ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

Research on Countermeasures of Personal Information Disclosure in Network Society

Haoran Fu[1, a, *], Huahui Li[2, b] and Weiwei Fu[1, c]

[1]School of Economics, Anyang Normal University, Anyang, China.

[2]School of Mathematics, Anyang University, Anyang, China.

[a]hao3681@foxmail.com, [b]853391460@qq.com, [c]798818768@qq.com

Abstract

Information security is the foundation of national security, and personal information security is the top priority of information security. At present, there is a serious problem of personal information disclosure in our country, but there is no perfect solution. In view of this situation, this paper classifies and combs the main ways of information disclosure on the basis of studying the harmfulness of disclosure and the importance of protection. The reasons for personal information disclosure are analyzed and further improvement measures are proposed. The research will provide reference for better solving the problem of personal information disclosure.

Keywords

Personal Information, Information Disclosure, Information Protection.

1. PROTECTING PERSONAL INFORMATION IS IMPERATIVE

In recent years, with the development of science and technology and the innovation of network technology, personal information security is in trouble while enjoying the great convenience of personal life. The data leakage level index survey report shows that the total data leakage in the first half of 2016 increased by 15% compared with the second half of 2015. In the first half of 2016, 974 data leakage events were exposed, and the total number of data leakage records exceeded 554 million. In 2016, public security organs across the country cracked more than 2,100 cases of online infringement of citizens' personal information, seized more than 50 billion pieces of citizens' personal information and arrested more than 5,000 suspects. At the same time, 99 million account information on Taobao has been stolen, which shows that the problem of personal information security has fully erupted.

Although the possibility of information being disclosed arbitrarily is very high, the possibility of information disclosure being detected is very low, and the possibility of punishment is even lower. The criminal law stipulates that violation of personal information "if the circumstances are serious, the offender shall be sentenced to fixed-term imprisonment of not more than 3 years or criminal detention and shall also be fined or only fined." Sentencing is too low to deter such crimes. In addition, there are some difficulties in obtaining evidence and responsibility identification of personal information disclosure cases, which makes the lawbreakers more confident. Therefore, how to effectively protect personal information has become the focus of the whole society.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

1.1. The Harm of Personal Information Leakage

(1) Spam messages, harassing phone calls and spam are all over the place, increasing the pressure o(1) Spam messages, harassing phone calls and spam are all over the place, increasing the pressure of citizens' life

Criminals use the cell base station as the sending center to send short messages to mobile users in the coverage area of the base station. This system can send 15,000 short messages every ten minutes, bringing great troubles to users. Private phone calls are often called in by strangers to promote sales, and their familiarity with citizens' information causes panic among citizens. After the information was leaked, citizens' e-mail boxes received more than a dozen advertisement mails every day, all of which caused mental pressure on citizens. These have once again increased the pressure of life for people who were under great pressure under the fast pace.

(2) Leading to citizens involved in legal cases and reputation damage

Illegal elements will use your personal information to deal with false identities, carry out illegal and criminal activities, involve you in legal disputes, and damage the reputation of citizens.

(3) Cause social credit crisis

Theft methods are multifarious and cannot be prevented. This has caused panic in citizens' hearts, and they can't believe anyone. They are full of fear and rejection of the society. Over time, it has caused a major social crisis.

(4) Hindering the economic development process in the information age

The key reason why some people dare not spend money online is that they are afraid of information disclosure. In order to avoid the disclosure of their own information, they dare not buy online or even use POS machines, which seriously hinders the economic development process in the information age.

1.2. The Importance of Protecting Personal Information

(1) Personal information protection is the need of safeguarding individual rights and dignity

Personal information rights are important rights enjoyed by citizens in the modern information society. Protecting personal information is of practical significance for protecting citizens' personal dignity, protecting citizens from illegal intrusion and maintaining normal social order.

(2) Personal information protection is conducive to maintaining social stability

Personal information is used by criminals, which not only brings troubles to citizens, but also brings spiritual pressure and property losses to citizens, which is not conducive to the stable and healthy development of society. The safer the personal information, the more stable the society.

(3) Personal information protection is the need to promote the informatization process

Information technology has brought extensive and profound influence in the world. Citizens are the promoters of the information age. Protecting citizens' personal information is conducive to breaking through the bottleneck of information development. Strengthening the protection of personal information is conducive to establishing and perfecting the information security system and accelerating the informatization construction.

(4) Personal information protection is the need to stimulate consumption and thus stimulate economic growth

Convenient payment based on the Internet stimulates citizens' online consumption, which is one of the three carriages driving the economy. Improper information protection forces citizens

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

to choose between safety and convenience, and every rational consumer must pay attention to safety. This will lead to slow economic growth, so strengthening personal information protection is the demand to stimulate consumption and thus stimulate economic growth.

2. ANALYSIS ON THE WAY OF PERSONAL INFORMATION DISCLOSURE

2.1. Improper Handling of Small Bills Leads to Personal Information Disclosure

In daily life, people will inevitably use various documents and receipts, such as train tickets, express tickets, supermarket shopping lists, etc. If it is accidentally lost or thrown away, it is likely to be used by people who are plotting against the law, causing personal information to be leaked, resulting in a series of hidden risks and even criminal acts.

2.2. Information Leakage Caused by Relevant Problems in the Internet Environment

(1) Mobile app

Every time we download and install APP on our mobile phone, everyone will always receive the prompt of "read address book, log", "read mobile phone status" and "read location". Usually we can only click passively to confirm to avoid the program being banned. Once we accept this "overlord clause", it is equivalent to our information being displayed naked on the other party's internet program terminal and being left to choose.

(2) Search engine

Some bad search engines collect and process personal privacy information and then market it through websites, making our privacy rights and interests extremely vulnerable to infringement. When the user opens the search engine, he types in the contents that need to be inquired. While expecting the search engine to give us the correct answer, he also exposes some problems such as the current location that the search engine user is concerned about. In addition, some websites have embedded third-party content in their web pages. Third-party content uses compliant pictures and video code segments to track users when accessing the Internet. Embedding third-party content increases the risk of disclosure of personal privacy information on the network.

(3) Online shopping

Collecting and using consumer's personal information can bring considerable economic benefits to businesses, so personal information disclosure incidents often occur, both in scale and quantity. With the advent of the information age, user information is a resource that many new businesses need urgently. According to the positioning of their own products, merchants buy corresponding customer information from "communicators" to expand their customer base. Driven by market interests, this kind of supply-demand relationship has formed a huge interest chain.

(4) Microblog information disclosure

Many people are keen to broadcast their personal life on microblogs, and even some parents can communicate how to educate their children. It involves children's photos, problems and gains in growing up and education. Some people who are willing can read their microblogs to understand all aspects of the user's personal information, which may even lead to crimes.

(5) Mobile social information disclosure

On the one hand, mobile social communication brings back the authenticity of interpersonal communication; on the other hand, it also increases the burden of user privacy protection.

At present, most mobile social applications support users to share personal information such as personal mood, photos and activities anytime and anywhere, with accurate location information. At the same time, WeChat, Tencent, QQ and MOMO applications also support users

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

to make friends with strangers through location information. Compared with a simple location service application, the location information of mobile social interaction is based on the characteristics of social interaction and mobile, and accurate positioning is realized, which is easier to expose the personal privacy of users. There are not a few real cases where people have made "friends" through social applications such as WeChat and MOMO and suffered personal and property losses.

2.3. Improper Handling of Items Carrying Information Leads to Information Disclosure

Mobile phones, notebook computers, tablets, digital cameras and other electronic products, because of their fast-changing characteristics, most people will have "new lovers" and forget "old loves". However, the consequences of personal information disclosure caused by improper handling of old electronic products are unpredictable. Many people think that they can rest easy after clearing the files and formatting the memory. In fact, those criminals who are familiar with electronic procedures can easily find the previous information. Therefore, when dealing with old electronic products, one must be careful.

2.4. Information Leakage Caused by Open Wifi in Public Places

In public places such as subway stations, railway stations and shopping malls, many people will use public wireless networks. However, most people did not expect that its weak protection function would bring opportunities to many undesirable people. They would invade WiFi and then the connected electronic mobile products through technology to steal the personal information of the owner. Taking the first tier cities of Beijing, Shanghai and Guangzhou as an example, the public WiFi security and potential threat survey data report shows that:

2.5. Information Leakage Caused by Illegal Trade of Information in Black Industry Chain

(1) The source of information leakage

The source of information leakage is mainly illegal elements in local state organs, enterprises and institutions and public service institutions.

These lawless elements working in the public sector have the opportunity to access and grasp a large amount of personal information of citizens because they have mastered a part of public power. Due to weak legal awareness, loss of moral bottom line and the drive of economic interests, some personnel regard all kinds of confidentiality clauses and industry norms as a dead letter. They sell the personal information they have to the personal information collectors to obtain economic benefits.

(2) Information collection platform

The information collection platform is the intermediate link in the whole interest chain. Their main profit-making way is to earn the price difference. The organization form includes QQ group and other network platforms. They use technical means to establish a large-capacity data collection platform, buy personal information in batches, sell it to illegal investigation companies or commercial organizations in the form of databases, and earn economic benefits by earning price differences. Illegal elements collect a large amount of personal information through the establishment of QQ group, which has the following characteristics: first, huge capacity. An information platform can hold millions or even tens of millions of pieces of information. All kinds of information of citizens are included in it. The large amount of information and the accuracy of the information make people angry. Second, the operating cost is low. They hardly need any hardware facilities and financial support. A computer and a network cable can easily make profits. Third, the rapidity of information dissemination. The network has the characteristics of immediacy, and criminals can engage in the business of buying and selling personal information 24 hours a day just by staying in front of the computer. The transaction process is simple, convenient and difficult to prevent. Fourth, the

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

characteristics of concealment. These platforms are lurking in the network and it is difficult to arouse people's vigilance. Once criminals feel the wind is blowing, they can quickly transfer equipment and destroy criminal evidence.

(3) Illegal investigation companies and businesses

This link is the last link of the whole interest chain, and also the most profitable one. They buy a lot of personal information from the information platform through the network, conduct citizen information survey and promote various goods and services, and make profits directly. They provide debt recovery services, extramarital investigation fees are not cheap, profitable. Some businesses also sell goods or services to the public by purchasing a large amount of personal information. Their profits cannot be counted, mainly reflected in the average profit growth of the company. Low cost, high income and huge profits are the source of information leakage. It is the improper behavior of malicious use of personal information that leads to the existence of a chain of interconnected interests in the industry. The huge profits induced some people to take risks and illegally obtain information from inside the organization. Once these interest chains are formed, they are difficult to break and all links are closely linked. Through research and analysis, it is found that the interest chain of personal information disclosure has the following characteristics: first, each link of the interest chain is closely linked, and there is collusion between inside and outside, and many information sources flow out of the relevant units. The second is that all links of the chain have low crime cost, large market demand and are easy to revive. Third, relying on the Internet, the interest chain has the characteristic of concealment and has gradually formed a huge underground industry. Criminals rely on the network and use virtual identities to engage in illegal information transactions. Personal information is stored electronically, and massive data can be destroyed in a short time. Because the network has the characteristics of openness and anonymity, these interest chains are difficult to break once they are formed, and every link has strong concealment. Even if one link is destroyed, a replacement will be found soon. The interest chain can be repaired in a short time and cannot be broken for a long time.

3. ANALYSIS ON THE CAUSES OF PERSONAL INFORMATION DISCLOSURE

3.1. Weak Awareness of Personal Prevention

Many people are indifferent to the protection of personal information, do not know the extensiveness of personal information disclosure, do not know the ways and harms of personal information disclosure, and do not pay enough attention to how to effectively protect their personal information. It is not enough to identify some dangerous websites when surfing the Internet, or it may lead to virus or even data loss in one's own computer due to visiting dangerous websites.

3.2. Huge Benefits from Personal Information Transactions

High profits and low costs have prompted some people to take advantage of loopholes and take risks to do these illegal activities. As far as the express delivery industry is concerned, there has even been a public selling of express delivery numbers. The general information is priced at one yuan per item. If the quantity is large, each item in 0.8 yuan can be sold at the lowest price or even the price of each item in 0.3 yuan. The price seems low, but the revenue is huge. According to news reports, a data thief in Heze, Shandong, confessed that as a manager of an express delivery unit, he stole customer information by taking advantage of his position and made a deal at the price of each 30 yuan. The information is accurate to the phone number, name, family and work address. The monthly profit is 20,000-30,000, and the profit is high. The cost difference between profit and cost is staggering.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

3.3. Relevant Laws and Regulations Are Not Perfect

(1) China has not yet issued a special personal information protection law. The status of legal protection is to protect citizens' personal information by setting special provisions in a single law. Relevant regulations are extremely scattered and fragmented, and there is no stable and binding personal information management standard. The specific pattern and mode of personal information management and protection have not yet been formed, so information crime lacks a strong law as the necessary foundation.

(2) The protection of personal information in criminal law is too weak. As the most severe and final sanction, criminal law requires other laws to affirm rights for certain interests first, and on this basis.

3.4. Openness of Network

The network attracts a large number of users and consumers with its huge resource advantages and convenient operation. The openness of the network enables people to upload, collect and share their personal life and information on e-commerce websites or interpersonal networks. The arrival of the mobile Internet era also promotes the spread of personal information more convenient, and can achieve multi platform account sharing. The openness of the network enables different websites to communicate with each other and easily share registration information and personal data authorization of other websites. With the rapid popularization of e-commerce, marketing has become more networked, interactive and interrelated. As a result, operators have more opportunities to come into contact with customers' personal information, and the means of collecting, transmitting and utilizing information tend to be diversified and secretive.

4. ANALYSIS OF THE COUNTERMEASURES TO PROTECT PERSONAL INFORMATION

4.1. Block the Causeway to Relieve the Pressure

Based on the current situation of personal information in our country, it is urgent to adopt legislation, set up information supervision departments and implement effective technologies to block the causeway of personal information disclosure. So as to prevent further disclosure of personal information and relieve the pressure of citizens' life and political and economic pressure under information disclosure.

(1) Accelerate the promulgation of a complete personal information protection law

On May 9, 2017, the scope of citizens' personal information was clearly defined in the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases Involving Violations of Citizens' Personal Information. "Citizen's Personal Information" includes identification information and activity information, that is, all kinds of information recorded by electronic or other means that can identify the identity of a specific natural person or reflect the activity of a specific natural person, including name, identification number, communication contact, address, account number, property status, whereabouts track, etc. 之It is also defined in the cyber security law, which was previously implemented on November 7, 2016. Although our country has made continuous efforts in the legislation of personal information protection, a real personal information protection law has not been issued. China should speed up the introduction of personal information protection law to make the personal information protection system more perfect.

(2) Preliminary establishment of legal system and clear responsibility bearing mode

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

①To establish a comprehensive legal system for personal information protection involving the constitution, criminal law, civil law, administrative law and other departments. According to the nature of the criminals illegal crime will be punished. To ensure that violators are prosecuted will serve as a deterrent to criminals.

②Clarify the responsibility subject of personal information protection. Establish "who collects, who protects; Who uses, who bears the responsibility "of the basic principle. The information collector bears the absolute responsibility of protection. No matter the cause of the leak is a technical defect, or due to hacker attacks, whether it is an active leak or a passive leak, the information collector should bear the responsibility.

③Clear compensation standard. For direct property losses suffered due to information disclosure, the victim can directly claim compensation from the disclosing party. Tortfeasors who intentionally disclose personal information such as buying and selling shall be jointly and severally liable for compensation. If the victim's information is disclosed due to negligence, the victim shall bear supplementary responsibilities within the scope of losses that the victim cannot recover. For information disclosure that has not caused actual losses, it shall be responsible for apologizing, stopping the infringement and compensating for the losses in combination with the impact on the victim, such as reputation damage, social evaluation reduction, degree of life harassment and other factors.

(3)Speed up the establishment of specific information regulatory departments and regulatory associations

The State shall establish a General Administration of Personal Information Supervision, which shall be divided into agencies of various industries. The agencies shall audit, supervise and inspect the status of personal privacy protection in various industries every quarter, and report the situation to the General Administration. Conduct moral education to the industrial departments and relevant personnel who divulge personal information, and even impose a fine or even a penalty on them if they are serious. At the same time, a personal privacy protection association will be set up, in which the third party will give credit scores to the members of the association's website, guide the netizens to browse the regular website with their scores, reduce information leakage and jointly maintain the network information security.

(4) Strengthen technological innovation and timely remedy leaked personal information

①From the process of protection, increase the difficulty of obtaining information

Strengthen technical short-term remedial measures to achieve immediate results. Such as fingerprint identification authorization for important information of citizens. That is, when other people collect personal information of citizens when they are not in special needs, they need fingerprint identification of citizens for authorization, and confidential language can be used considering regional distance. Citizens can authorize by telling each other the secret words. Gradually innovate technology, make full use of fingerprint identification to strictly limit the flow of information.

②Supplement of automatic login function

The function of "auto-filling" brings convenience to users, at the same time, it also gives criminals an opportunity to log in automatically and frequently. Once in a while, if you accidentally quit and forget your password, you should set up a reminder bar to remind the owner of the machine how many times this is the automatic login. Please don't forget the password and try to unlock the phone by setting the password.

③Application of "invisible face sheet"

"Invisible face sheet" means to encrypt and hide the personal information on the express order, improve and strengthen the information confidentiality and comprehensive anti-counterfeiting functions of the express order, which is equivalent to adding a "security lock" to

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

the personal information of consumers. And the express industry is not only in the express list set invisible words, but also to make good use of this technology, in-house rectification.

4.2. Dredge up Problems and Thoroughly Manage Them

Under the condition of preventing information leakage, the existing problems will be further unblocked layer by layer by improving the implementation of the law, optimizing the regulatory structure, carrying out long-term and in-depth technological innovation and improving citizens' awareness, so as to finally achieve the ideal effect of radical cure.

(1) Strengthen publicity and education of legal system, implement and perfect legal system

First legislation still needs to be continuously improved. While dealing with old problems, we should also take into consideration the handling of new ones. Second, legal publicity and education should be carried out in depth. The establishment of legal aid outlets, legal publicity and education activities, and the holding of a national competition on legal knowledge have helped to make legal concepts deeply rooted in the hearts of the people. Third, set up a warning column. The common methods used by criminals and the consequences of crimes are listed in the warning column for public comment, which serves as a warning to citizens.

(2) Strengthen citizens' awareness of protection and prevent information leakage

①Do not fill in personal information at will and keep personal identity information

In life, there are many activities of small investigation and small relay, which will induce citizens to fill in personal information and cause information leakage. When you need to provide a copy of your identity, be sure to write "only for such and such units, other uses are invalid". In addition, attention should be paid to the destruction of redundant copies during the copying process. Use unique and high-security user names and passwords in e-commerce and payment systems involving property to avoid hacker attacks and disclosure of personal information.

②Do not use free WIFI in public places or others. When using public places or other people's free "WIFI" for shopping or logging into social networking sites, sensitive information such as bank cards, identity cards and other information will be exposed on the internet at will, causing serious losses to citizens' property.

③To protect the information security of personal computers, mobile phones and other information terminals. Check and kill computer viruses in a timely manner and do not click on unknown links such as SMS, email and WeChat to avoid "fishing".

④Pay attention to updating the password in time to avoid reusing one password. Passwords are the basis for citizens to protect their own information security. However, due to the problem of citizens' memory, the vast majority of citizens use a fixed number of passwords all their lives, which makes it easy to leak all their personal information. Therefore, citizens should make targeted adjustments when setting passwords.

（3）Establish reporting mechanism and expand credit system

①Establish reporting mechanism and coordinate multiple interests

Establish a sound reporting system to protect the interests of the victims. Citizens who have been illegally harassed after the disclosure of personal information can report to the relevant regulatory authorities in a timely manner, so as to report and handle in a timely manner. At the same time, large and medium-sized enterprises can also inform the regulatory authorities to carry out anti reporting after they encounter malicious reports. The supervision department should open up reporting channels and expand the sources of clues. Strengthen the internal restriction system to avoid the occurrence of such phenomena as failure to investigate the reported clues, inadequate investigation and unauthorized handling of clues. Scientifically carry out the work of reporting primary nuclear accidents; We will improve the protection and

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

reward system to fully ensure the effectiveness of public reporting and effectively protect the legitimate rights and interests of informants.

②Speed up the construction of credit laws and regulations and expand the application scope of credit system

Try to establish a credit evaluation mechanism for enterprise personal information protection. Break through the firm's competition for products and expand the competition to areas such as the overall contribution to society and the perfection of personal information protection. Regulatory agencies and industry organizations have incorporated the level of enterprise personal information protection into the enterprise credit evaluation system. As one of the important indicators for evaluating the credit of enterprises, the evaluation results should be made public to the public in an appropriate way to improve the initiative and initiative of enterprises in strengthening the protection of personal information. And combined with the future gradually improved disciplinary mechanism of dishonesty, the social evaluation mechanism of corporate integrity, the market withdrawal mechanism of dishonesty enterprises, the restriction mechanism of market activities, and even various special supervision mechanisms of personal information protection are comprehensively applied to corporate supervision.

(4) Strengthen the innovation of technology and use technology protection effectively

①Tracking and positioning of citizens' personal information means that citizens' personal information forms a transparent state to themselves. Citizens can always query their own information status, such as who has checked the information, who has copied the backup information. Once a citizen's information is disclosed, he or she can be held accountable accurately, which not only effectively protects the citizen's personal information, but also acts as a deterrent to criminals and greatly reduces the crime rate.

②We will improve the construction of an enterprise's internal information management system, conduct real-time network monitoring in combination with transparent encryption and decryption of documents and internal network management, and provide an integrated information security solution for enterprises. From the source to ensure the safety of data storage and use, standardize computer operations, prevent data leakage, to ensure information security.

(3) Establish a temporary information bank, combining the digital forgetting right with the currently hotly discussed block chain technology. Under the background of economic globalization, personal information forgetting has become an accident, while memory has become the norm. Two nouns, digital forgetting right and block chain technology, came into being. The right of digital forgetting is a right enjoyed by data subjects, which requires data controllers to delete personal information related to themselves so as to control the further dissemination and improper use of such personal information. It emphasizes the information subject's control over personal information, which is of great significance to the legislation of personal information protection. However, block chain technology is a kind of chain data structure that combines data blocks in chronological order in a sequential manner, and is cryptographically guaranteed to be tamper-proof and unforgeable distributed books. It is an Internet database technology. It is characterized by decentralization (i.e. no third-party platform), openness and transparency, and is currently being studied by all countries in the world. The temporary savings bank is mainly used in places where information is to be collected temporarily, such as job-seeking systems (for example, when enterprises recruit talents, the employed employees are screened out, the resume information of the unemployed employees will be automatically cleared, the system will only show when the person has applied several times, and other useless information will be forgotten). After clearing up, only the information subject can be found to have visited several times, and other information will be completely

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

cleared. If digital forgetting right can be combined with block chain technology, the information subject can control his own information and cannot be changed or forged.

4.3. Strengthen Prevention and Avoid Circulation

After solving the problem step by step, we should draw lessons from experience and work hard ideologically so that enterprises can truly establish a sense of responsibility, so that citizens do not encroach on citizens' personal information from the bottom of their hearts and truly avoid a vicious circle.

(1) Strengthen the construction of corporate culture and raise the sense of corporate responsibility

While strengthening the internal supervision of enterprises, we should strengthen the management of enterprise culture, strengthen the moral cultivation of employees, and form the culture of protecting users' privacy information in enterprises. Through the mechanism of training, supervision, rewards and punishments, a consensus and culture of "user privacy protection is my responsibility" has been formed. Enterprises shall provide targeted training for data security sensitive posts and personnel. For customer service personnel, operation personnel and sales personnel who often have convenient access to user's private information, they must know which user information can be used in what scope, which common behaviors are prohibited or even illegal, and what technical measures the company has set up to monitor.

(2) Carrying out the course education of personal information protection and infiltrating the thought of information protection

Gradually carry out personal information protection courses from the education system and adopt new media communication methods to enable individual citizens to have the awareness of not infringing on other people's personal information. At the same time, we should earnestly study laws and regulations so that when personal information is violated by others, we can safeguard our rights in a proper and timely manner. Finally, citizens can consciously protect their own and other people's personal information.

(3) The government increased its funding for anti hacker groups to crack down on lawbreakers

We will continue to strengthen network maintenance and increase the government's funding for "combating cyber terrorism". It is mainly used for information security research, research and development of technologies to combat cyber terrorism, and training of relevant professionals. Increase the government budget in this regard, intensify the research on anti hacker technology, train anti hacker experts, so that hackers who steal personal information no longer have a chance.

5. SUMMARY

With the transformation from industrial economy to knowledge economy, the characteristics of informatization, digitalization and networking in the world economy are becoming more and more obvious. The networking of business activities and the virtualization of capital operation have not only provided unprecedented speed and convenience for various economic activities, but also greatly increased the risk of personal information disclosure. Under this background, we put forward how to improve the current situation and prevent the disclosure of personal information through laws, technologies, etc. At the same time, it puts forward a three-step personalized plan of blocking the causeway, dredging the problem and preventing the circulation, which provides reference for the government to control information leakage, clears the obstacles for economic development and guarantees national security.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202005_6(5).0020

REFERENCES

[1] Wang Hongyi. On the legislation of government regulation of personal information protection [J]. E-government, 2015

[2] Liu Chang. Research on personal information protection in the era of big data [D]. Northeast University of Finance and economics, 2016

[3] Mo Xiaochun. On the protection of personal information of Chinese citizens in the era of big data [a]. Innovation, 2015

[4] Gao Meiyan. Reflections on legislation of personal information protection [a]. School of Social Sciences, Shanxi University, 2015

[5] He cultivate, Lin Ying. On the right to be forgotten of personal information in the digital age [J]. Modern intelligence, 2016

[6] Wang Zhiwen. Blockchain information storage and privacy protection method [P], 2016

[7] He Chuang. The stone of another mountain: the investigation and reference of personal information protection legislation in Germany [J]. Chongqing and the world: Academic Edition, 2015

[8] Shi Yaxin. Study on the criminal protection of personal information of Chinese citizens [J]. Law and society, 2015