Criminal Law Protection Boundary and Legislation Construction Strategy of Citizens ' Personal Information in the Era of Artificial Intelligence

Wang Wei[1]

[1]Associate Professor. Institute of Rule of Law, Shandong Agricultural University, Shandong, Taian, 271018.Email: 271849006@qq.com.

Abstract : Due to the influence of the Internet age, citizens' personal information is often maliciously stolen, illegal trafficking and infringement, which makes the personal information security of citizens seriously damaged. Therefore, in the era of artificial intelligence, this paper puts forward the criminal law protection boundary and legislative construction strategy of citizens ' personal information. Using the boundary of civil tort and criminal offenses and the boundary of administrative illegality and criminal offenses, this paper analyzes the boundary of crime and non-crime of infringing citizens ' personal information. Combining with the boundary of criminal law, this paper analyzes the criminal law protection boundary of citizen personal information in the era of artificial intelligence. By improving the technical means of the judiciary and adopting diversified dispute resolution mechanisms, the judicial protection of personal information from the perspective of artificial intelligence is strengthened. By strengthening the supervision of personal information protection, establishing and improving the self-regulatory organizations of the information industry and using blockchain technology to regulate, the supervision and regulation of citizens' personal information protection are carried out. At the same time, the construction strategy of citizen personal information legislation is given to avoid the violation of citizen personal information and ensure the safety of citizen personal information.

Key words : the era of artificial intelligence ; personal information of citizens ; criminal law protection boundary ; legislative construction strategy ;

Tob Regul Sci.™ 2022; 8(1): 666-679
DOI: doi.org/10.18001/TRS.8.1.58

In today's social development, the reform of science and technology and the application of network ushered in the era of artificial intelligence. Artificial intelligence technology has gone through nearly ten years of development from the beginning to the vigorous development stage. In the 21 st century, artificial

intelligence technology is at the peak stage of development, with which is illegal infringement of citizens ' personal information[1]. In the era of artificial intelligence, collecting, processing and integrating personal information is a very simple thing, and it is not easy to find, so that the personal information of citizens is maliciously violated [2]. At present, the domestic laws and regulations related to the application of artificial intelligence technology to the protection of personal information of citizens are not detailed enough, and there is no specific legislative organization to protect the personal information of citizens, resulting in some judicial organs in the adjudication of specific personal information protection cases there is no law that can be used to basis[3]. Some supervision and management subjects in society lack the attention to the supervision of citizens ' personal information, resulting in the plight of relief after the invasion of citizens ' personal information.

In the era of artificial intelligence, many emerging technologies and the Internet industry have gradually risen and expanded, which has increased the risk of citizens' personal information leakage[4]. There is a close relationship between the personal information of citizens and any stage of the development of artificial intelligence. The development of artificial intelligence is inseparable from the collection of information. It is necessary to establish a personal information database for every citizen to analyze data in various industries to meet the individual preferences of different users.[5] Ensure its personal information security. In order to stand out in the fierce social competition, artificial intelligence technology must have the function of analyzing and processing information. Some information without accurate recognition can become accurate recognition information after processed by artificial intelligence technology. In this context, the phenomenon of over-collection of citizens ' personal information has emerged, and its weaknesses in security protection have gradually emerged, leaving no trace of omission.Infringement of personal information rights can be divided into infringement of personality rights and infringement of property rights. Data mining and analysis are the main trend of current social development, which is conducive to the in-depth grasp of customer preference information in various industries and the better

[1]Yu Chong.The legal interest attribute and conviction boundary of ' citizen personal information ' in the crime of infringing citizen personal information [J].Politics and law, 2018 (4) : 15-25.

[2]Jiang Yaowei. The boundary of criminal law protection of personal information of citizens in the era of big data - centered on the substantive interpretation of ' violation of relevant provisions of the state ' [J]. Journal of Chongqing University : Social Sciences, 2019 025 (001) : 152-161.

This work was supported by National Social Science Fund Youth Project “Ethical Basic Research on Personality Right Confirmation” (17CFX026), Shandong Social Science Planning Research Project " Food and Drug Safety Administrative Law Enforcement and Criminal Justice Linkage Mechanism Empirical Study in Shandong Province" (19CFZJ26).

[3]Jing Lijia. The legal interests of the crime of violating citizens ’ personal information in the bigdata environment should be turned. [J] Legal review, 2018, 036 (002) : 116 – 127.

[4]Ma Xiao, Di Xiaohua. Study on the Limits of Criminal Law Protection of Personal Information of Citizens [J]. Jiang Hai Journal, 2019,000 (002) : 231-237.

[5] Cheng Lei.Citizen personal information protection in criminal justice [J].Journal of Renmin University of China, 2019, 33 (01) : 110-119.

provision of related products and services. However, it is necessary to pay attention to the protection of users' personal privacy and the use of data within a reasonable and legal range. Once the citizen 's personal information has been illegally infringed, its impact is at the same level as that of the citizen 's personal safety and property safety, which means that the infringement of information also needs the attention of the relevant departments, and it needs to be stopped in time when the infringement occurs, prevented before the infringement occurs and relieved after the infringement occurs. However, the domestic relief effect on citizens' personal information after being invaded is not ideal, and there are relatively few relief ways. For the legislative perspective of citizens ' personal information, China has not yet carried out legislative protection of citizens ' personal information in the era of artificial intelligence, and relevant provisions on legislative protection are scattered in different laws and regulations[6].

According to the above background analysis, citizens' personal information has been seriously violated in the era of artificial intelligence, and it needs to be fully protected. Therefore, in the context of the era of artificial intelligence, it is of far-reaching significance to study the criminal law protection boundary and legislative construction strategy of citizens' personal information.

1.The boundary of criminal law protection of citizens' personal information

(1) The boundary between crime and innocence of infringement of citizens' personal information

1. Boundary between civil violations and criminal offences

The definition of a criminal act is that the act has a negative impact or infringement on the interests of persons or things within the scope of legal protection, and there is a risk of infringement. First of all, the harmful results of citizens ' personal information violations and criminal acts are the most basic criteria to determine whether violations of citizens ' personal information have been violated. No crime does not mean no crime, there is a certain threat or risk is also considered to be a violation of personal information. The crime of infringement of citizens ' personal information is objectively mainly manifested as trafficking, theft, providing and other ways to obtain[7] . However, in general, the infringement of citizens ' personal information refers to the illegal collection, use and processing of collected information, illegal trafficking through certain means of transmission and disclosure of citizens ' personal information. It can be seen that both of them exist independently in other aspects, regardless of subjective or objective factors, in addition to the similarities in the links of sale, illegal acquisition and supply[8]. Therefore, behavior is an important standard to judge whether a crime is committed, and the intersection of subjective factors and

[6]Guo Zeqiang, Zhang Xinxi. Get out of the myth of protecting the legal interests of the crime of infringing citizens ' personal information - the promotion of super personal legal interests [J]. Tianfu New Theory, 2020 (3) : 93-101.

[7]Chen Wei.The reflection and construction of juvenile recidivism criminal legislation on adult legal issues [J].Jinan Journal : Philosophy and Social Sciences Edition, 2018, 40 (2) : 26-36.

[8]Zhang Yong.The fragmentation and systematic interpretation of the criminal law protection of citizens ' personal information [J].Social Science Editorial, 2018 (2) : 86-93.

objective factors in behavior can reflect the interoperability and integrity of the legal system. If the intersection of the two factors is difficult to judge, the severity of the consequences needs to be taken into account.

Secondly, the infringement of personal information behavior in the subjective sense is mainly from the infringer in the subjective sense whether can realize the illegality of the infringement of personal information behavior, whether can actively investigate the consequences caused by the infringement of personal information behavior, investigate the concealment of the means used by the infringement of personal information behavior. In the aspect of infringement of citizens ' personal information, not only includes the leakage and trafficking of personal privacy information, in each data platform, citizens should have the right to query, delete and change the submitted and published personal information. Each platform should not hinder citizens ' reasonable and legal information personality rights for any reason, otherwise they can be regarded as violations. Compared with the criminal law, the civil law has relatively low coercive force and deterrence on whether the tort is a civil act or a criminal offence. If the actor is allowed to bear civil liability in a mild way, it cannot achieve the desired effect and cannot curb the infringement of personal information. Therefore, it must be regulated by the criminal law. In addition, other criminal incidents are likely to arise in the context of malicious theft and trafficking of personal information, usually the last part of this illegal industrial chain is the crime of information fraud.For example, Song Mou, the defendant in a fraud case, bought a large number of college students ' information on the Internet, and disguised it as the financial department staff of the school where the victim was located. He defrauded CNY 6,000 yuan in total on the ground that the grant of the grant required deposit. In this case, the criminal suspect connected the victim with a large amount of information obtained through the acquisition, and fabricated false events according to the identity and living environment of the victim to obtain the victim ' s property. This behavior transformed the personal information infringement into the personal property security infringement, which posed a certain degree of threat to the victim ' s property security and had reached the conviction standard of personal information infringement. Therefore, the treatment of personal information violations should be in accordance with the same sentencing methods as property security violations.

Finally, victims of violations of citizens ' personal information may discover the possibility of the perpetrator and claim their rights . Civil litigation, in other words, is self-prosecution, which requires a clear defendant, when the victim 's personal information has been violated, can be timely and clearly locked in violations of citizens ' personal information perpetrators, otherwise, can not successfully start civil relief procedures. If the actual situation of the violation of personal information of citizens, civil remedies for victims, will lead to specific violations of personal information of citizens difficult to find, which requires the protection of criminal law to give full play[9]. If it is considered from the perspective of the victim and the infringer respectively, there is no way to obtain a balanced solution, resulting in the

[9]Jia Yuan, Liu Renwen. Connotation, extension and benchmark : criminal law protection of citizens ' personal information [J]. Journal of Shandong Police College, 2019,031 (001) : 36-43.

lack of fairness and legitimacy of the final results. At this time, it is necessary to play the role of criminal law in the protection of citizens ' personal information and actively protect the victims ' personal information rights.

2. Boundary between administrative violations and criminal offences

Criminal crime has dual illegality. We must correctly handle the relationship between criminal illegality and administrative illegality, prevent excessive expansion of penalty power, and confuse the boundary between criminal illegality and administrative illegality.

According to the nature of criminal illegality and administrative illegality, in terms of the relationship between the two, it is generally believed that the harm of criminal illegality to society is far greater than that of administrative illegality, and the degree of illegality is relatively large. Scholars in the academic circle believe that the nature of criminal law and administrative law should be distinguished according to the nature of different legal interests, and the scope of punishment of criminal law should be delimited by the substantive judgment of legal interests, so as to avoid expanding the area of punishment for violations of citizens ' personal information. The legal benefits of administrative law in the process of protection are relatively abstract, and the legal benefits protected by criminal law have exceeded the scope of administrative law.

For the infringement of citizens ' personal information, judging whether the infringement of citizens ' personal information is a criminal crime or an administrative violation, mainly from the means of behavior, consequences, plot and amount of factors. For example, when considering the factors of behavioral means, the relationship between the two should be clarified. Those who hinder the national staff from performing their official duties according to law, or use violence, threats and other methods that constitute serious consequences should be judged as criminal offenses, while those who do not use violence threats and other methods should be classified as administrative offenses. While considering the amount factor, it should be judged according to the relevant provisions of the relevant laws. When the amount of money involved in some crimes reaches the ' larger ' standard, it should be divided into criminal offences, otherwise it should be attributed to administrative violations.In addition, in the process of illegal judgment, factors such as means of behavior, consequences, plot and amount should be comprehensively analyzed. This is because illegal behavior may not only involve one factor, but often appear in a state of coexistence of multiple factors. Once several people are separated, it is easy to lead to the problem of excessive or light punishment, causing inconvenience for law enforcement personnel to work. Therefore, it is necessary to comprehensively analyze multiple factors to determine the type of crime. In addition, the essence of crime is an infringement of legal benefits. If the infringement of citizens ' personal information only violates administrative norms and does not violate specific legal benefits, it can be regarded as an administrative illegal act. Both administrative violations and criminal acts that violate citizens ' personal information are within the scope of public law, and there are overlaps in the legal constitution, which makes it difficult to distinguish between punishment and administrative punishment. In this case, legislators and institutional designers need to continue their efforts later to make the

difference between the two clearer and to make the division of their boundaries clearer.

(2) Keeping the boundaries of criminal law

Law is a very serious field. Once the applicable law has a wrong understanding of the boundary of the criminal law and ignores the boundary of the criminal law, it will lead to the emergence of miscarriages of justice, which is not conducive to fair justice, but also leads to the emergence of social injustice. Therefore, it is necessary to keep the boundary of the criminal law and make the problem of the criminal law reasonably explained from the perspective of the criminal law. According to the degree of punishment, property punishment belongs to lighter civil punishment, administrative punishment is relatively lighter, including not only short-term freedom punishment, but also property punishment, which can be used as a transitional punishment ; and criminal punishment is a more serious way of punishment, according to the provisions of China ' s criminal law, criminal punishment mainly includes two parts, mainly punishment and additional punishment. The principal punishment mainly includes fixed-term imprisonment, life imprisonment, death penalty and other penalty methods, and the supplementary punishment includes fine, deprivation of political rights or confiscation of property. Thus, once a criminal offence is penalized, the perpetrator is not only deprived of life and liberty, but also of property[10] .

From the perspective of social governance, criminal law belongs to the most severe legal means in all means of social governance. Because of its severity, the state cannot use criminal law at will to regulate other legal acts that can effectively prevent or do not pose a fundamental threat to the normal operation of other legal systems. Moreover, crime is a complex phenomenon caused by various reasons. Therefore, it is unrealistic to punish and eliminate crime by adopting severe punishment method. Therefore, criminal law should be regarded as the final means of legal interest protection, and the consequences of judicial judgment should be paid attention to. If the criminal law must be used, the state should try to avoid harm to citizens, choose the method that has the smallest harm to the basic human rights of citizens, and objectively evaluate the results of a certain judgment and its social impact. In terms of criminal acts that violate citizens ' personal information, the expansion of criminal law charges will also lead to a shrinking phenomenon of citizens ' personal information freedom, affect people 's freedom of expression, and cause a panic atmosphere in society to stimulate social contradictions. Therefore, it is necessary to keep the boundaries of criminal law and avoid such problems. And the guarantee attribute of criminal law determines that criminal law can only passively deal with the crime of infringing citizens ' personal information behavior, rather than actively involved in the lives of citizens, in order to put all the legal benefits of infringement under their own protection. However, for those behaviors that are bad and seriously endanger the society, the criminal law must stop, correct and give due sanctions to safeguard social fairness and justice and eliminate the hidden dangers that threaten social security.

From the above analysis, it can be seen that the criminal law must conform to the concept of prudent

[10]Zhang Yang. On the Criminal Law Protection of Personal Information in Cyberspace [J]. Zhongzhou Journal, 2018 (8) : 58-62.

justice and strictly abide by its own boundaries. Especially in the new era, people ' s requirements for judicial justice are getting higher and higher, which puts forward higher requirements for the confirmation of related criminal acts. In this case, the significance of strictly adhering to the boundaries of the criminal law is more prominent and must be paid enough attention.

2.Citizen personal information legislation construction strategy

(1) Strengthening the judicial protection of personal information from the perspective of artificial intelligence

1. Technical means to improve the judiciary

With the development of science and technology and the arrival of the era of artificial intelligence, the problem of personal information security of citizens has attracted more and more attention. The diversity of means of stealing personal information and its concealment and untraceability pose a great challenge to the work of the judiciary [11].Therefore, strengthening the judicial protection of personal information from the perspective of artificial intelligence, combined with today ' s artificial intelligence technology, improve the technical means of the judiciary.

The biggest problem faced by the judiciary is the forensics of personal information theft. Therefore, in order to improve the technical means of the judiciary, first of all, it is necessary to use artificial intelligence technology to construct the management system of the judiciary, and focus on the forensics link. Combined with the current artificial intelligence technology, the whole process of personal information infringement is reviewed, and the operation process of the information operator is accurately controlled to achieve the purpose of accurate forensics[12]. Artificial intelligence technology is applied to judicial proceedings to solve simple disputes online. The application of artificial intelligence technology to the evidence judgment of the judiciary provides help for judges to adopt expert evidence, collect evidence in time, and effectively assist in evidence judgment through multi-party cooperation.

The application of artificial intelligence in evidence judgment should follow the auxiliary principle, the limitation principle and the refutable principle, so as to avoid the deviation or even miscarriage of justice caused by uncertain factors. Artificial intelligence can be applied to formal constraints, according to the law, judicial process, etc., to determine whether the evidence meets the formal specification, determine whether the inquiry notes meet the procedural requirements, determine whether the physical evidence has a list of notes, etc. The application of artificial intelligence technology in evidence judgment focuses on the protection of personal information such as evidence. Combined with information encryption methods, such as key transmission, encryption protocol, identity authentication, electronic signature and other technologies, the key personal information in evidence retained in the management of the judiciary is

[11]Gao Chunan. Reanalysis and expansion of the legal interests of citizens ' personal information from the perspective of criminal law [J]. Chinese Journal of Criminal Law, 2019,002 (002) : 87-96.

[12]Zheng Yufeng. Research on crimes against personal information of citizens in the era of big data [J]. Guangxi Social Sciences, 2018, 278 (08) : 117-122.

encrypted to facilitate storage and transmission.

Strengthen the database management technology of the judiciary to ensure the safety of personal information in the database. The database of the judiciary stores a large number of case information. The rise of artificial intelligence technology brings great challenges to the database management of the judiciary. The application of a variety of database security techniques, such as blockchain, hybrid dynamic data encryption, ciphertext coding, timestamp authentication, has important practical significance for the personal information security and leakage prevention of the judicial authority database. In addition, it is necessary to apply artificial intelligence technology to real-time monitoring of the management system of the judiciary, find problems, timely forensics, and effectively improve the technical means of the judiciary through multi-party cooperation.

2. Diversified dispute resolution mechanisms

The application development of artificial intelligence requires a large number of personal information, which enhances the degree of information sharing. Personal information contains the characteristics of commercialization, with high economic value, resulting in illegal collection and transaction of personal information crime. The scope of personal information collected has gradually escalated from static basic information, and a large number of IP addresses, network browsing traces and positioning information have been leaked. Using artificial intelligence technology, personal information has been deeply excavated, bringing great challenges to personal information security. In view of the huge litigation pressure faced by information manipulators when they use artificial intelligence technology to violate personal information, the judicial authorities should combine the actual situation of the current society and adopt diversified ways to establish a dispute resolution mechanism. Improve the legal basis of personal information, the introduction of judicial interpretation of personal information protection, increase the scope of legal protection, increase the litigation system of citizens ' personal information infringement, give criminals a strong deterrent. For individual information violations, litigation costs are too high, litigation procedures are numerous, resulting in many people give up rights litigation, the judiciary should play a law enforcement function. Since the process of obtaining personal information by information manipulators is batch, individual personal information can be subject to collective litigation, which can reduce the cost of individual litigation and maintain personal information security. The judicial organs should simplify the procedure of litigation, provide a window for handling cases, reduce litigation links, and make the proceedings more humanized. Second, popularize relevant laws.At present, China ' s citizens ' awareness of personal information infringement is relatively weak. There are many terms for the use of mobile software protocols to collect user personal information from multiple dimensions, and even user information collected by software involves personal photos, property information, biometric information, financial transaction records, network browsing records, etc. Especially, it is difficult for minors to find illegal access to personal information. When using family intelligent equipment, personal information is violated. Wearable equipment excessively collects user health data and residential information. At this time, relevant law enforcement departments need to increase the publicity of relevant laws and popularize

citizens ' awareness of personal information protection[13]. Law enforcement should also be strengthened to limit violations of such mobile software. The use of diversified dispute resolution mechanisms to prevent violations of personal information from the root.

(2) Supervision and Regulation of Personal Information Protection from the Perspective of Artificial Intelligence

1. Strengthening the supervision of personal information protection

Artificial intelligence technology promotes human development and progress, but also brings great hidden dangers to the safety of personal information. Simple personal information protection can not meet the current social situation. Lack of supervision has caused great risk to personal information security. Therefore, in order to effectively strengthen the supervision of personal information protection and solve the problem of low efficiency of lack of supervision, the following aspects should be done.

First, set up special personal information supervision mechanism.

In today ' s artificial intelligence era, more and more countries have established personal information supervision departments. China has not paid enough attention to the protection of personal information. At present, it is still in the stage of decentralized supervision, and it is completely incompatible with the actual situation in the era of artificial intelligence. At present, the supervision mechanism of personal information in foreign countries has been relatively mature, such as the ' European Parliament and Council Directive 95 / 46 / EC on personal protection involving personal data processing and free circulation of such data ' promulgated by the European Union in 1995 and the ' General Data Protection Regulations ' (GDPR) promulgated in 2018, which gives a relatively comprehensive provision for the protection of personal information in the intelligent era. At the same time, it emphasizes the protection of personal information and standardizes the circulation and utilization of information in relevant departments. Compared with the EU, the US has more relaxed protection of personal information. Looseness here does not mean contempt and laissez-faire about citizens ' personal information protection, but rather the introduction of scenario-led personal letters.That is, to make a reasonable judgment on the supervision of personal information protection in different work scenarios or demand environments, if there is a mistake in the supervision of personal information protection in this scenario, it is necessary to inform the upper disposal institutions in a timely manner, and convey to third-party platforms, enterprises or relevant departments in an appropriate manner whether they need to bear the corresponding risks and how they wish to choose to reduce the risks. Based on the above information protection measures of developed countries, it can be seen that in the process of personal information supervision, relevant mechanisms need to be balanced as much as possible, that is, to grasp the relaxation of personal information supervision[14]. Therefore, China should learn from the advanced experience of developed

[13]Li Jingran, Wang Suzhi.Research on the plot elements and quantitative standards of the crime of infringing citizens ' personal information [J].Law application, 2019,426 (09) : 71-78.

[14]Wang Qiangjun, Guo Rongyan. Rational thinking on criminal law protection of personal information [J]. Journal of Shenyang University of Technology : Social Sciences, 2018, 011 (004) : 297-306.

countries, set up special personal information supervision mechanism, and combine the technical means of judicial organs to effectively protect personal information security. The personal information supervision mechanism should be directly managed by the central government to avoid weakening security through multi-level organizational relations and ensure the smooth development of the personal information supervision mechanism.

Second, establish a sound regulatory rules and regulations.

At present, most enterprises ' personal information is in a state of lack of supervision. Even if some enterprises establish the corresponding regulatory system, there are problems of poor supervision and weak standardization, which makes information operators can arbitrarily steal personal information and make personal information violated. Therefore, in order to ensure the security of personal information, perfect regulatory rules and regulations should be established. First of all, a comprehensive surveillance system is constructed to monitor personal information in real time, prevent personal information infringement, and track personal information loss. Secondly, the use of risk assessment departments to establish a sound personal information loss survey system, the full range of personal information protection. Finally, laws and systems are used to regulate supervision. From the perspective of legislation, relevant laws on personal information protection are formulated, the subject of responsibility is clarified, the rights and obligations of the protected and the subject of responsibility are divided, and a unified management and relaxed executing agency is established to form normative regulatory rules and regulations.

Third, improve the regulatory efficiency of personal information.

The information of citizens in the artificial intelligence environment is seriously threatened. There are many means and methods for information operators to obtain personal information, and the number is complex and difficult to control. Man-made information supervision has long been unable to meet the effective supervision of personal information. An advanced personal information supervision system should be introduced to carry out penetrating supervision of personal information. Once the illegal use of personal information is found and confirmed, it is necessary to execute it in accordance with the law and punish it strictly in the first time. In response to specific problems, timely countermeasures should be given, such as the disclosure of personal information of consumers in the era of artificial intelligence. Once confirmed, it is necessary to collect personal information institutions or operators to assume corresponding responsibilities and penalties to further improve the efficiency of supervision.

2. Establishment and improvement of self-regulatory organizations in the information industry

With the rapid development of artificial intelligence technology, relevant laws and regulations are obviously lagging behind. The infringement of citizens ' personal information cannot be timely protected. Therefore, China should establish a sound self-regulatory organization in the information industry, learn from the advanced experience of developed countries, and coordinate with China ' s actual national

conditions[15]. The government should carry out macro-control to protect the safety of citizens ' personal information in the era of artificial intelligence. This requires not only that the state needs to develop relevant information supervision mechanisms to effectively guide the protection of personal information, but also that relevant departments such as enterprises and third-party platforms need to appropriately modify and supplement privacy protection policies within the internal affordability, and take the initiative to assume the responsibility of information protection. In this process, it can not only realize the multi-protection of personal information within enterprises, but also win a good reputation for enterprises in the market.

Firstly, the artificial intelligence organization association is constructed by the government. It is helpful to lead more companies in the field of artificial intelligence to join by requiring companies that are outstanding in the field of artificial intelligence. The core idea of industry self-regulatory organizations is self-discipline, and the use of core forces to protect personal information security.

Secondly, build a perfect artificial intelligence industry behavior norms. According to the actual situation of the domestic artificial intelligence era, as well as the relevant laws and regulations of the personal information protection judiciary, the behavior norms suitable for the development of artificial intelligence industry are formulated. The establishment of behavioral norms in the artificial intelligence industry helps to constrain the illegal behavior of the industry and help protect the personal information of citizens. Members of AI Association can formulate rules and regulations applicable to the company according to AI behavior norms and the actual situation of the company.

Finally, improve the artificial intelligence industry self-regulatory organization. The government shall formulate relevant certification systems for relevant enterprises, evaluate them according to stages, give recognition to enterprises with better performance, and give relevant government support to enterprises, and punish enterprises with poor performance. Through the government macro-control, the formation of a benign competitive environment, so as to improve the information industry self-regulatory organizations.

The development of artificial intelligence technology and the safety of citizens ' personal information complement each other. To establish a sound self-regulatory organization of the information industry to promote the benign development of the artificial intelligence industry, and to better ensure the safety of citizens ' personal information in the era of artificial intelligence through internal and external measures.

3. Regulation using blockchain technology

The core of blockchain technology is to ensure the safety of information, so that personal information cannot be obtained and tampered without authorization. Individuals and artificial intelligence enterprises should register account information through blockchain. When individuals use artificial intelligence equipment, they first pass information to blockchain to prevent information from being violated. The

[15]Liu Xianquan. Foundations and limits for criminal law protection of artificial intelligence products [J]. Journal of East China University of Politics and Law, 2019,022 (006):60-67.

specific operation principle is as follows. After uploading personal information to blockchain, artificial intelligence enterprises manage it. However, in the management process, enterprises do not authorize any operation on personal information, so as to ensure the safety of information. Blockchain technology has anonymous attributes, and information uploaded to the blockchain is relatively independent and cannot be accessed by each other. Using blockchain technology to regulate, so that everyone can control their personal information and avoid the information security problems caused by the infringement of personal information. At the same time, artificial intelligence enterprises can also use personal information legally under the regulation of blockchain technology to realize the sustainable development of enterprises.

The asymmetric public key and private key encryption technology in blockchain technology is used to solve the problems of personal information disclosure and tampering. Public and private keys in blockchain can encrypt personal information. In encryption, the use of private key encryption, public key decryption, by verifying the user information of the private key owner, in order to prevent the private key owner login information is tampered with. Through private key decryption, personal information can be transmitted to the public key owner. With the support of blockchain technology, the information address corresponds to the corresponding private key. When modifying or editing the information in the address, it needs to be authenticated by the owner of the private key before it can be enabled. Citizens can use public key by anonymous or public name, and can access their personal information.

The intelligent contract of blockchain can also be used to protect personal information. First, personal information data and events need to be input into the contract to determine whether they meet the original contract conditions and confirm that the code on the back chain can be continuously and automatically executed. According to citizens ' personal information, determine the corresponding authorization or contract, and automatically take different protection measures according to different levels of privacy information. Using intelligent contracts, strict control is carried out according to the level of personal information, and big data and data mining are used to obtain the possibility of personal information of citizens, so as to reduce the risk of readers ' personal information disclosure.

In personal information protection, blockchain technology is combined with crawlers and big data to analyze and identify violations. When citizens publish personal resumes or personal login information on the Internet, if others illegally steal relevant information files of citizens, the use traces of information files are recorded through blockchain technology, and the stolen files are analyzed to determine whether they constitute infringement. At the same time, combined with the crawler and big data analysis, the damage caused by infringement of citizens is analyzed dynamically to determine the amount of compensation for infringement of victims.

On the basis of blockchain technology, identity authentication technology can also be added to prevent the disclosure of personal information through data authentication, identity documents and biometrics. At the same time, in order to prevent authentication information from being tampered with by others, the user certificate is generated by matching the user certificate with the public key. When the private key of authentication information is consistent with the public key of user certificate, personal information can be modified.

3. Concluding remarks

The personal information of citizens is affected by the network era, resulting in serious harm to the personal information security of citizens. Therefore, this paper puts forward the criminal law protection boundary and legislative construction strategy of personal information of citizens in the era of artificial intelligence. In the era of artificial intelligence, the boundary of criminal law protection of citizen ' s personal information is analyzed by using the boundary of crime and non-crime of infringing citizen ' s personal information and keeping the boundary of criminal law. Through strengthening the judicial protection of personal information from the perspective of artificial intelligence, improving the technical means of judicial organs, adopting diversified dispute resolution mechanism, the supervision and regulation of citizen ' s personal information protection, strengthening the supervision of personal information protection, establishing and improving the self-discipline organization of information industry, and using block chain technology to regulate, the legislative construction strategy of citizen ' s personal information is given to ensure the safety of citizen ' s personal information.

References

[1]Yu Chong.The legal interest attribute and conviction boundary of ' citizen personal information ' in the crime of infringing citizen personal information [J].Politics and law, 2018 (4) : 15-25.

[2]Jiang Yaowei. The boundary of criminal law protection of personal information of citizens in the era of big data - centered on the substantive interpretation of ' violation of relevant provisions of the state ' [J]. Journal of Chongqing University : Social Sciences, 2019 025 (001) : 152-161.

[3]Jing Lijia. The legal interests of the crime of violating citizens ' personal information in the big data environment should be turned. [J] Legal review, 2018, 036 (002) : 116 – 127.

[4]Ma Xiao, Di Xiaohua. Study on the Limits of Criminal Law Protection of Personal Information of Citizens [J]. Jiang Hai Journal, 2019,000 (002) : 231-237.

[5]Cheng Lei.Citizen personal information protection in criminal justice [J].Journal of Renmin University of China, 2019, 33 (01) : 110-119.

[6]Guo Zeqiang, Zhang Xinxi. Get out of the myth of protecting the legal interests of the crime of infringing citizens ' personal information - the promotion of super personal legal interests [J]. Tianfu New Theory, 2020 (3) : 93-101.

[7]Chen Wei.The reflection and construction of juvenile recidivism criminal legislation on adult legal issues [J].Jinan Journal : Philosophy and Social Sciences Edition, 2018, 40 (2) : 26-36.

[8]Zhang Yong.The fragmentation and systematic interpretation of the criminal law protection of citizens ' personal information [J].Social Science Editorial, 2018 (2) : 86-93.

[9]Jia Yuan, Liu Renwen. Connotation, extension and benchmark : criminal law protection of citizens ' personal information [J]. Journal of Shandong Police College, 2019,031 (001) : 36-43.

[10]Zhang Yang. On the Criminal Law Protection of Personal Information in Cyberspace [J]. Zhongzhou Journal, 2018 (8) : 58-62.

[11]Gao Chunan. Reanalysis and expansion of the legal interests of citizens ' personal information from the perspective of criminal law [J]. Chinese Journal of Criminal Law, 2019,002 (002) : 87-96.

[12]Zheng Yufeng. Research on crimes against personal information of citizens in the era of big data [J]. Guangxi Social Sciences, 2018, 278 (08) : 117-122.

[13]Li Jingran, Wang Suzhi.Research on the plot elements and quantitative standards of the crime of infringing citizens ' personal information [J].Law application, 2019,426 (09) : 71-78.

[14]Wang Qiangjun, Guo Rongyan. Rational thinking on criminal law protection of personal information [J]. Journal of Shenyang University of Technology : Social Sciences, 2018, 011 (004) : 297-306.

[15]Liu Xianquan. Foundations and limits for criminal law protection of artificial intelligence products [J]. Journal of East China University of Politics and Law, 2019,022 (006):60-67.