ISSN: 2710-0170

Research on the legal framework of personal information privacy protection in automated administrative environment: centered on data security and rights balance

Zhongsen Zhang

College of Political Science and Law, University of Jinan, Jinan 250024, China

Abstract

In the digital age, with the increasing importance of personal information, especially in the field of automated administration, the protection of personal information is particularly urgent. Ensuring the security of personal information in automated administration not only helps to safeguard the realization of individual dignity rights and meet the inherent requirements of the principle of proportionality, but also regulates the use of algorithms to avoid discrimination. However, although the legislation on the protection of personal information in automated administration has made some progress, there are still some shortcomings: the legislation is not directly specified, the law is not operable, the supervision and management mechanism is not perfect; There are also problems at the law enforcement level: improper use of immunity in administrative procedures, excessive expansion of the scope of personal information processing; In the relief aspect, there are also challenges: the provisions of administrative public interest litigation are vague, and there are loopholes in the way of liability. In order to improve the protection mechanism of personal information in automated administration, it is necessary to expand the direct regulation of automated administration in legislation, enhance the operability of laws, and improve the supervision and management mechanism of personal information. At the same time, it is also necessary to amend the administrative due process and strictly implement the principle of least necessity at the level of law enforcement. In terms of relief, the applicable rules of administrative public interest litigation should be clarified, and more targeted ways of assigning blame should be established.

Keywords

Automated administration, Personal information protection, Personal information in automated administration, Informed consent rules, Principle of least necessity.

1. Introduction

In recent years, with the vigorous development of digital information technology, government activities are moving towards a new stage of digital transformation. In the process of digital government transformation, traditional administrative methods are undergoing profound changes, and automated administration has become a widely adopted form of administrative activities. Under the background of scarce administrative resources and increasingly complex administrative affairs, automated administration is playing an increasingly important role to deal with this contradiction. However, while enjoying the efficiency improvement brought by the innovation of digital governance system, we also need to realize that automated administration still has certain negative effects, especially in the field of personal information protection, the legitimacy of automated administration is facing more severe challenges.

ISSN: 2710-0170

2. An overview of personal information protection in automated administration

2.1. Overview of personal information in automated administration

2.1.1. Concepts and characteristics of automated administration

With the continuous development and application of big data and artificial intelligence, automated administration has gradually become the focus of attention. The term automation administration consists of two words automation and administration, according to the general scientific definition, automation refers to the use of machines to control production, business and other work processes, in the case of reducing or eliminating human intervention, to achieve the expected goals to carry out the process of human will[1]. During the Industrial Revolution, people's understanding of automation technology was limited to machines replacing manual labor; With the advent of the information revolution, the scope of automation technology extends to replace or assist intellectual labor, showing a certain degree of creativity and flexibility. From the narrow point of view, administration mainly refers to the process in which administrative organs and their staff exercise their functions and powers according to law and manage various state and social affairs. Therefore, automated administration can be understood as the behavior of administrative subjects using automated technology to carry out administrative management activities. Although there is not yet a unified definition of automated administration, it can be summarized as a specific link or all links in administrative procedures handled by artificial intelligence or automated systems, without manual intervention, so as to achieve part or all of the unmanned administrative activities. The operating principle of automated administration is described as a technical specification, that is, the legal procedure is written into a programming language in advance, and the automated administrative equipment applies the programming language to handle administrative activities. In general, automated administration refers to an administrative activity mode in which automated equipment or systems deal with part or all of the administrative procedures on behalf of the administrative subject, attributing the legal effect to the administrative subject, and improving the efficiency of administrative management.

2.1.2. The concept of personal information in automated administration.

The meaning of personal information can be mainly discussed from the theory of association, the theory of privacy and the theory of identification. According to the relevance theory, personal information in automated administration refers to all the information related to specific natural persons collected and applied by administrative subjects in the process of automated administration. According to Privacy, it involves information that individuals do not want to be made public, such as captured footage of private behavior. According to the identification theory, it mainly refers to the information collected and applied electronically in automated administration that can be used to identify specific individuals, such as the ID number, address, property and other data submitted by individuals to a specific system in the automatic administrative approval[2]. In this context, the author advocates the adoption of the relevance theory, which defines personal information in automated administration as: all kinds of information related to specific individuals that are processed electronically by administrative agencies and their staff in the process of automated administration.

2.2. The necessity of personal information protection in automated administration

2.2.1. Concepts and characteristics of automated administration

The protection of personal information in automated administration contributes to the realization of the right to human dignity, especially where the right to survival and development

ISSN: 2710-0170

are concerned. In the public sphere, representative automated administrative devices such as electronic eyes or cameras can be seen almost everywhere, and people are under surveillance almost all the time. Sensitive personal information, such as personal whereabouts and tracks, as well as general personal information, such as clothing, are constantly transferred to the databases of public institutions, and the government collects personal information about citizens in various aspects with the help of administrative powers. Compared with traditional administrative activities, automated administration has gradually become the main way for the government to collect, store and utilize personal information through its wide range of information collection objects, continuous information transmission and intelligent information utilization. Personal information is processed in an automated manner at any time, and there is a risk of leakage[3]. Once sensitive personal information is leaked, it will have a significant impact on the survival and development of the information subject. For example, in the "high-speed chest touching case" in Deyang, Sichuan Province, the private behavior of the owner in the car was captured by the electronic eye, and the behavior was immediately uploaded to the network, which brought great trouble to the normal life of the owner. Generally speaking, the car is regarded as a private space, exposing the private behavior of individuals in the private space may violate the independent personality of the parties, making it difficult for them to exercise fair survival and development rights. Therefore, the regulation of personal information processing behavior in automated administration is conducive to the realization of citizens' right to personal dignity.

2.2.2. Help meet the inner requirements of proportionality.

The traditional "three-level" principle of proportionality, which originated from German police law, has gradually become the main criterion for evaluating the legitimacy of public power in a country ruled by law, including the principle of appropriateness, the principle of necessity and the principle of narrow proportionality[4]. In automated administration, administrative organs and their staff must follow the principle of proportionality when handling personal information to ensure the legality of the exercise of power. First of all, under the principle of appropriateness, the means of information processing must be appropriate, whether using electronic surveillance or intelligent systems, should be oriented to the overall interests of society. Secondly, under the principle of necessity, the automation equipment used by administrative subjects must be necessary and minimize the risk of personal information disclosure and other damages to personal information rights and interests. Finally, under the narrow proportionality principle, the public interest achieved by the administrative subject using automation equipment must maintain a reasonable proportion between the damage to personal information rights and interests.

2.2.3. Helps regulate algorithmic discrimination.

Discrimination refers to unequal behaviors and feelings between different groups. Algorithmic discrimination is the unfair classification and accurate profiling of individuals caused by the black box nature of algorithms. Algorithmic discrimination can be divided into human-caused, data-driven and machine-self-learning discrimination[5]. At present, in automated administration, human and data-driven algorithm discrimination is more common. The protection of personal information rights and interests in automated administration helps to ensure the fairness and justice of information processing results, so as to better realize the "internal consistency of public interests and individual interests with justice as the core". For example, the first paragraph of Article 24 of China's Personal Information Protection Law stipulates the transparency of automated decision-making and the fairness and justice of the results, among which transparency is the fundamental regulation of the algorithm black box, and the fairness and justice of the results are the effective defense of "algorithm neutrality". Ensuring the openness and transparency of the information processing process and the fairness

ISSN: 2710-0170

and justice of the processing results in automated administration will be beneficial to regulating the algorithm discrimination caused by artificial and data-driven.

3. Current situation and problems of personal information protection in automated administration

3.1. Current situation of personal information protection in automated administration

3.1.1. Current legislative situation.

The legal protection of personal information in our country mainly consists of two ways: public law and private law. The automatic administration of personal information mainly involves public law protection. Searching "personal information" in the laws and regulations database of Peking University shows that there are 51 laws, 19 administrative regulations, 634 local regulations, 133 departmental rules, 217 local government rules and other normative documents with provisions related to "personal information" in the full text. It can be seen that the personal information protection system in China's automated administration has begun to take shape, and its legislative status is described as follows:

First, the Constitution imposes fundamental requirements on the protection of personal information. Article 33 (3) stipulates that the State respects and protects human rights; Article 38 The personal dignity of citizens shall be protected against unlawful infringement; Article 40 Protecting the freedom and privacy of correspondence of citizens; Article 41 provides that citizens shall have the right to complain, accuse or report and to obtain relief. China's Constitution has the highest effect in the legal system, but most of them are abstract provisions and need to be combined with specific systems to play the actual role of protecting personal information[6].

Secondly, the Personal Information Protection Act establishes the basic framework for the protection of personal information in automated administration. Article 13 of the Act establishes general rules for the processing of personal information, that is, rules with the principle of informed consent as the core and six exceptions without the consent of the information subject. As far as informed consent is concerned, the personal information processor shall follow the principles of legality, legitimacy, necessity and good faith, and comprehensively inform the information subject of relevant matters in a significant manner and clear language before processing, so as to fully protect the individual's right to know, right to withdraw and other rights. Article 24 of the law sets out rules for the processing of personal information in automated decision-making, the first of which aims to regulate algorithmic discrimination represented by "big data killing." The second paragraph provides for the individual's right to opt out of automated decision-making to avoid falling into the "information cocoon"; Paragraph 3 gives individuals a limited right of interpretation of automated decisions and a corresponding right of refusal. Article 26 of the Act essentially regulates the collection of personal information by automated equipment in public places, and stipulates that the installation of equipment can only be used for the purpose of maintaining public safety, and has a prominent prompt sign, unless it is approved by the individual. The third section of Chapter II of the law stipulates that state organs shall process personal information according to the procedures and powers established in accordance with the law, and shall fulfill the obligation of notification when processing. Article 55, paragraph 1, paragraph 2 of the Act mentions that when using personal information for automated decision-making, an impact assessment of personal information protection shall be conducted before the information is processed. Article 62 of the Law stipulates the specific work of the national network information department to coordinate the protection of personal information, of which the second work specifically mentions the development of standards and rules on the protection of personal information in

ISSN: 2710-0170

new technologies and new applications such as artificial intelligence, reflecting the prudent attitude of lawmakers. In addition, the Personal Information Protection Law also provides for the relief system of personal information and rules for cross-border provision[7].

Thirdly, the important provisions on the protection of personal information in other basic laws or special laws. The two "security laws" of the "Data Security Law" and the "Network Security Law" are legal norms for government data security management at the national level, and the relevant provisions include: first, the principle of data security protection. Both security laws attach equal importance to data security and data development and utilization, and adhere to the coordinated development of the two. Second, data security governance body. Article 9 of the Data Security Law stipulates that all social entities, including the government, society, and individuals, are data security maintenance entities; The fifth chapter defines the responsibility of the government in the security and utilization of government data. Article 8, Article 11, and Article 14 of the Cybersecurity Law put forward specific requirements for all social entities to maintain data security[8]. Third, specific systems for data security. The two security laws stipulate specific systems such as data use norms, such as Article 41 of the Network Security Law, which stipulates that network operators should process personal information on the basis of the principles of legality, legitimacy and necessity, and obtain the consent of the collected person, which is similar to the informed consent rule stipulated in the Personal Information Protection Law.

"Administrative Punishment Law" "Administrative Licensing Law" "Administrative enforcement Law" known as the trilogy of administrative law, including the relevant provisions include: "Administrative Punishment Law" article 41, the use of electronic technology monitoring equipment to process personal information, should go through legal and technical review; Article 50: Personal privacy that is known in the process of administrative punishment shall be kept confidential; Article 62, Article 75 and the relevant provisions of the hearing procedure establish the supervision system of administrative punishment, and individuals enjoy the right to know, the right to make statements, the right to plead, and the right to remedy the administrative punishment that infringes on the rights and interests of personal information. Article 5 of the Administrative Licensing Law relates to the general rules for the establishment and implementation of administrative licensing, the principle of the administrative organ disclosing the confidential information submitted by the applicant is to obtain consent, with the exception of the applicant's consent, and the information subject is granted the right of objection if the administrative organ discloses the information according to law; Article 7 and Article 36 provide for citizens' right of presentation, right of defense and right to obtain relief in administrative license. Article 33 requires administrative organs to implement e-government, encourages the implementation of administrative license in an automated manner, and allows the sharing of administrative license information among administrative organs. Article 8 of the Administrative Coercive Law stipulates that the parties have the right to make a statement, the right to plead and the right to obtain relief in the process of administrative coercive law. Article 18 The general rules for the implementation of administrative compulsory measures by administrative organs also stipulate the corresponding obligations of administrative organs[9].

The relevant provisions of the "Road Traffic Safety Law", "Deed Tax Law", "Public Security Administration Punishment Law" and other laws include: "Road Traffic Safety Law" Article 114 affirms the legality of electronic police in the application of administrative punishment. Article 13 of the Deed Tax Law, Article 80 of the Public Security Administration Penalty Law, Article 6 (3) of the Resident Identity Card Law, Article 10 (1) (5) of the Prosecutor Law, Article 16 and Article 40 (2) of the Audit Law, Article 92 of the Social Insurance Law, Article 12 (3) of the Passport Law, and Article 11 (2) of the Military Service Law are all provisions for administrative organs and Its staff have the obligation to keep confidential the personal information collected,

ISSN: 2710-0170

and have not made special provisions for the protection of personal information in automated administration.

Finally, the regulations and rules represented by the Regulations on Government Information Disclosure and the Regulations on Administrative Punishment Procedures for Hangzhou Market Supervision and Management have a large number of important provisions on the protection of personal information. In particular, there are as many as 631 local regulations. Limited to the length of the article, briefly one or two. Article 15 of the Regulations on the Disclosure of Government Information stipulates that if the disclosure of classified information would harm the legitimate rights and interests of a third party, an administrative organ shall not disclose it, unless it has the consent of a third party to disclose it or the administrative organ considers that the unfair meeting has caused a major impact on the public interest. Article 9 of the Provisions on the Protection of Personal Information of Telecommunications and Internet Users regulates the processing of personal information by telecommunications business operators and Internet information service providers, etc. In general, most of the normative documents at other levels of effectiveness only involve the framework provisions of personal information protection, and fail to reflect the specialization of personal information protection in automated administration[10].

3.1.2. Status quo of law enforcement

In automated administrative law enforcement, commonly used automation equipment or systems include electronic eyes, administrative punishment system and discretionary system of Nanjing Environmental Protection Bureau, "traffic management 12123" App developed by the Traffic Management Science Research Institute of the Ministry of Public Security, and autonomous tax payment system. Among them, the automatic administrative punishment represented by the electronic capture of traffic violations is the most common. In the field of public transport, electronic eyes continue to collect traffic violations of motor vehicles, non-motor vehicle drivers and pedestrians, upload the evidence to the internal system of the traffic administrative department, and the relevant departments and staff make administrative punishment decisions. These decisions are also sent to the person punished. In the whole automatic process of electronic capture of traffic violations, the electronic eye mainly plays an auxiliary role, and its function is limited to the input of personal information. Therefore, in the electronic capture of traffic violations, the violation of personal information is usually unrelated to automated equipment, but related to the penalty decision and output stage after manual intervention, and the relevant regulations mainly regulate the information processing behavior of law enforcement personnel. In law enforcement practice, administrative organs and staff mainly focus on satisfying administrative purposes and promoting public interests, while personal information protection and protection of personal rights and interests are secondary.

In the process of granting administrative law enforcement, the commonly used automation equipment or system includes automatic examination and approval system, government service website, etc. Automatic examination and approval generally refers to the whole process of administrative examination and approval online, manual intervention or only responsible for background audit. According to the degree of manual participation, automatic approval can be divided into two types: one is completely without manual intervention, the automatic system can immediately process the approval matters, also known as "second batch", which belongs to fully automated administration; The other is the combination of automation and manual audit, after the applicant submits the application materials online, the manual audit in the background, and sometimes the applicant needs to go to the scene. The automatic examination and approval system can be applied to a wide range of applications in various social fields such as education, medical care and service[11]. It can take many forms, either as a standalone automated system or embedded in existing government service websites and mobile applications. Cities such as Guangzhou, Shenzhen and Qingdao are leading the country in the reform of civilian approval

ISSN: 2710-0170

services. For example, Qingdao is at the forefront of the country in terms of enterprise registration "second batch" and online processing of electronic construction permits. The degree of automation of automatic approval is very high, and the implementation relies on sufficient and accurate shared data in the background database, which usually requires manual intervention, and the staff of the background administrative organs review the application materials submitted by the applicants. Regardless of the type of administrative approval, the personal information submitted by the applicant will enter the government database. Our government has a huge database, in the storage and reuse of personal information, there have been some information security incidents, which is also an important issue faced by automated administrative law enforcement[12].

In the automated administration, there is also a new law enforcement model that is neither burden nor benefit administration. The typical example is the implementation of administrative management based on health code. The health code, which emerged during the fight against COVID-19, processes personal information such as travel time, method and contact to generate QR codes in red, yellow and green. The colour of the QR code can be used to assess an individual's risk of carrying the virus. The behavior of generating health code belongs to administrative rating, although it will not directly lead to the creation, change or termination of administrative legal relations, but its rating results can be used as the basis for personnel classification management. Sometimes the health code can be used as a prerequisite for administrative licensing, for example, red code personnel may be restricted from taking legal professional qualification examinations; Sometimes it can also be used as a basis for administrative enforcement, such as red code personnel may be restricted from travel freedom. Health codes process personal information digitally and are of great significance in responding to public health emergencies. Legal provisions such as the Law on the Prevention and Control of Infectious Diseases and the Law on Response to Emergencies give administrative agencies the power to directly collect and use personal information during special periods. The use of health codes for "compulsory" collection of personal information during special periods is in line with the exceptions for informed consent in the Personal Information Protection Law, but this legality is based on the satisfaction of significant public interests. After the outbreak is effectively controlled, the risk of personal information infringement in health code applications may increase[13].

3.2. Issues of personal information protection in automated administration

3.2.1. Legislation provides too little directly

In 2021, China promulgated the Personal Information Protection Law, which initially established a personal information protection system and got rid of the lack of special legislation. However, in the field of automated administration, the direct legal provisions on the protection of personal information are very limited, and the relevant personal information protection provisions need to be referred to in the application of the law. The provisions on automated decision-making in the Personal Information Protection Act generally apply to automated administration, but only in relation to articles 24, 55 and 73. In addition, Article 26 of the Personal Information Protection Law, Article 41 of the Administrative Punishment Law, article 33 of the Administrative Permission Law, and Article 114 of the Road Traffic Safety Law contain provisions on automation equipment, although they can barely be regarded as direct provisions. In addition to these seven laws, it is difficult to find more direct provisions on the protection of personal information in automated administration at the legal level, and this lack of direct system design may not be conducive to regulating the risk of personal information being infringed in automated administration[14].

ISSN: 2710-0170

3.2.2. Legal operability is not strong

The effectiveness of the law lies in its implementation, so it is necessary to consider the operability of the law: First of all, as far as the personal information protection framework constructed from the legal level is concerned, China has adopted the individualistic protection path, and the personal information protection in automated administration also applies this path. Informed consent rule is the core rule. The law entrusts individuals with the right to know, the right to consult, the right to copy, the right to withdraw and so on, and expects individuals to exercise these rights independently to implement the informed consent rule. However, in the face of automated administration with the development of artificial intelligence and big data technology to a certain extent, it is difficult for individuals to exercise their so-called rights. On the one hand, due to the black-box nature of the algorithm, individuals are almost unable to realize the risk of the algorithm to their personal information, so personal information rights are difficult to play a practical role[15]. On the other hand, when administrative organs process personal information based on six special circumstances that do not require personal consent, it is more difficult for individuals to exercise information rights against public power subjects.

Secondly, the principle of personal information protection relying solely on top-level design is just a castle in the air, and it must be implemented by laws and regulations at a lower level of effectiveness. Although there are many provisions on the protection of personal information in regulations, rules and other normative documents, from the perspective of their application field, the provisions on the protection of personal information in various industries and departments are mostly framed, and also lack specific procedural provisions. From the perspective of its effectiveness level, most of the local provisions follow the provisions of the superior law, and it is difficult to have regional characteristics.

3.2.3. Help meet the inner requirements of proportionality.

According to the provisions of Article 60 of the Personal Information Protection Law, the national network information department is responsible for coordinating and coordinating various departments to carry out personal information protection supervision by industry, and this kind of horizontal and vertical supervision system helps to rationally allocate the power of regulatory authorities and improve the professionalism of supervision in various industries. However, this regulatory system also has inherent defects: on the one hand, major information leakage incidents usually involve national security, finance, medical and other social fields, and supervision by various departments by industry is not an effective coping mechanism. On the other hand, the main responsibility of the national network information department is to coordinate network security and related supervision and management, rather than specifically responsible for personal information protection, and its functions and powers overlap with administrative organs such as telecommunications authorities and public security departments, so it is worrying whether its coordination responsibilities can be effectively performed[16]. The Data Security Law and the Network Security Law emphasize that social subjects such as the government, society and individuals are the subjects of information security, but also do not clearly specify the supervision and management authority of various industries and departments.

3.2.4. Improper immunity from administrative procedures.

The burden administrative act is to realize the punishment and education effect by reducing the rights and interests of the administrative counterpart or increasing the obligations, or to provide public services and promote the public interests of the society. The arbitrary exemption of administrative procedures in the burden of administrative acts will make it difficult to achieve the balance between public interests and individual interests. For example, automated administrative punishment partially exempts the procedures of notification, hearing, presentation and defense provided for in the Administrative Punishment Law, which is more

ISSN: 2710-0170

disadvantageous to citizens in vulnerable positions. Citizens often have their personal information collected without their knowledge and lack the means to make statements and defend themselves when their information is violated[17].

4. Perfection of legal protection of personal information in automated administration

4.1. Current situation of personal information protection in automated administration

4.1.1. Expand the direct provision of automated administration.

Due to the lack of direct provisions on automated administration in China's current laws, personal information cannot be effectively protected in automated administration, and there is a legislative gap. Therefore, it is necessary to strengthen the explicit provisions of legal norms on automated administration. Specifically, on the one hand, it is to amend the Personal Information Protection Law, add the definition of automated administration, the type and scope of protection of personal information to the special personal information protection law, and clarify the legal reasons for the processing of personal information in automated administration. On the other hand, it makes special legislation for the protection of personal information in automated administration, promulgates higher level legal norms or judicial interpretations, clarifies the specific provisions on the protection of personal information in automated administration and its application in the existing legal system, and provides direct provisions for solving actual information security incidents[18].

4.1.2. Make the law more operational.

China's personal information protection system is centered on the informed consent rule. In view of the application of the informed consent rule in automated administration, continuous information disclosure mechanism and dynamic consent mechanism need to be established to strengthen the operability of the informed consent rule. Specifically, the law can set reference standards for the protection of personal information in automated administration, strengthen the information disclosure obligations of administrative organs at all levels through regulations, ensure that citizens can exercise the rights related to dynamic consent, clarify more stringent informed consent rules, and establish a phased and hierarchical dynamic consent mechanism. The law should also provide guidance to implement the informed consent rule, standardize the formulation of the lower law, and require the lower law to take into account the actual situation of the industry, department, and region, and formulate a personal information protection system in line with the characteristics of the respective industry, department, and region.

4.1.3. Improve the supervision and management mechanism of personal information.

In our country, the departments that perform the duties of personal information protection exist in both horizontal and vertical aspects, but there are still shortcomings in the provisions of the duties of each department. The first paragraph of Article 60 of the Personal Information Protection Law provides for the special responsibility of the national network information department to coordinate, but the second paragraph adopts the arbitrary rule, resulting in the lack of specific responsibilities of local government departments at or above the county level. Therefore, in order to further improve the supervision and management mechanism of personal information, the key is to clarify the specific responsibilities of the functional departments of personal information protection, including the rights and obligations of various departments, in order to give full play to the effect of the horizontal and vertical combination of the supervision system.

ISSN: 2710-0170

4.2. Perfection of law enforcement

4.2.1. Correct administrative due process.

In the burden administrative act, the legitimacy of the law enforcement procedure is the basis of the legitimacy of the administrative act. Whether it is the use of automated equipment that can collect images and information, or automated systems such as mobile phone apps with more discretion, administrative organs and their practitioners should make clear the following points: First, burden administrative acts do not reduce the procedural obligations of administrative subjects because they involve automation, and legal norms such as the provisions on procedural requirements in the Administrative Punishment Law should not be arbitrarily exempted. Secondly, law enforcement should adapt to the development of science and technology, and leave room for innovation for technological change. For example, in terms of the notification obligation in traditional administrative penalties, administrative subjects can inform the penalized person in advance through smart SMS and other means.

4.2.2. Implement the principle of least necessary.

With the continuous upgrading of government data governance model, personal information security is facing more and more threats, so it is necessary to strictly implement the minimum necessary principle of information processing in order to restrain the unlimited expansion of public power. Article 6 of the Personal Information Protection Law stipulates the minimum necessary principles that personal information processors should follow, including that the processing of information is directly related to the purpose of processing, the profit or loss is minimized, and the scope of information collection is limited to the minimum necessary scope. The principle of least necessity is derived from the principle of proportionality, which requires that information processing must consider appropriateness, necessity and proportionality at the same time.

Although the administrative organs adopt the automatic way to promote the convenience of grass-roots governance, the motive of simplifying governance tends to the limit of public power, resulting in the information processing behavior of administrative organs actually deviating from the principle of minimum necessity. In order to implement the principle of least necessity and fully protect the security of personal information, the following measures can be taken: First, when designing new governance tools such as "health code", administrative organs should consult the public extensively and disclose information processing to the public on a regular basis. Secondly, individuals not only have the right to informed consent, but also the right to supervise, report, and Sue the administrative authorities and their practitioners. In order to cultivate citizens' consciousness of active participation in political and economic life, citizens should be guided to participate in information security supervision spontaneously.

4.3. Perfection of relief

4.3.1. Clarify the applicable rules for administrative public interest litigation.

In my opinion, administrative public interest litigation should be applied to the protection of personal information in automated administration to clarify the applicable rules, which can be started from the following two aspects: First, promulgating judicial interpretations or improving legal norms to stipulate that the protection of personal information in automated administration belongs to the scope of administrative public interest litigation filed by procuratorates. Secondly, establish the criteria for the identification of damage to national interests and public interests, specifically enumerate the cases where the infringement of personal information in automated administration leads to damage to national or public interests. Because of the cluster effect of information, when the administrative subject abuses its power or fails to act, the damage often involves the collection of many personal information interests, and the case of individual damage to specific personal information rights and

ISSN: 2710-0170

interests is rare. At the same time, due to the rising judicial costs of individuals seeking damages by filing lawsuits, this is one of the reasons why the Personal Information Protection Law specifically stipulates public interest litigation. The application of administrative public interest litigation is necessary in theory and practice. For example, in view of the illegal collection of personal information by many government apps, procuratorial organs should file administrative public interest litigation cases and launch investigations if they have reason to believe that the illegal acts of relevant departments may harm the national or public interests. This kind of system design can more effectively restrain the problem that the administrative organ does not fulfill the information security obligation.

4.3.2. Build a scenario-based imputation method.

There is a legislative tendency to adopt a unified imputation of fault for different information rights and interests. The author believes that if lawmakers recognize that the disclosure or illegal use of sensitive personal information will cause harm to the personal and property safety of the information subject, then they can consider imposing no-fault liability on the actors who violate such personal information. Similarly, in the case of a general breach of personal information, it may be stipulated that only the offender is subject to the presumption of fault liability. With reference to the provisions of Article 1198 of the Civil Code, when the actions of a third party lead to the infringement of personal information, the law can provide that the direct infringer shall be investigated for infringement liability, and the administrative organs and their employees shall bear corresponding supplementary responsibilities if they fail to fulfill reasonable security obligations. Such scenario-based regulations help to cope with new personal information protection issues brought about by the development of science and technology.

Such differentiated liability provisions can be better applied to information infringement in different situations and help to improve the protection of information subjects. At the same time, for those who intentionally or negligently disclose sensitive information, imposing no-fault liability may be more conducive to safeguarding the rights and security of information subjects. Such a legislative trend can establish a more comprehensive and effective legal framework in the field of information protection to ensure that the security and privacy of personal information are adequately protected.

References

[1] Zhan Penghe. Review on the Legitimacy of power in Digital administrative Mode [J]. China Law School, 2021 (03) : 114-116.

[2] Chen Yang, Pei Yanan. On Application Risk and Prevention Path of Algorithm decision Making in Automated Administration [J]. Law, 2021 (01) : 75.

[3] Ao Shuanghong. On Automated Administration and its Legal Regulation [J]. Journal of Hunan Police College, 2017 (01) : 84-85.

[4] Special system logic and regulation strategy of Sensitive Personal Information protection [J]. Administrative Law Studies, 2022 (01) : 119-130.]

[5] Huang Xuexian. Research on the Principle of Proportion in Administrative Law [J]. Science of Law, 2001 (01) : 72-73.

[6] [Li Yuan. Research on Personal Information protection in Big Data era [D]. Chongqing: Southwest University of Political Science and Law, 2016:52-53.]

[7] Ye Bifeng. The Humanistic Spirit of Administrative Law [M]. Beijing: Peking University Press, 2005:114-115.

[8] [Ma Yanxin. Digital Government: Change and rule of Law [M]. Beijing: China Renmin University Press, 202:361-362.]

ISSN: 2710-0170

[9] Zha Yunfei. Academic Basis and Functional Orientation of Automation of Administrative Discretion [J]. Administrative Law Studies, 2021 (03) : 114-124.

[10] Ma Yanxin. Administrative Punishment under automated administrative mode: Challenges and Responses [J]. Politics and Law, 2020 (04) : 139-148.

[11] Li Qing. Why Automated administrative Punishment is Just [J]. Learning and Exploration, 2022 (02) : 72-81.

[12] HartzogW ContiG, NelsonJ, etal. InefficientlyAutomatedLawEnforcement [J]. J Michigan State Law Review, 2015 (02) : 1769.

[13] Wang Zhengxin. Why Machine Discretion: Automation of Administrative punishment discretion and its risk control [J]. Administrative Law Studies, 2022 (02) : 166-176.

[14] He Xiaoli, Yang Xingmei. Research on the path of orderly Promoting the second batch of government services: based on the investigation of Qingdao City [J]. Journal of Qingdao Administration College, Party School of the CPC Qingdao Municipal Committee, 2021 (01) : 46-52.

[15] Zha Y F.Health code: Automated rating and utilization of individual epidemic risk [J]. Zhejiang Journal, 2020 (03) : 28-35. (in Chinese)

[16] Bao Kun. Restriction of proportionality principle in normalizing application of health code data [J]. E-government, 2021 (01) : 32-41.

[17] Ding Xiaodong. Personal Information Legislation in the era of big Data and Artificial Intelligence: On the challenge of new technologies to information privacy [J]. Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition), 2020 (03) : 8-16.

[18] Zhang Linghan. Conflict and Reconciliation between Algorithmic automated decision-making and administrative due process system [J]. Eastern Jurisprudence, 2020 (06) : 4-17.