Research on Legal Protection of Personal Information in Artificial Intelligence Environment

Longyunhanlou[1], Sarana Photchanachan[2], & Sukuman Shumnij[3]
[1]PhD Candidate, School of Management,
Metharath University: Email: 16924093@qq.com
[2]Dean of School of Management,
Metharath University: Email: sarana.p@mru.ac.th
[3]Lecturer of School of Management,
Metharath University

Received: 19/04/2023, Revised: 15/05/2023, Accepted: 23/05/2023

Abstract

The research idea and content of this paper is based on the background of big data era. First, it is to study the definition of personal information in the artificial intelligence environment and the difference between personal information and privacy; Then it analyzes the current situation and new challenges of personal information protection in the artificial intelligence environment, and then analyzes the reasons for information leakage; The second is to study the current situation of personal information protection in some countries or regions outside the region and its enlightenment to China; Finally, it puts forward suggestions on personal information protection in China under the artificial intelligence environment. The overall research idea is problem-oriented, that is, finding problems and putting forward countermeasures. Based on the introduction information and the above questions, this study aims to find the answers to the following three questions: 1 How to protect personal information in AI environment? 2. How is the legal protection of personal information conceived and practiced in the AI environment? 3. What are the obstacles to the legal protection of personal information in the AI environment? On the basis of theoretical analysis, this article discusses the impact of perceived risk, willingness to protect, and perceived response on personal information protection behavior. Based on data analysis and hypothesis testing, the theoretical hypothesis is tested, and the research finds that personal information perceived risk has a significant impact on protection behavior; The perceived risk of personal information has a significant impact on the willingness to protect; The willingness to protect personal information has a significant impact on the protection behavior; Willingness to protect plays an intermediary role between perceived risk and protective behavior; Perceived response plays a regulatory role between perceived risk and protective behavior.

Keywords: Artificial Intelligence Environment, Personal Information, Legal Protection

Introduction

At present, there are more and more topics related to artificial intelligence in the academic field. From the current situation, artificial intelligence is a vigorously developed field in China and becomes a powerful power for economic development. Artificial intelligence has broad application prospect and its great development is the inevitable trend of globalization. In the era of artificial intelligence, information data has become a new type of energy with strong potential value, driving competition among large enterprises.

Artificial intelligence has been deeply embedded in people's lives, such as "facial payment", "fingerprint unlock", intelligent commodity recommendation, and so on, has become a necessary tool in life. If artificial intelligence wants to achieve sustainable growth, it must rely on a huge amount of data as its fundamental support. Without information and data, artificial intelligence will be unable to make progress. People need artificial intelligence to meet the needs of life, and at the same time, artificial intelligence also needs people's information, as the "energy source" for survival and development. With the help of powerful computing power and deep learning technology, major breakthroughs have been made in the collection, use, analysis and reorganization of personal information. Personal information is faced with the risk of excessive and improper analysis and use by artificial intelligence, especially at present, highly identifiable biological information is widely collected and used, so the risk will continue to increase.

As the report of "315 Party" in 2021 shows, consumers' personal information faces serious risks of leakage and trading. For example, the camera installed by Kohler Sanitary Ware captures the facial information of every customer entering the store without their prior consent and without their awareness. And through intelligent analysis to identify the consumer's gender, age and even mood when entering the store, to each piece of face information for unique ID marking, accurate identification of the consumer is the number of times to enter the store, what is the consumption demand, when the consumer enters other chain stores, through face information recognition, access to all the information of the consumer in other stores. Guide stores to carry out precision marketing for this consumer. Meanwhile, the total account storing face information can view all face information. Thus, when artificial intelligence is applied to the real economy, consumers' personal information is also faced with numerous risks. After the real economy is supported by intelligent devices, it also brings unprecedented new challenges to the protection of personal information.

Therefore, in order to deal with the great risk of personal information protection caused by the development of artificial intelligence, explore the challenges faced in the field of personal information protection under the background of artificial intelligence era, to seek effective protection of personal information countermeasures, for giving consideration to the protection of personal information and the development of artificial intelligence, it is of important practical significance. Taking this as the starting point, this paper analyzes the main problems existing in the field of personal information protection, and explores possible countermeasures by referring to the relevant experience of countries and regions outside the region, so as to promote the development of artificial intelligence and effectively protect the personal information of natural persons.

With the increasing maturity of artificial intelligence technology, autonomous driving, biometrics, autonomous learning and other technologies develop rapidly and are widely used. As a cutting-edge technology, artificial intelligence greatly facilitates people's lives, but also brings many risks to human society, such as violating citizens' privacy, destroying social order and even endangering national security. Among these risks and challenges, AI's snooping on citizens' privacy is of particular concern. Due to the extensive application of artificial intelligence, the collection and extraction of citizens' personal information by commercial

institutions and government agencies has become omnipresent. Coupled with intelligent and relevant analysis and portrait, the property rights and personal safety of citizens have generated new risks caused by "transparency". Various applications of artificial intelligence are changing our life, improving our work efficiency and changing our way of thinking. At the same time, they are also threatening our personal information security with comprehensive coverage. Our personal information is collected secretly and silently by a variety of mobile phone computer applications, cameras, detectors, and the collected information after deep processing and analysis, the data capacity carried by the original information is constantly expanding, increasing association, the boundary of information security is less and less obvious, some seemingly does not have the identification of information after technical processing may also accurately locate to the individual. The management ability and right of the subject of personal information to the information have been dissolved in essence, which leads to the potential threat of property safety and personal safety.

The importance of artificial intelligence laws, regulations, ethics and policy system construction has been emphasized in top-level strategy. On July 20, 2017, The State Council issued the "Development Plan for the New Generation of Artificial Intelligence", which put forward requirements for the construction of legal and ethical systems in the outline goals: by 2020, artificial intelligence ethical norms, policies and regulations in some fields will be preliminarily established; By 2025, AI laws, regulations, ethics and policy systems will be initially established to form AI security assessment and control capabilities; By 2030, a more complete system of AI laws, regulations, ethics and policies will be established. As the guarantee of the healthy development of the AI industry, the legal framework of laws, regulations and ethics should be carried out in the future, including the recognition of civil and criminal liability, privacy and property rights protection, information security utilization and other legal issues related to the application of AI. The focus should be on the segmentation fields with good application foundation, such as autonomous driving and service robots, to speed up the research and formulation of relevant management regulations.

With the advent of the new era of artificial intelligence, the topic of personal information protection has once again become a hot topic in the society and has been widely concerned by people. Artificial intelligence products can be seen everywhere around us, such as smart phones, access control system with facial recognition, various apps, etc. Artificial intelligence is a double-edged sword. On the one hand, it facilitates our life, but on the other hand, it also bothers us. In recent years, more and more incidents of personal information infringed, such as the case of Xu Yuyu who suffered from telephone fraud in 2016, the case of AI infringing on citizens' personal information in 2017, the first case of face recognition in China in 2019, and the data of nearly 500 million users of Sina Weibo was leaked in 2020. It's fair to say that there are different threats to our information all the time. There is no denying that we enjoy the convenience brought by artificial intelligence every day and develop dependence on it, but we also suffer from the daily intrusion of information, such as nuisance calls, spam text messages and so on. People may be victims of personal information leaks, but sometimes we don't even know it. There are many reasons for the frequent infringement incidents: for example, the reason of science and technology, artificial intelligence technology is still in the early stage of development, not mature enough, personal information is inevitably exposed to technical loopholes; The reason for having supervision, our country supervision organs, the supervision mode provisions are not perfect; There are industrial reasons, in such a vanity fair, companies are chasing profit maximization; There are also legal reasons, our country's legal system of the protection of personal information is not systematic enough, especially in the background of artificial intelligence, tort subject, scope of personal information protection and the legal attribute of personal information is not clearly defined,

and then leads to the difficulty of relief. In the era of artificial intelligence, the development of artificial intelligence is an inevitable trend, its development needs the support of data and information, at this time, personal information security is facing the risk of being infringed at any time, which prompts us to speed up the pace, improve the legal protection of personal information.

In recent years, with the application of artificial intelligence technology, strengthening the protection of personal information from the legislative level has become the consensus of all countries in the world. The European Union has introduced the General Data Protection Regulation (2016) (GDPR). In order to realize the development of its artificial intelligence industry and improve the protection of its citizens' right to personal information, Germany has modified its relevant legislation by referring to international mainstream standards. The US government has also introduced a lot of special legislation related to artificial intelligence technology and the protection of citizens' personal information. With the deepening of globalization, China has also realized the importance of strengthening citizens' personal information in the era of artificial intelligence, and has gradually strengthened the protection of citizens' personal information from the legislative level. Not only has the Civil Code clearly stipulated the protection of personal information, but also has specially formulated the Personal Information Protection Law. Has made our country to personal information legal protection on a new stage, this is undoubtedly worth affirming. But at the same time, we should see that in the face of the challenges brought by artificial intelligence to the protection of personal information, there are still many problems that have not been responded to in the current legislation, which makes it necessary to further study this issue.

The research ideas and contents of this paper are carried out around the background of the era of big data. Firstly, the definition of personal information in the environment of artificial intelligence is studied, and the difference between personal information and privacy is studied. Secondly, it analyzes the protection status and new challenges of personal information under artificial intelligence environment, and then analyzes the reasons for information leakage. Secondly, studying the current situation of personal information protection in some foreign countries or regions, and the enlightenment to our country. Finally, some suggestions for the protection of personal information in the artificial intelligence environment are put forward. The overall research idea is problem-oriented, that is, problems are found and countermeasures are proposed.

Based on the introduction information and the above questions, this study aims to find the answers to the following three questions:

1. How does the protect personal information in an AI environment?
2. How is the legal protection of personal information conceived and practiced in the artificial intelligence environment?
3. What are the barriers to legal protection of personal information in the AI environment?

Research Objectives

Based on the above research questions, the goal of this study is to find the answers to the above three research questions:

1. to study the protect personal information in an AI environment.
2. to investigate the legal protection of personal information is conceived and practiced in an intelligent environment.
3. to identify the obstacle to legal protection of personal information in the environment of artificial intelligence.

Literature Review

It is generally believed that risk consists of three basic elements, namely potential loss, the size of loss and the uncertainty of loss. In the studies of statistics, economics, insurance and other disciplines, it is often assumed that risk is quantifiable. A commonly used formula is: risk = the degree of injury or loss × the possibility of occurrence. However, this assumption ignores the people who face the risk, that is, the subjective recognition of the risk, which determines the non-objectivity of the risk itself.

Williams and Heins (2013) introduced human subjective factors into risk analysis, believing that although risk is objective, it exists to the same extent for everyone. But uncertainty is the subjective judgment of the risk analyst, and different people may have different views on the same risk. Many scholars have carried out subjective research on risk, and introduced a new concept -- risk perception into the field of risk research to study individuals' perception and cognition of objective risk, emphasizing the influence of individuals' experience acquired through direct observation and subjective perception on individual perception. Risk perception is a subjective assessment of the probability of occurrence at a given time and how much we worry about its consequences. The perception of risk is a multifaceted phenomenon that varies from individual to individual and from situation to situation.

Paul (2011), as a famous expert in the field of risk and decision making, has done a lot of research on risk perception. According to his research, there is a big difference between the general public's perception of risk and the perception of experts in the field of risk. The analysis results show that many factors can cause people's risk perception degree deviation. On the basis of previous studies on risk perception, Huang Dinglong et al. selected factors related to people's cognition of information security for research and factor analysis, identified six factors, and built the KISCAP model of information security perception. He found that knowledge, influence, severity, controllability, possibility, and perceptibility all influence user perception and further influence user behavior.

People's perception of risk plays a big role in how they make decisions. Differences in risk perception are at the heart of disagreements between experts and ordinary people, men and women, and people from different cultures about what is best behavior. Both individual and group differences in choice preferences for risk decisions and situational differences in risk preferences have been shown to be related to the perception of relative risk of different choices, rather than to attitudes towards risk (that is, the tendency to accept or avoid risky choices). Users' perception of risk can determine their willingness to embrace technology. In fact, research has proven that users are more willing to embrace technology when they think the benefits outweigh the potential risks.

Mobile devices are often more "personal" than PCS. Users may think their phones are safer than their computers because they are always on them. But physical control of computing devices does not automatically guarantee information security. Users' false perception of handheld and portable devices can lead them to believe that they are safe to store sensitive information on them. Attacks on mobile devices can affect users' most personal information: numbers, names, contacts, appointments, passwords, and even authentication information. Although this personal information is also stored on computers, it is stored in a more fragmented, disorganized and sparse way than on mobile phones. In fact, attacks on mobile devices usually take much less time to find private information (Zhang Ping, 2017).

In an AI environment, usability issues are exacerbated by the fact that devices are not easy to operate. We analyze information security in AI environment based on literature,

experience and previous research. We found that two new factors may have an impact on people's perception of information security in an AI environment: trust related to the organization and the impact on privacy. Trust is important because mobile communications are supported by carriers. They have a lot of responsibility for keeping mobile information secure. The importance of trust to mobile information security has also been mentioned in previous studies. Privacy is also very important for device users in artificial intelligence environment, because mobile devices often store a lot of personal information (Zhang Li 'an, 2016).

First, users are more likely to risk a loss than to accept a certain loss. Tversky (2016) found that when the consequences of different choices were presented in terms of income, people were more inclined to avoid risks; When the consequences of different choices are represented by losses, people are more likely to take risks. In the field of security, failure to carry out safe behaviors may result in losses, while safe behaviors require certain time and energy expenditure. Also, people tend to believe that they are less vulnerable than others. Computer users also think they are less vulnerable than other users.

Second, users see security as a secondary task. When making decisions under time pressure, people focus more on losses than gains that will affect their immediate goals. Helen (1998) analyzed from the perspective of economics why people ignore security advice in terms of passwords, identifying URL addresses of phishing websites and verifying warnings. She believed that users do so because it takes time and energy to take safe behaviors immediately, while the possible security benefits are illused and often happen late.

As "user-centered design" has become a widely accepted concept in the field of human-computer interaction, it is now being gradually applied to the field of security. Several researchers have studied usability issues in security tools. Schintz, Proctor(2019) presents a taxonomy regarding the availability aspects of security controls and explains why elements of the taxonomy are necessary. Whitten (2016) pointed out that many usability problems in information security are fundamentally different from those in other user software, and usability design criteria need to be carefully adjusted to successfully solve these problems. She also points out that making security tools easy to use requires creating a user interface design approach that addresses these challenges. Stewart (2017) studied the effectiveness of security warnings. They suggested that security warnings must clearly convey information about threats and give simple and easy to understand instructions to avoid threats. Other researchers go beyond the usability issue to a broader dimension that puts users at the center of security design. They take user behavior and psychology into account. Clam (2016) provided several suggestions on how to persuade users to adopt safety measures, including an in-depth understanding of the losses that users can bear, user education for high-risk groups, weeding out inappropriate old safety suggestions, prioritizing safety suggestions, and respecting the time and effort required for users to adopt safety suggestions.

Classification of personal information is of great significance to protect the rights and interests of the information subject. In the theoretical circle, there are different classification standards for personal information, among which the most important classification standard is the sensitivity of personal information. According to the sensitivity of personal information, it can be classified into sensitive information and general information. Due to differences in social system, level of development and religious belief, countries have different definitions of "sensitive". In Britain, for example, sensitive information is defined as race, religion, health and sexual status. The European Union (Article 9 of the General Data Protection Regulation) added political ideas and genetic information on the basis of the UK. Germany (Article 3 of the Federal Data Protection Act) combines the UK and EU enumerations of sensitive information. The opposite of sensitive information is general information, which usually refers to information that does not identify a particular information subject. Denmark calls this "trivial

data." There is a great dispute about the right attribute of personal information. As far as we can see, there are four mainstream views, which are personality right theory, property right theory, new rights and new personality rights theory.

At the individual level, the services provided by social e-commerce sites (personalization) are based on what users propose For personal privacy information, such as: group bargaining, personalized product recommendation. In the process, the user Personal privacy information will inevitably be collected and used, users like the platform to disclose personal privacy information

Risks and benefits, such privacy concerns affect the user's attitude to disclose their personal privacy information, and then shadow Ring the user's personal privacy disclosure wishes.

In the privacy computing theory of Culan and Armstron (2019), when users disclose personal information for the purpose of economic and social benefits, some evaluation behaviors are often carried out. The main concern of users is whether the private information is used legally and whether the use of information will have a negative impact on individuals. Its view can be expressed by the formula: U(X)=Benefit-Cost. It also shows that consumers' analysis of benefits is not accurate, but trade-off costs and benefits.

Third, the range of personal information will continue to expand. Due to the strong information collection and analysis ability of artificial intelligence algorithms, the scope of personal information is expanding, and the types are also growing. In addition to the traditional ID number, contact information, home address and other information, although some information can not independently identify a specific subject, but if added with other information to assist, it can achieve the purpose of searching for a specific person, such as interests, hobbies, age, occupation and other information, also belong to the list of personal information. "Information Security Technology, personal information security Code" stipulates that, through the use of intelligent technological means to information, "anonymous" processing, because the information can not identify specific individuals, so no longer is personal information. However, due to the special ability of artificial intelligence to process information, the anonymous information can be input into the intelligent program to achieve "de-anonymization", and then get an accurate personal portrait. Taking the Netflix case as an example, Netflix (2019) published a database containing movie ratings and rating time of viewers after anonymising in order to improve the service of movie Twitter. However, the experimental result was surprising: most relevant user records in the database could be re-identified and de-anonymised with only a small amount of susuke information. It only takes eight movies to score and within 14 days to identify 99 percent of the users in the library, and only takes two movies to identify 68 percent of the users. Therefore, it is not difficult to find that while the current technological development can bring convenience, technology can also threaten the protection of information, bringing new protection problems and greater challenges. In the current digital society, de-anonymization is bound to expand the scope of personal information. In 2010, Paul Ohm, an American lawyer, wrote that while in practice malicious attackers often use personally identifiable information (such as social security numbers and names) to identify individuals, in practice, even if an attacker only uses non-essential information that is not defined as "personally identifiable information," It can also achieve its purpose. The de-anonymization technology is only one way for artificial intelligence to process data. In addition, with the development of deep learning, there will be a large number of intelligent technologies for special information processing to realize personal purpose. Therefore, in the era of artificial intelligence, the scope of personal information will continue to expand.

Biometric information will become the key type of information needed in the era of artificial intelligence. Traditional personal information, such as ID card numbers, which are

mainly protected by law, is only a part of the personal information collected by artificial intelligence at present. Compared with previous information collection methods, the outstanding advantage of artificial intelligence is that it can efficiently collect and use biometric information in large quantities. Biometric information is the main type of personal information required by artificial intelligence. On March 12, 2020, the Face recognition Service Law was passed in Washington State. The law provides the legal basis and legal guarantee for the application of face recognition technology in Washington State. It is the first special bill on face recognition. In 2008, the US state of Illinois issued the "Biological Information Privacy Act", which clarified the connotation of "biological information" for the first time and stipulated the obligation of notification when collecting "biological information" for the first time, and the subject's authorization should be taken as the legal premise of information collection. Our "information security technology, personal information security standards", improved the biometric information protection provisions, and detailed the specific management regulations. A series of laws and regulations regulating the use of biometric information have been issued worldwide, reflecting that biometric information is widely used and has a wide range of application prospects. In the context of intelligent society, biometric information will become the key type of information needed by artificial intelligence, which is also the key problem that current laws need to deal with (Cheng Xiao, 2020).

Western scholars mainly study online personal information in the information society from the two categories of property rights and privacy rights, but more scholars tend to study from the perspective of information privacy. As Warren and Brandeis argue, the value of [privacy] does not lie in profiting from the disclosure of information, but in the peace of mind and faith provided by the ability to prevent any disclosure. In the usual sense of the word, it is difficult to regard it as a kind of asset right. Based on this, both ALan F. Westin, a professor emeritus at Columbia University, and Artheur R. Miller, a scholar at the New York University Law School, have linked privacy to the control of personal information, Professor Westin defined privacy in Privacy and Freedom as "an individual, a group or an organization has the right to independently decide when, how and to what extent to convey information related to oneself to others. However, Miller pointed out in Attack on Privacy that the basic quality of privacy is" the ability to control the flow of information related to oneself. Adam D. Moore also agrees that the right to privacy is a right that allows citizens to control their personal information, body and location. Perderson proposes that in addition to portraits, names, personal space, secrets that you don't want to know and private information that can easily be misunderstood by others, friends' information, family information, and personal video and audio data should also be included in the privacy indicators in the new media age. In fact, it also shows that the essence of privacy is an individual's control over his own information. Luciano Floridi further points out that personal information refers to identity rather than ownership. "The concept of 'you' in 'your information' is different from the concept of 'you' in 'your car'. The former is more like the 'you' in 'your body', 'your feelings',' your memories', 'your thoughts' and' your choices'. It expresses the idea of a constitutive asset rather than external ownership.

To sum up, for the definition of personal information, some Chinese and foreign scholars use generalization and enumeration to define the scope of the concept of personal information, and some use abstract concepts to describe the attribute of the right of personal information. As for the infringement liability of artificial intelligence, it is mainly divided into three kinds: the responsibility of artificial intelligence itself, the responsibility of the user and the responsibility of the manufacturer. As for the identification of infringement fault and the remedy of the right of the information subject, there are theories such as "minimum collection of information principle", "informed consent principle" and "notice deletion rule". However,

how does the current academic community determine the specific behavior of artificial intelligence infringing on personal information, or whose behavior? How to divide the tort liability of manufacturers, users and even artificial intelligence itself? How to specifically examine the so-called "degree of necessity" for AI to collect, process and analyze information? How to further implement and amend the personal information right stipulated in the Civil Code in judicial practice and legislative supplement still exists a considerable ambiguity area which needs to be discussed and solved

Conceptual Framework

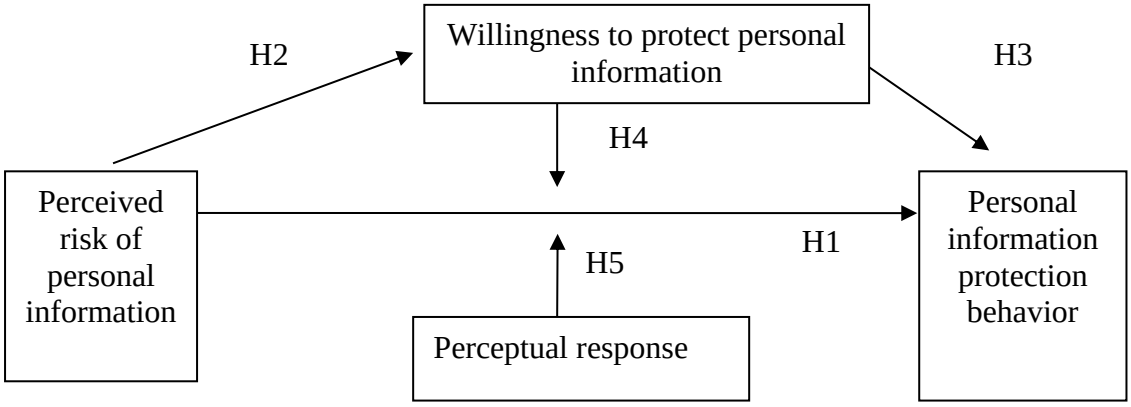

Figure 1 Research Framework

Research Methodology

Select research samples from the APP that processes personal information, and conduct in-depth research on the legal protection of personal information under the artificial intelligence environment.

The perceived risk scale of this study is mainly based on the research of Alan's perceived risk scale and is revised according to the characteristics of personal information in the AI environment.

This research on the willingness to protect scale is mainly based on the research of Kamil's willingness to protect scale and is revised according to the characteristics of personal information in the intelligent environment.

The Perceptual Response Scale of this study is mainly based on Henry's Perceptual Response Scale and is revised according to the characteristics of personal information in the AI environment.

The protective behavior scale in this study is mainly based on the Langer protective behavior scale and is revised according to the characteristics of personal information in the intelligent environment.

Research Results

Statistics and research are made on these relevant findings. Table 1 shows the research results. The average value of each dimension of perceived risk is close to 4.0, and the average value of overall body water is 3.91, which means that the perceived risk has reached a high level in general.

Table 1 Statistical Table of Perceived Risk Survey Results

level	The average	The standard deviation
Security threats	3.88	1.028
Privacy risks	3.93	1.030
Information stolen	3.92	1.130
As a whole	3.91	1.000

The independent sample t-test was used to analyze the gender differences of each level and the whole of perceived risk, and the results are shown in Table 2. It can be found from the table that the t value of each level of perceived risk and the overall gender does not reach a significant level, indicating that there is no obvious difference between many indicators of perceived risk and the overall gender.

Table 2 Difference analysis of variables based on gender

variable	gender	The mean	The standard deviation	p-value
Security	male	3.8776	1.05376	.071
threats	female	3.8720	1.00067	
Privacy risks				
Information	male			
stolen				
As a whole	female	3.9346	1.03631	.256
variable	male	3.9145	1.02340	
Security	female			
threats				
Privacy	male	3.9618	.99943	1.054
risksInformat	female	3.8788	1.06258	
ion stolen				
As a whole	male			
variable	female	3.9288	.99680	.573
	male	3.8851	.99940	

The age difference of each level and the whole of perceived risk was analyzed by using single factor variance, and the results are shown in Table 3. It can be found from the table that the t value of each level of perceived risk and the overall age reach a significant level, indicating that there are significant differences in each level of perceived risk and the overall age.

Table 3 Analysis of differences in variables based on age

level	age	The average	The standard deviation	p-value
Security	Under the age of 20,	3.0419	1.45645	
threats	20 to 25 years old	4.1633	.59799	.134
Privacy	26 to 30 years old	4.2569	.44454	
risks		4.1417	.57741	
Information stolen	More than 30 years of age			
As a whole				
level	Under the age of 20,			
Security	20 to 25 years old	3.0710	1.46694	
threats	26 to 30 years old	4.2082	.56947	.842
	More than 30 years of age	4.3007	.45317	

Privacy risks		4.2563	.53090	
Information stolen	Under the age of 20,			
As a whole level	20 to 25 years old			
Security threats	26 to 30 years old	3.0882	1.44161	
	More than 30 years of age	4.1933	.60408	.068
Privacy risks	Under the age of 20,	4.2876	.51613	
		4.2646	.56456	
Information stolen	20 to 25 years old			
As a whole level	26 to 30 years old			
Security threats	More than 30 years of age	3.0565	1.43494	
	age	4.2064	.50713	.034
	Under the age of 20,	4.2748	.40157	
	20 to 25 years old	4.2052	.51111	

Empirical analysis results this chapter discusses the impact of perceived risk, willingness to protect, and perceived response on personal information protection behavior on the basis of theoretical analysis. Based on data analysis and hypothesis testing, the theoretical hypothesis passes the test. The final test results are summarized in the following table.

Table 4 Hypothesis Analysis Results

No	**Assumptions**	**Results**
Hypothesis 1	Perceived risk of personal information has a significant impact on protection behavior	Supported
Hypothesis 2	Perceived risk of personal information has a significant impact on willingness to protect	Supported
Hypothesis 3	The willingness to protect personal information has a significant impact on protection behavior	Supported
Hypothesis 4	Willingness to protect plays an intermediary role between perceived risk and protective behavior	Supported
Hypothesis 5	Perceived response plays a moderating role between perceived risk and protective behavior	Supported

Discussion and Suggestions

With the development of the era of big data, the protection of personal information faces new challenges. The boundaries of personal information are blurred, the subject of infringement is difficult to determine, the means of infringement are diversified, and the protection of rights is difficult (X. Zheng & Z. Cai, 2020). Personal information leakage not only affects normal life, but also causes property damage and disturbs social order. For example, the recruitment website leaked the resume, the hospital leaked the patient's privacy information, the university student information leakage fraud suicide case, the personal information security problem needs to be solved (J. Lee, 2020).

In the practice of personal information protection, there are some problems, such as scattered legislation, unclear functions and powers of supervisory organs, weak attack force

and imperfect litigation mechanism. The enactment of the Civil Code has made a big step forward in the legislative protection of personal information, but there is still no special protection law for personal information (X. Cai, J. Wang, S. Zhong, K. Shi, & Y. Tang, 2020). In view of the problems existing in the legal protection of personal information in the era of big data, firstly, in terms of legislation, the right of personal information should be clarified, different rules of information processing should be formulated, the right of informed consent should be improved, and information processing should be made open and transparent (X. Cai, K. Shi, S. Zhong, & X. Pang, 2021). There should also be clear legislative regulations on face recognition technology in the era of big data. Secondly, it is to improve the judicial remedies for the protection of personal information. In view of the difficulty of proof, the burden of proof is reversed to improve the personal information infringement cases that damage social public welfare, and the public interest litigation system is used to deal with them (Y. Zou, W. He, L. Zhang, J. Ni, & Q. Chen, 2019).

Due to the lack of practical experience and theoretical knowledge, it does not go deeply into the related problems, and it still has some shortcomings in the analysis of the content of this paper. We can only throw forward some views and suggestions, hoping to provide help to our personal information protection work (Z. P. Cai, Z. B. He, X. Guan, & Y. S. Li, 2018). According to the legislative plan of the National People's Congress, the Personal Information Protection Law and the Data Security Law will be deliberated this year, which will build a personal information protection system and improve the current situation of personal information infringement.

Suggestions for this research

By learning from the experience of foreign industry organizations and combining with the actual situation in our country, we make user management rules in line with the development laws of the industry, and produce corresponding privacy protection guidelines. The content of the guide should include the following:

First, state the terms in advance. This clause is the prior commitment made by the intelligent technology provider, which promises whether to collect users' private information, the scope of collection and the purpose of use, that the use process of private information shall comply with legal provisions, that illegal sharing of private information to third parties shall be prohibited, that users' rights shall be safeguarded, and that the highest confidentiality measures shall be provided in the processing process.

Second is the user rights clause. Users' legal rights, such as the right to be forgotten, the right to know, the right to withdraw, and the right to carry information and data, should be clearly defined in the privacy information protection guide. The purpose of such clauses is to warn users of their rights.

Third, the classification protection clause. Classified protection classifies different types of privacy information related to users according to the degree of confidentiality, and provides specific classified protection schemes according to the types of privacy information. Classified protection has higher requirements for the protection of users' privacy information, but it meets the needs of both sides and is more scientific and reasonable.

Fourth, private information disclosure clause. Specify the details of the disclosure of private information to a third party, such as relevant laws; Clarify the specific purposes and procedures used by third parties to ensure transparency of disclosure.

Fifth, personnel training standard clause. In fact, the staff of intelligent service providers really master the privacy information of users on the platform, so they have high requirements on the quality of employees, requiring them to conduct professional training on the laws and regulations of privacy information, privacy information protection technology, etc. It is necessary to clearly stipulate the punishment measures when information is leaked,

including the method and scope of punishment, which should be consistent with the profit revenue, so as to ensure the reasonable and safe use of users' privacy information.

References

Cheng Xiao (2020). On the Nature of Personal Information Rights and Interests in China's Civil Code. Politics and Law, 6(08), 2-14.

Cheng Xiao (2016). On civil liability for infringement of personal Information. Hainan Journal (Philosophy and Social Science edition), 42(02), 39-47.

Gao Zhiming (2016). The Attribute and Constitution of Personal Information Right. Journal of Qinghai Normal University (Philosophy and Social Science Edition), 12(05), 2-13.

Hong HAilin (2016). The legislative concept of personal information protection is explored between information protection and information circulation. Hebei Law School, 3(01), 108-113.

He Nurturing (2016). Personal information protection of consumers in online transactions. China Circulation Economy, 8(03), 38-49.

J. Lee (2020). "Access to finance for artificial intelligence regulation in the financial services industry," *European Business Organization Law Review*, vol. 21, no. 4, 731–757.

Qin Qian (2021). On the right basis of personal Information protection. Journal of Chongqing University, 27(09), 1-13.

Qi Aimin (2019). Personal Information Protection Law of the People's Republic of China. Hebei Law School, 37(01), 33-45.

Shi Bin (2020). Path selection and reconstruction of APP personal Information protection. People's Forum, 3(15), 146-147.

The legislative path of civil confirmation of personal information right -- comment on article 111 of General Principles of Civil Law. Journal of North China University (Social Science Edition), 20(06), 65-73.

Wang Liming (2021). Personal dignity: the primary value of personality right in civil Code. Contemporary Law, 35(01), 3-14.

Wang Liming (2016). On the legal protection of personal Information right -- The center is the division between personal information right and privacy right. Modern Law, 21(03), 38-47.

X. Cai, J. Wang, S. Zhong, K. Shi, & Y. Tang (2020). "Fuzzy quantized sampled-data control for extended dissipative analysis of T–S fuzzy system and its application to WPGSs," *Journal of the Franklin Institute*, vol. 358, no. 2. 1350–1375.

X. Cai, K. Shi, S. Zhong, & X. Pang (2021). "Dissipative sampled-data control for high-speed train systems with quantized measurements," *IEEE Transactions on Intelligent Transportation Systems*, no. 99. 1–12.

X. Zheng & Z. Cai (2020). "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, 968–979.

Y. Zou, W. He, L. Zhang, J. Ni, & Q. Chen (2019). "Research on privacy protection of large-scale network data aggregation process," *International Journal of Wireless Information Networks*, vol. 26, no. 3, pp. 193–200.

Z. P. Cai, Z. B. He, X. Guan, & Y. S. Li (2018). "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590.

Zhang Xinbao (2015). From Privacy to Personal Information: Theory and Institutional Arrangements for benefit Remeasurement. Chinese Law Journal, 4(03), 38-59.

Zhou Hanhua (2016). Exploring the way of personal data governance with incentive compatibility -- the legislative direction of Personal Information Protection Law in China. Law Studies, 40(02), 3-23.

Zhang Li 'an, Han Xuzhi (2016). Private law attribute of personal information right in big data era. Law Forum, 31(03), 119-129.