data application risk, and safeguard the reasonable use and safe protection of citizens' personal information in the era of big data.

3.1.3. Administrative supervisiont and enforcement mechanisms

Administrative organs conduct on-site verification and assessment of the protection of personal information of various subjects through regular or irregular supervision and inspection. For example, the Ministry of Industry and Information Technology (MIIT) organises special inspection campaigns on personal information protection for telecommunication and Internet enterprises, which include the construction of the enterprises' personal information management systems, the implementation of technical measures for information security protection, and compliance with the collection and use of user information. During the inspection process, law enforcement officers test the information security protection capability of enterprises in the field by reviewing their relevant documents and information, technical system records, user agreements, etc., and put forward timely rectification requirements for problems found, and follow up on the rectification situation, so as to ensure that the enterprises effectively fulfil their obligations for the protection of personal information.

The State Internet Information Office will also obtain clues through network monitoring, user reports and other channels, and conduct investigations, evidence collection and law enforcement on online platforms suspected of violating personal information. Once it is verified that an online platform has violated the laws and regulations on personal information protection, severe penalties will be taken in accordance with the law, including imposing high fines on the platform, ordering the suspension of the relevant business, and revoking the relevant licences, etc., and the directly responsible supervisory personnel and other directly responsible personnel will also be punished in accordance with the law, so as to form a strong deterrent to the infringement of personal information through the rigorous law enforcement mechanism, and to urge the online platforms Through the strict enforcement mechanism, a strong deterrent against the infringement of personal information will be formed, and online platforms and other types of subjects will be urged to consciously comply with the provisions of personal information protection, and safeguard the rights and interests of citizens' personal information and the rule of law in cyberspace.

3.2. Problems in the administrative law protection of personal information

3.2.1. Insufficient systematisation and coordination of laws and regulations

Although China has introduced numerous laws and regulations relating to the protection of personal information, there is a lack of systematicity and coordination among these laws and regulations. Horizontally, there are differences in the definition, scope of protection, rights and obligations of personal information between different sectoral laws, leading to possible conflicts and uncertainties in the application of the law in the process of actual application. Provisions on the rights of personal information in the civil law and provisions on the

ISSN: 2710-0170

supervision of personal information in the administrative law fail to form an effective connection, which makes it possible to deal with some disputes on the protection of personal information in such a way that there is a lack of co-ordination between the civil remedies and the means of administrative supervision, which affects the comprehensive protection of the rights and interests of personal information.

Vertically, the hierarchical relationship between higher and lower laws is not clear enough, and some of the lower laws fail to fully implement the legislative spirit and principles of the higher laws in the process of enactment, and there are even inconsistencies with the higher laws. At the same time, there is also a lack of effective coordination and integration between some special laws and regulations, with duplicative provisions and regulatory gaps co-existing, making it possible for administrative agencies to face problems such as unclear bases and responsibilities in the course of law enforcement, and reducing the overall effectiveness of the administrative law on the protection of personal information.

3.2.2. Unreasonable set-up and configuration of powers of administrative regulatory bodies

Currently, the administrative regulatory bodies for personal information protection in China are decentralised, with several departments having certain regulatory responsibilities, but this decentralised regulatory model has led to the problem of cross-powers and fragmentation. There is some overlap in the scope of responsibilities between different regulators, which is prone to duplication of regulation, increasing compliance costs for enterprises and wasting administrative resources. In terms of personal information protection on Internet platforms, the Ministry of Industry and Information Technology, the State Internet Information Office, and the Market Supervision and Administration Department all have the authority to regulate, but the regulatory focus and approach of each department is different, and there is a lack of effective coordination mechanism, which leads to enterprises being at a loss when facing the regulatory requirements of different departments, and also causes some personal information protection issues to be shifted around between departments without being resolved in a timely and effective manner. The lack of an effective coordination mechanism has led to the confusion of enterprises when facing the regulatory requirements of different departments.

At the same time, some administrative and supervisory agencies have relatively weak powers and lack sufficient enforcement powers and resources to effectively respond to the complex and changing situation of personal information protection. Some grassroots supervisory departments have deficiencies in staffing, technical equipment, and law enforcement capabilities, making it difficult to conduct comprehensive and in-depth supervision, inspection, and law enforcement of personal information protection under their jurisdiction, resulting in loopholes in the supervision of personal information protection in some areas, and failing to create an effective deterrent to personal information infringement, which affects the actual effectiveness of the protection of personal information under the Administrative Law.

3.2.3. Personal information protection standards are unclear and unworkable

Although existing laws and regulations put forward some principled requirements for the protection of personal information, there is a lack of clarity and detail in the specific protection standards, and a lack of operability. As for the ‘security protection measures’ for personal information, the laws and regulations only generally require information processors to take necessary technical and management measures, but do not make detailed provisions on the specific content, technical indicators, and implementation steps of these measures, which makes it difficult for enterprises to judge whether their own personal information protection measures comply with the legal requirements due to the lack of clear guidance in the actual implementation process. Personal information protection measures comply with legal requirements.

ISSN: 2710-0170

There are also ambiguous standards regarding the specific rules for the collection, use, storage and sharing of personal information. There is a lack of clear criteria for defining the 'necessary scope' of personal information in different industries and scenarios, leading to the possibility of over-collection of personal information by enterprises; there is also a lack of clear regulations on the conditions and procedures for the sharing of personal information among different subjects, which can easily lead to security risks in the process of sharing personal information. The lack of clear and explicit regulations on the conditions and procedures for sharing personal information among different subjects may easily lead to security risks in the process of sharing personal information.

4. Improvement Path of Administrative Law Protection of Personal Information in the Era of Big Data

4.1. Improvement of the administrative law protection system for personal information

4.1.1. Development of a unified personal information protection law

The formulation of a unified law on the protection of personal information is a key step towards improving the administrative law protection system for personal information in China. It should integrate the existing personal information protection provisions scattered in various laws and regulations, clarify the basic principles, basic systems and basic norms of personal information protection, and construct a comprehensive, systematic and coordinated personal information protection framework.

A unified personal information protection law should establish a sound classification and grading system for personal information, classify personal information into different categories and levels according to its sensitivity, importance and impact on the rights and interests of individuals, and establish corresponding protection measures and regulatory requirements for different categories and levels of personal information. For highly sensitive personal information, such as biometric information, medical and health information, financial account information, etc., stricter restrictions on collection, storage, use and sharing should be implemented, and information processors should be required to adopt higher-standard safety and protection technical measures, and strict approval and supervision should be carried out in all aspects of information processing.

At the same time, the system of rights of personal information subjects should be improved. In addition to the existing rights to know, decide, consult, copy, correct, delete, etc., consideration should also be given to granting personal information subjects a certain amount of income rights, that is, in the case of personal information being legally used commercially and generating income, personal information subjects have the right to obtain reasonable economic returns, so as to better balance the relationship between the protection of personal information and the development of the data industry. In addition, the unified personal information protection law should also consider granting the subject of personal information the right to income.

In addition, a unified personal information protection law should also clearly stipulate the obligations and responsibilities of information processors, including the establishment of an internal personal information management system, the designation of a person responsible for personal information protection, regular information security risk assessment and auditing, and timely response to requests for the rights of the subject of personal information, etc., as well as the setting up of severe administrative penalties for violation of the law by the information processors, including hefty fines, ordering suspension and rectification, revocation of relevant business licences, etc., and, in serious cases, pursuing criminal liability in accordance

ISSN: 2710-0170

with the law, in order to enhance the deterrent effect of the law and ensure that information processors effectively fulfil their obligations to protect personal information.

4.1.2. Improve the supporting convergence of relevant laws and regulations

On the basis of the formulation of a unified law on the protection of personal information, it is also necessary to further improve the supporting articulation of relevant laws and regulations, so as to form an organic and coordinated legal network for the protection of personal information.

Firstly, the coordination and articulation between the personal information protection law and other sectoral laws should be strengthened. In the field of civil law, the criteria for determining civil liability and the scope of compensation for infringement of personal information should be further refined, and the status and protection of personal information rights and interests in the civil rights system should be clarified, so that personal information can be adequately compensated and relieved through civil legal means when it is infringed upon; in the field of criminal law, the constitutive elements of crimes of infringing on personal information and other related crimes should be adjusted and perfected in due course according to the actual needs of personal information protection and new changes of illegal behaviours. In terms of criminal law, in accordance with the actual needs of personal information protection and new changes in illegal behaviours, adjust and improve the constituent elements and penalties for crimes against citizens' personal information, increase the strength of the crackdown on serious crimes against personal information, and strengthen the role of the criminal law as a barrier to the protection of personal information. lawful behaviour, proper procedures and appropriate penalties in the process of law enforcement, so as to improve the level of the rule of law in the administrative law protection of personal information.

Secondly, each industry shall, in accordance with the requirements of the unified personal information protection law, formulate corresponding industry implementation rules and norms, so as to concretely implement the principles and requirements of personal information protection into the business processes and operational practices of each industry. The financial industry should formulate personal information protection implementation rules for financial institutions to clarify the personal information protection duties and operation norms of financial institutions in various aspects such as customer information collection, credit business processing, financial product marketing, customer credit rating, etc., and strengthen the protection of personal information in the financial sector; the medical industry should introduce special regulations on the protection of medical data and personal health information to regulate medical institutions, medical research institutions, medical information platforms and other subjects in the process of collection, storage, transmission, sharing and use of medical data, to safeguard the security of patients‘ personal health information; the Internet industry should further improve the self-regulatory norms and technical standards for the protection of personal information on Internet platforms, and supervise Internet enterprises to strengthen the protection of users’ information, prevent the leakage and misuse of users' information in the network environment, and create a safe, healthy and credible cyberspace.

4.2. Optimising administrative regulatory bodies and regulatory mechanisms

4.2.1. Integration and restructuring of administrative regulatory bodies

In view of the current situation of fragmented administrative and supervisory organisations for personal information protection in China and the intersection of their powers, it is necessary to integrate and reconstruct the administrative and supervisory organisations, and to set up a comprehensive administrative organisation for the protection of personal information that is authoritative and professional in nature. It should integrate the functions and resources of the Ministry of Industry and Information Technology, the State Internet Information Office, the Market Supervision and Administration Department and other relevant departments in the

ISSN: 2710-0170

protection of personal information, and be responsible for the planning and formulation of personal information protection, the formulation of standards, supervision and inspection, and law enforcement penalties, so as to avoid inefficiencies and gaps in supervision brought about by multiple supervisory authorities and unclear responsibilities.

The newly-established comprehensive personal information protection administrative organisation shall have independent law enforcement and decision-making powers, and be able to independently carry out supervision of all kinds of personal information-processing subjects without interference or influence from other departments, so as to ensure the impartiality and authority of the supervision work. At the same time, the agency should be equipped with professional law enforcement personnel and technical experts with rich legal knowledge, information technology knowledge and practical experience in personal information protection, so as to be able to effectively deal with the various complex technical and legal issues facing personal information protection in the era of big data, and to improve the professionalism and effectiveness of the regulatory work.

4.2.2. Clarify the terms of reference and coordination mechanisms of regulatory bodies

Clarifying the terms of reference of a comprehensive personal information protection administrative body is key to ensuring that it effectively fulfils its regulatory responsibilities. The agency should have a wide range of powers, including, but not limited to, formulating administrative rules, regulations and technical standards for personal information protection; managing the registration and filing of various types of personal information processors, and reviewing the compliance of their personal information protection systems and measures; carrying out day-to-day supervision and inspection and special law enforcement actions, and investigating, collecting evidence and imposing penalties for suspected violations of personal information protection regulations; accepting complaints and reports on personal information protection and handling them in a timely manner; and carrying out international cooperation and exchanges with personal information protection regulatory agencies in other countries and regions to deal with cross-border violations. protection complaints and reports, and timely handling and feedback; and international cooperation and exchange with personal information protection regulatory bodies in other countries and regions to jointly address cross-border personal information protection issues, etc.

In order to ensure co-ordination between different regulatory bodies, a sound co-ordination mechanism between personal information protection regulatory bodies should be established. For example, an inter-departmental personal information protection coordination committee should be set up, led by a comprehensive personal information protection administrative agency, with the participation of all relevant departments, to hold regular meetings to coordinate and resolve major issues and difficult cases in personal information protection supervision and to strengthen information sharing and communication and collaboration, so as to form a supervisory synergy.

4.2.3. Enhancing enforcement capacity-building for regulatory agencies

First of all, the training of law enforcement personnel should be increased, and training courses and business seminars on personal information protection laws and regulations, information technology and law enforcement procedures should be organised on a regular basis, so as to improve the legal literacy, professional skills and law enforcement level of law enforcement personnel. Through training, law enforcement officers should be familiar with the latest laws, regulations and policy requirements on personal information protection, master the basic principles and application scenarios of big data technology, understand the procedures and techniques of personal information protection law enforcement, and be able to skilfully use legal and technological means to carry out personal information protection law enforcement,

ISSN: 2710-0170

so as to effectively respond to the various complexities and challenges faced by personal information protection in the era of big data.

Secondly, the technical equipment construction of law enforcement agencies should be strengthened and equipped with advanced information technology equipment and tools, such as data monitoring and analysis software, electronic forensic equipment, network security detection equipment, etc., so as to improve the technical monitoring capacity and law enforcement forensic capacity of law enforcement agencies. A personal information protection supervision platform has been established using big data technology to achieve real-time monitoring, risk warning and data analysis of personal information processing activities, so that clues to personal information leakage, misuse and other violations of the law can be discovered in a timely manner, and the efficiency and precision of supervision can be improved.

Finally, a sound law enforcement supervision mechanism should also be established to strengthen internal and external supervision of the law enforcement behaviour of personal information protection administrative agencies. In terms of internal supervision, through the establishment of a law enforcement quality assessment system and a system of accountability for law enforcement errors, the law enforcement actions of law enforcement personnel are regulated to ensure that law enforcement is fair, lawful and standardised; in terms of external supervision, the supervisory roles of the general public, the media and industry associations are brought into full play by setting up a system of reporting and complaint handling and a system of disclosure of information to receive timely reports and supervisory oversight of the law enforcement of personal information protection by the public, and to disclose the results of law enforcement and typical cases to the public. In terms of external supervision, a system for reporting complaints and disclosure of information has been established to receive timely reports from the public on the enforcement of personal information protection, and to disclose the results of law enforcement and typical cases, and to accept the supervision and evaluation of the public, so as to enhance the transparency and credibility of law enforcement.

4.3. Clarification of administrative law standards and norms for the protection of personal information

4.3.1. Refinement of rules for the collection, storage, use and sharing of personal information

With regard to the collection of personal information, clear collection rules should be established, stipulating that information collectors must follow the principles of lawfulness, legitimacy and necessity, specify the purpose of collection, and fully inform the subject of the personal information of the purpose, manner, scope and storage period of the information to be collected before collection, and obtain the express consent of the subject of the personal information. At the same time, the scope of information collection should be limited to avoid over-collection of personal information that is not relevant to achieving the purpose of collection. For example, for an ordinary mobile phone application, the collection of personal information shall be limited to that which is necessary for the realisation of its basic functions, e.g. location information shall be collected only when the user uses location-related functions, and the user shall be clearly informed of the purpose and use of the collection and shall obtain the authorised consent of the user.

For the storage of personal information, strict storage security standards should be stipulated, including requiring information storers to take necessary technical measures, such as data encryption, access control, and backup and recovery, to ensure the confidentiality, integrity, and usability of personal information in the storage process. At the same time, the storage period should be clarified, stipulating that information storers should delete or destroy personal information in a timely manner after the storage period has been reached, unless

ISSN: 2710-0170

otherwise provided for by laws and regulations or authorised by the subject of the personal information.

With regard to the use of personal information, rules of use shall be formulated to limit the scope of use of personal information to ensure that personal information is used only for purposes consistent with the purposes for which it was collected, and that the purposes for which personal information is used shall not be altered without authorisation. In using personal information, information users shall take appropriate safety measures to prevent the leakage and misuse of personal information. For example, when using personal information for marketing purposes, companies shall ensure that the personal information used is legally collected and used within the scope of authorisation, and shall not sell or disclose personal information to third parties for other unauthorised commercial purposes.

Regarding the sharing of personal information, strict sharing rules shall be established. The conditions, scope and procedures for the sharing of personal information should be clearly stipulated, and information sharers should be required to review the legitimacy, security and necessity of the subject of sharing before sharing personal information, and to sign strict confidentiality agreements and data protection agreements with the subject of sharing to clarify the rights and obligations of both parties with respect to the protection of personal information. At the same time, it shall ensure that the subject of personal information has the right to know and the right to choose the sharing of his or her personal information, and the information sharer shall inform the subject of personal information of the circumstances of the sharing and obtain his or her consent prior to sharing personal information, unless otherwise provided for by laws and regulations.

4.3.2. Establishment of technical and managerial standards for the security and safety of personal information

In terms of technical standards, technical specifications for personal information security should be formulated, including technical standards for data encryption, identity authentication, access control and network security protection. For example, it is stipulated that when storing and transmitting personal information, enterprises must use encryption algorithms that comply with national standards for encrypting personal information, so as to ensure the security of personal information in the network environment; information systems are required to have reliable identity authentication mechanisms, such as the use of multifactor authentication methods, to prevent unlawful users from accessing the personal information system; and network security protection technical standards should be formulated to require enterprises to set up perfect network security protection facilities such as firewalls, intrusion detection systems, anti-virus systems, etc., to resist external network attacks and protect the safe and stable operation of personal information systems.

In terms of management standards, a sound personal information security management system should be established, including the formulation of a personal information security management system, operating procedures and emergency plans. Enterprises are required to set up special personal information security management positions and equip professional security management personnel, who are responsible for the organisation, implementation, supervision and inspection of personal information security management within the enterprise. At the same time, enterprises should regularly carry out personal information security risk assessment and auditing work, timely detection and rectification of personal information security risks, and ensure the effective implementation of the personal information security management system.

In addition, supervision, inspection and certification assessment of personal information security technology and management standards should be strengthened. Administrative and supervisory bodies should conduct regular inspections and assessments of

ISSN: 2710-0170

enterprises‘ personal information security technology and management measures, and order enterprises that do not meet the requirements of the standards to rectify them within a certain period of time; enterprises are encouraged to pass the certification and assessment of third-party certification bodies to prove that their personal information security safeguard capacity meets the requirements of the corresponding standards, so as to improve the level of enterprises’ personal information security management and their credibility in society.

5. Conclusion

This paper discusses the path of administrative law protection of personal information in the era of big data, through the analysis of the connotation, characteristics and value of personal information, sorting out the current situation of administrative law protection of personal information in China and pointing out its problems, and puts forward a series of improvement paths, aiming at building a more sound and effective personal information protection system, balancing the relationship between the protection of personal information and the use of data, and safeguarding the citizens' information rights and interests and the public interests of the society. The aim is to build a more sound and effective personal information protection system, balance the relationship between personal information protection and data utilisation, and safeguard the information rights and interests of citizens and the public interest of society. In terms of the characteristics and value of personal information, personal information in the era of big data has a large amount of data, wide range of sources, a variety of types, complex structure, and dynamic real-time characteristics, and has a non-negligible value for personal and commercial, which lays the foundation for the subsequent discussion of the necessity and importance of the protection of personal information.

Although the administrative law protection of personal information in China has formed a certain system of laws and regulations, established administrative regulatory bodies and their duties, implemented the administrative licensing and filing system for the collection and processing of information, and set up administrative supervision and inspection and law enforcement mechanisms, there are still insufficient systematic and coordinated laws and regulations, irrational setup and allocation of powers of the administrative regulatory bodies and unclear standards for the protection of personal information, and the lack of operational problems, which seriously affects the protection of personal information and its importance. However, there are still problems such as insufficient systematic and coordinated laws and regulations, irrational administrative supervisory organ setup and authority allocation, and unclear and lack of operational standards for personal information protection, etc., which seriously affect the actual effect of the protection of personal information by administrative law. In view of these problems, this study proposes a path of improvement. In the construction of the protection system, a unified personal information protection law should be enacted to clarify the basic principles, systems and norms, and to improve the coordination of relevant laws and regulations; optimise the administrative supervision institutions and mechanisms, integrate and restructure the supervision institutions, clarify their terms of reference and coordination mechanisms, and strengthen the construction of law enforcement capacity; clarify the standards and norms of administrative law for the protection of personal information, and to detail the rules of collection, storage, use and sharing, and to establish the technical and management standards of safety and security; and safety and security technology and management standards; strengthen the administrative relief mechanism, improve the administrative complaint and reconsideration system, and establish an administrative compensation system; promote social co-rule, strengthen industry self-regulation and enterprise self-regulation, encourage public participation and supervision, and promote public awareness of information security.

ISSN: 2710-0170

Through the above research, a relatively complete theoretical and practical framework for the protection of personal information under administrative law in the era of big data has been initially formed, which provides useful references and guidance for the improvement of China's personal information protection system, and helps to better safeguard the rights and interests of personal information while giving full play to the value of personal information, and to safeguard the public interests of the society and the healthy development of the digital economy.

References

[1] ZHU Hao. Comparative Law Study on Personal Information Protection, Hebei Enterprise,2024 No.9, p.158-160.

[2] Jin Song. Practical Review and Regulatory Path of Mobile APP Privacy Policy, Tianjin Law, Vol. 40 (2024) No. 3, p.77-85.

[3] Chen Kaipan. Study on the Protection of Consumers' Personal Information in the Context of Digital Economy, Journal of Xinjiang Open University, Vol. 28 (2024) No. 3, p.67-71.

[4] Lu Jun,Huang Chen. Reasonable limits and normative path of judicial disclosure of personal information in the era of big data, Journal of Shandong Judges Training Institute, Vol. 40 (2024) No. 4, p.11-25.

[5] Li Yu. Towards a doctrinal reconstruction of the offence of infringing citizens' personal information in the “risk” paradigm, Journal of Soochow University (Law Edition), Vol. 11 (2024) No. 3, p.86-99.

[6] Ruan Li. Dilemma and optimisation of legal protection of personal whereabouts information, Journal of Chongqing University of Technology (Social Science), Vol. 38 (2024) No. 8, p.146-160.

[7] Ren Fuxuan. Research on the legal protection of sensitive personal information, Journal of Tianshui Administrative College,Vol. 25 (2024) No. 6, p.94-97.

[8] Ping Yaguo. Research on personal information protection based on cyberspace security, Cyberspace Security, Vol. 15 (2024) No. 4, p.47-51.