ISSN: 2688-9323

The Conflict and Resolution of Personal Data Information Protection and Data Application

Xiaochen Jiang

Qingdao University of Science and Technology, Qingdao, China

Abstract

In the era of big data, Internet technology is developing rapidly. With the increasing value of data applications, personal data information has become an indispensable key part of corporate decision-making, and citizens' personal information privacy is therefore facing unprecedented challenges. Big data application is a double-edged sword. While it brings convenience to our lives and improves our quality of life, it also erodes our right to privacy step by step. The different value orientations of different subjects for the same information lead to data applications. The contradiction with data privacy, the contradiction between data application and data privacy is geometric, how to balance this contradiction becomes the top priority of this article. In the context of big data, the traditional privacy protection model no longer meets the needs of personal data privacy protection. It is also urgent to explore ways to protect personal information privacy under the new situation. This paper explores specific solutions from the aspects of domestic legislation, industry Self-discipline and subjective awareness, so as to effectively protect citizen's personal information privacy.

Keywords

Big Data; Data Application; Personal Data Information; Privacy; Legal Protection.

1. Introduction

In recent years, with the popularization of the Internet and the rapid development of Internet technology, big data application technologies have emerged. The maturity of data collection and data analysis and processing technologies and the use of personal information data have enabled most information data to play its commercial role. Value generates economic benefits and facilitates our lives. But at the same time our lives are being monitored by the "ubiquitous third eye"[1] Through electronic transactions and the recording, storage and analysis of digital traces formed by Internet users on the Internet, people's daily habits of food, clothing, housing and transportation may be known one by one. For example, e-commerce platforms can easily analyze users' shopping habits, living standards and other private information through user purchase records, browsing information, and harvest addresses; social software such as QQ, Weibo, and WeChat Moments can help us to connect with people. It's clear; mobile apps can more easily obtain basic information such as the user's geographic location, address book, etc.... In the context of the era of big data, the scope of privacy is "shifted", and personal privacy is getting closer and closer to transparency. How to grasp The boundaries of data application, the fullest use of personal data, and the balance between data application and data privacy protection. Nowadays, there is no unified conclusion in each country, and the standards for the "degree" of data application are not the same. The protection of privacy cannot keep up with the rapid development of data application technology. The disconnection between protection measures and the rapid development of technology has led to the leakage of citizens' privacy. Personal privacy rights are unknowingly violated. Therefore, a balance between data application and data privacy protection is sought. The point is imminent.

ISSN: 2688-9323

"Big data is hailed as a revolutionary undertaking in the 21st century"[2] However, not many people can clearly introduce what big data is. Different scholars and institutions have different opinions on big data, whether it is the "3V" characteristics of big data proposed by the more recognized Doug Laney, namely velocity (Velocity), diversification (Variety) and scale (Volume) [3], Or later with the development of data application technology, such as "4V", "5V" and "6V" features such as validity, veracity and visualization. I think big data is a huge amount of diverse data., Can be used as reference content, has reference value, and can reflect the social insight, commercial value and other functions of its data through network data application analysis technology. So, I am more inclined to the "4V" feature of big data proposed by Sanil Soles, that is, adding a value to Lenny's point of view.[4]. Big data is required to reflect the economic effectiveness of data. It was mentioned in the article "Personal Privacy Protection in the Era of Big Data": "Most of the data in big data comes from people and sensors, including information that users browse online, and social networks. User's information and comments, sensor data and monitoring data, etc. on the Internet."[5] It can be seen that there is a strong contradiction between data application and personal data information protection in the big data environment.

"Privacy" as a broad concept has a long history. As an abstract right, it is difficult for us to define the right of privacy with a single definition. Scholars from all over the world have conducted in-depth discussions on the right to privacy. Different scholars have different overviews of the meaning of the right to privacy under different era backgrounds. So far, there is no unified definition that can be widely recognized. In the context of big data, as a natural extension of traditional privacy rights on the Internet, data privacy rights are essentially the same in terms of subjects and legal interests as traditional privacy rights. Therefore, data privacy rights are the peace of life citizens enjoy on the Internet. Private information is protected in accordance with the law, and is not illegally infringed, used, collected, copied, disclosed and known by others, including the right to choose, control, security, know, and claim for personal data information. [6] Privacy is a right of personality and is closely related to personal dignity. Therefore, the current abuse of other people's personal information on the Internet seems to be a serious violation of the dignity of others.

In the era of big data, the application of data will inevitably involve personal privacy information. Citizens' right to privacy has been violated unknowingly. Mastering the balance between data application and privacy protection has aroused social concern and reached a basic consensus. This research will focus on In-depth research and discussion on this balance point, through the discussion of its contradictions, practical dilemmas and other issues, try to propose methods to protect private privacy while making full use of private data.

2. Conflict between Data Application and Personal Data Information

In the era of big data, data analysis and processing technologies have developed rapidly. The application of big data has made personal private information economically beneficial. As a result, the connotation of privacy rights has changed. It no longer only belongs to personality rights, but also possesses property attributes. It is precisely because of this that data information owners can freely access and apply personal data information for different purposes, which increases the risk of data privacy violations. Many cases exposed at home and abroad have also exposed the embarrassing situation of data privacy protection. In our country, "Human Flesh Search" incidents have occurred frequently since the 2001 "Chen Ziyao was Human Flesh Incident". "Human Flesh Search" is a practice of rapid development of social network information technology today, and it is also a violation of our privacy rights by data applications. The "Prism Project" that was exposed in 2013 made the United States, which has always paid more attention to privacy protection, been under public scrutiny. This data monitoring project started by the US government in 2007 has directly raised the infringement

ISSN: 2688-9323

of personal privacy by data applications to the level of national security. Therefore, the contradiction between data application and personal data information protection is prominent.

The source of the contradiction between data application and personal data information protection lies in the different pursuit of interests by different subjects. Whether it is the wide application of data or the in-depth protection of privacy rights, both pros and cons coexist. Therefore, no matter what kind of interest we are pursuing, we cannot To make a single judgment, we hope that the law can make a clear definition. However, the times are developing, and many emergencies are not predictable by legislative practice. The law cannot clearly define the boundaries of data application, nor can it clearly define the data. The legal status of privacy, so the boundary between data application and personal information protection is blurred, and the contradictions between the two are endless. Tian Xinling scholars described it as a paradox between public data disclosure and personal privacy protection, and revealed the cause of this public opinion from different levels of society, politics, and culture.[7] But the fundamental reason lies in the different interests we pursue. Therefore, as long as we can balance the interests behind the two, we can find a reasonable boundary between the two.

Interest is the interest enjoyed by the subject, so we analyze the contradiction between the two from the perspective of the subject. Generally speaking, there are three types of important subjects in the context of big data-enterprises, governments, and individuals. First of all, in order to maximize the profits and increase the profits of the enterprise in economic activities, the main body of the enterprise will collect, classify, analyze and summarize the various information that it has in order to formulate the strategic plan and marketing method of the enterprise, reduce production costs, and enhance its own competition. Secondly, in order to maintain social order and create a safe and comfortable social environment in the management and control of social life, the government will use technical means to collect data and information of the managed, in order to monitor social groups in an all-round way and reduce social management costs. , Crime prevention; finally, individuals or small groups of natural persons, such as private investigators, network hackers, etc., based on various purposes, for profit, they will also collect and analyze private data. In the era of big data, a new type of data application entity-data brokers emerged. Most data intermediaries have mastered massive amounts of data information and have absolute advantages in data quality and quantity. They can conduct transactions with data demanders, and can also collect and process data in place of entities lacking data resources, and analyze data to obtain Corresponding labor remuneration, or you can directly analyze the data information of a specific field to obtain breakthrough progress to make a profit.

In summary, “the conflict of interest between data applications and the protection of personal data information is mainly the opposition between the right to privacy and the right to know, the right to freedom of speech, and the public interest.” [8] The essence of this opposition is the different value pursuits of different subjects for the same private data information. For information providers, personal information is closely related to their personal dignity and personal safety, as Rousseau said: Every honest person should maintain his dignity. Information providers have the right to require others to respect their own personality and dignity. For enterprises and governments, data represents huge economic benefits and efficient management value. The needs of different subjects also represent corresponding legal demands. Citizens focus on the protection of personal information and therefore require the protection of privacy rights. In order to maximize the use of data and information and extract the economic benefits, enterprises and governments will require expansion. Data application scope and collection authority. Different values have different needs, which is bound to seek a balance of interests between the two.

To achieve a balance between data application and personal data protection, we should first set a bottom line for the interests of multiple subjects, because only when the basic interests of the

ISSN: 2688-9323

subjects are protected can we begin to talk about the issue of "balance". Take the user of data information as an example. The bottom line of its data application lies in its ability to make full use of the data and information it possesses to obtain basic economic benefits. However, due to the development and progress of data application analysis technology, data acquirers are likely to involve unexpected personal privacy information when collecting and processing information within the scope of data collection and application authorized by the data provider. This reflects from another aspect that we need to implement strict supervision on the collection and application of personal privacy data information. However, it must be noted that in some emergency or special circumstances, these bottom lines can be completely broken. The government can collect and use necessary personal privacy information beyond the authorization of the data information provider for national or public interest safety, social order stability, and emergency situations, and the corresponding natural person has no right to demand protection of their privacy. Due to the existence of this exception, it is likely to be a legitimate reason for infringing on data privacy rights, which will seriously damage the legitimate rights and interests of the parties and is not conducive to the protection of data privacy rights. Therefore, we must use legal means to strictly limit this exception. In short, through the analysis of the contradiction between data application and data privacy protection, it is not difficult for us to find the blurring of the dividing line between the two. We need to find the balance point between the two to reasonably delimit the two. Resolve its contradictions and conflicts.

3. Forms of Data Application Infringement of Personal Data Information

Through the above analysis, we understand the conflicts between data application and personal data information protection. With the expansion of the Internet application field, citizens' personal information is more or less collected by network platforms, especially derived from the era of big data. Specialized organizations and institutions focus on collecting these personal information, collecting, categorizing, and analyzing to generate various result data for use in order to generate economic benefits. The good application of this kind of data can produce positive economic benefits. It can be described as low investment and high income. If it is not used well, it will produce negative consequences. In the slightest, it also violates the privacy of citizens, causing privacy leakage and harassment of phone calls. Frequent occurrences and telecommunications fraud have lost both fame and fortune, and severely endangered the personal safety of citizens and even national security. At the same time, compared with the traditional forms of infringing on privacy rights, the forms of infringing on citizens' private information also present new features such as subject diversity, complexity of content, concealment of means, and wide geographical coverage. In the context of data, how does data application infringe on citizens' private information?

3.1. Improper Collection of Personal Privacy Information

In the era of big data, the popularization of mobile communication devices such as mobile phones and computers and electronic payment methods have enabled various software and e-commerce platforms to record our personal behavior, communication records, transaction habits, consumption information, etc. all the time. This requires Our information collectors use personal data information extensively while grasping the degree of collection. In reality, there are mainly two phenomena of excessive collection and illegal collection.

(1) Excessive collection. In layman's terms, that is, information that is not necessary to be collected is collected. In the era of big data, driven by data as profit, many information collectors exceed the limits required at the time when collecting information, and excessively collect personal information. Nowadays, most mobile device software logins need to register personal information first, and even obtain personal geographic location and other information.

ISSN: 2688-9323

Although some private information is useless for specific software, the software platform can use the acquired "useless information". Storage analysis, as the data for secondary use, can still contribute to the development and utilization of other software. Excessive collection has also become a typical data application infringement in the era of big data.

(2) Illegal collection. Illegal collection refers to the collection of data by information collectors beyond the authority prescribed by law, and mainly includes three situations. One is collection without consent, such as network operators collecting their account information and browsing records without the consumer's permission; the other is collection without approval, such as some illegally operated websites without obtaining operating qualifications and investing The market, collecting user information, seriously infringes on users' private information; the third is to use hacking techniques aimed at network vulnerabilities or defects to illegally invade network users' computers and steal their private information.

3.2. Improper Use of Private Information

Data acquisition is the prerequisite, and data application is the ultimate goal. After obtaining personal privacy information, information collectors can only obtain economic value by analyzing and using it. During this period, it is relatively easy to infringe on privacy, which can be mainly summarized as improper disclosure and illegal transactions.

(1) Improper disclosure. The information collected by the data information collector through legal and effective means can be reasonably used within the scope authorized by the information provider, but the information collector often exceeds the authorized scope during the use process, and discloses the personal privacy of citizens without the consent of the other party. information. Just like in the entertainment industry today, the lives of celebrities have almost no privacy at all. The existence of entertainment reporters and crazy fans such as "paparazzi" and "illegal meals" monitors the daily lives of celebrities all the time. Our privacy is their resource for profit. Searching the Internet, the seller will have a lot of account information, he will not only tell you the idol's recent itinerary, flight information, hotel address, even the very private WeChat account, mobile phone number, etc. are all sold at a clear price, if you want to know, without them Not for sale. Therefore, regardless of whether the collector leaked it intentionally or negligently, and whether the party leaked the legally collected or illegally collected private information, it will not affect the qualitative nature of the act infringing on citizens' privacy.

(2) Illegal transactions. Data information collectors sell their collected personal privacy information for profit. It is reported that in the information trading market, data collectors categorize different types of private information and sell them at clear prices. In real life, we will find that if a student downloads a certain learning software, soon after the registration is successful, we will receive a call from the counseling agency in the relevant field; pregnant mothers will receive hospitals, confinement centers, etc. Phone calls in the maternal and infant industry; people who have searched for rental information will receive calls and text messages from the selling agent... Maybe we have never contacted them, but they know our communications and private information about our personal situation well. Behind this is the data. The illegal transaction chain of information is at play, and it is precisely because of the existence of this industrial chain with clear division of labor and ordinary transactions that network fraud, pyramid schemes, and harassing calls emerge one after another.

(3) Data abuse. At the beginning of 18 years, the annual bill launched by Alipay blasted WeChat Moments. Behind this seemingly simple bill is the fact that Alipay abuses user privacy. When Alipay generates the annual bill, the option "I agree to the "Sesame Service Agreement"" is checked by default, but this line of "Agreement" is extremely small and will be ignored by users if it is not careful. Once the network user agrees to sign this agreement, it means that the Alipay platform can arbitrarily collect their own personal data information, including data stored in

ISSN: 2688-9323

third parties. What's even more excessive is that after signing the agreement, Alipay can re-analyze all the user's collected information and push it to cooperative institutions, such as banks, insurance, funds, securities companies, catering and entertainment companies, etc., and the user cannot withdraw the third-party Authorization.

Alipay bills are only the tip of the iceberg of privacy abuse, and a large amount of software on mobile phones is the main channel for citizens' privacy leakage. With the rapid development of mobile Internet technology, people have been enjoying the great convenience brought by mobile phones, but at the same time, people's location, email, address book, text messages, and even names, home addresses, ID numbers, phone numbers, Extremely sensitive and private information such as bank card accounts and work units may be collected and abused by illegal companies or individuals. The user's personal information has almost become a "don't use it" public resource, and the phenomenon of unrestrained abuse of private data seems to be very serious.

4. The Status Quo and Dilemma of Big Data Applications for Personal Privacy Information Protection

4.1. New Situations in Personal Privacy

In the era of big data, new situations have emerged in personal privacy: (1) The scope of privacy has shrunk. In the era of big data, citizens' private information is no longer confined to dissemination within physical space. Public space and network virtual space have become a new field for the dissemination of private information. The privacy of citizens is constantly shrinking. At the same time, the openness and fast dissemination of virtual cyberspace make the dissemination of private information faster and more convenient, and the dissemination range is wider. As long as there is a network, the dissemination of data and information can be seen everywhere, even for the general public. We can also use network technology to obtain the private information we want. Isn't "human flesh search" the principle? The privacy of citizens is constantly eroding. (2) The scope of the object of privacy is expanded. The traditional right of privacy, as a kind of personality right, mainly protects citizens' most basic personal information, such as names, portraits, addresses, and communication methods. The object of privacy right now extends to valuable data information, such as citizens' shopping habits, loan records, hobbies, web browsing footprints, etc. The right of data privacy has changed from a pure personality attribute to a property attribute. (3) The economic value of privacy is prominent. Compared with the traditional right to privacy, which focuses on the protection of human dignity, data privacy now pays more attention to the display of economic value. In the era of big data, data information has become an important social resource. Through the analysis of big data, enterprises cater to market needs, grasp development opportunities, and occupy the commanding heights of market competition, so that they can remain invincible in the fierce market competition and obtain high profits. For example, banks can analyze more attractive lending policies through private enterprise loan mortgage records and generate income for the bank's financing and lending business. (4) The demand for privacy protection is more proactive. The traditional right of privacy is usually considered as a passive and inviolable power of personality, but now, the commercial use of data information makes the right of data privacy a proactive power with both personality and property attributes. The subject of privacy rights protects their own economic interests in a more active and effective way, and avoids serious losses caused by data leakage.

ISSN: 2688-9323

4.2. The Dilemma Caused by Data Application to Personal Privacy Data Protection

The Internet brings efficiency and convenience to mankind, and at the same time makes users' privacy rights face unprecedented challenges and threats. The era of big data has also increased the difficulty of protecting privacy.

(1) The right to privacy is difficult to define. As mentioned above, privacy has a long history, and the right to privacy is defined by different people, and wise people see wisdom. The right of data privacy expands the scope of the object. As the original right of personality, the right of privacy adds property in the practical sense, leading to the dilemma between the two. The value of personal privacy data is not the basic purpose of the original collection of data and information. Most of it lies in the secondary use of this information, and it is usually in the process that illegal behaviors such as credit card fraud and extortion that seriously violate the right to privacy have occurred.

(2) The privacy of data privacy being violated. The big data environment is built in a virtual cyberspace. The network is a virtual space with features such as anonymity, decentralization, neutrality, interaction, convenience, and transnationality. @Privacy infringement usually happens without the infringee knowing it. The development and popularization of Internet technology and the increase of anonymous users on the Internet make it difficult to capture online infringements and to obtain evidence. In the process of obtaining evidence, even if there is a domain name, there are corresponding network laws and regulations, but the real-name system is not fully implemented, and even some domain name registrations are inaccurate, making it impossible to find the infringer himself, and more importantly, it is impossible to ensure that it is The infringement committed by me. In a lawsuit filed by U.S. citizens against the government's implementation of a large-scale data monitoring program that violated the Fourth Amendment of the Constitution, the Federal Supreme Court held that the plaintiffs could not prove that they were monitored and therefore could not prove that they had suffered sufficient "factual harm" and therefore could not Get the support of the court. [9]

(3) Personal data privacy is difficult to manage. Managing private data is a huge and complex process. Managing private data includes data collection, utilization, storage, publication, sharing, etc. For managers of personal private data, management information is mainly divided into four aspects: first, how to ensure the integrity of private information. Second, what technology is used to ensure that information is not stolen or accessed illegally. Third, what kind of strict access control strategy should be set when using it without increasing the workload of departments and units. Fourth, how to define the information that can be published online and how to define the scope of users who can access such information. [10] The management of private data must not only maximize the value of the data, but also protect the privacy and security of the data, so as not to cause damage to individuals, thereby increasing the difficulty of private data management.

4.3. Defects of Personal Privacy Data Information Protection under Big Data

4.3.1. Incomplete Data Privacy Legislation

1. Insufficiency of civil legislation. Article 42 of the "Cyber Security Law of the People's Republic of China" officially implemented in 2017 stipulates that: network operators shall not disclose, tamper with, or destroy the personal information they collect; they shall not provide personal information to others without the consent of the person being collected. However, except for those that cannot be identified and cannot be recovered after processing. Network operators shall take technical measures and other necessary measures to ensure the safety of the personal information they collect and prevent information leakage, damage, or loss. When personal information leakage, damage, or loss occurs or may occur, remedial measures shall be taken immediately, and users shall be notified in a timely manner and reported to the relevant

ISSN: 2688-9323

competent authority in accordance with regulations. Article 111 of the "General Principles of the Civil Law of the People's Republic of China" adopted in March 2017 stipulates: any organization or individual that needs to obtain the personal information of others shall obtain and ensure the security of the information in accordance with the law, and shall not illegally collect, use, process or transmit the personal information of others. They are not allowed to illegally buy, sell, provide or disclose their personal information. Although the above two laws clearly stipulate the protection of personal information on the Internet and clearly stipulate that the personal information provided must be processed so that specific individuals cannot be identified and cannot be restored, information without the consent of the parties shall not be disclosed to others. However, my country's civil legislation is mainly formulated by government entities, and there are still shortcomings: First, it does not clearly stipulate the scope of personal information. There is no specific definition of the specific protection content of privacy, such as private space and private secrets, and there is no clear protection scope, so there is no talk about a complete legal system for the protection of citizens' privacy. Secondly, there is no clear status of privacy. The previous article discussed that the right of privacy, as a right of personality, has both property attributes, and so far there is no independent law specifically to protect it.

2. The criminal legislation is full of loopholes. Compared with the civil law, my country's criminal law also has the defects of unclear definition of personal privacy data, unclear property attributes of privacy rights, incomplete interpretation of citizen information, inability to clearly analyze judicial interpretations, and huge amounts of citizen data, resulting in the current criminal law. The system cannot fully and effectively solve the current infringement of online citizens' private data information. The current criminal law's legislation for the protection of citizens' online privacy rights is still in its infancy, but the rapid development of the Internet has increased the risk of using online platforms to commit crimes. Legislative protection cannot keep up with the pace of illegal crimes. The asymmetry between the two makes the criminal law's legislation The loopholes were revealed one by one.

4.3.2. The Form of Data Information is Difficult to Supervise

"Big data has promoted the development of the Internet, and the efficiency of information exchange and social operations has been improved. However, due to people's weak awareness of data and information security protection, some criminals seek opportunities to sell data for profit, or use privacy to engage in criminal activities such as fraud. "In Tan Jianfeng's view, data trading poses the greatest risk. This is not unfounded. Since citizens' private information is collected and stored in the information collector's database in digital form, it is difficult for data producers to track its subsequent use, and it is driven by huge economic benefits. , It is difficult for data collectors not to re-integrate and use the data they possess for huge economic benefits in order to make huge profits. In fact, this is true. In the past few years, Internet platforms have repeatedly been involved in user information leakage incidents: Alipay 20G user information was leaked in 2014, Dangdang again fell into the hacking door in the same year, and 8 million user information on Xiaomi forums was dragged. Library. This includes multi-dimensional information, such as user name, password, ID card, phone number, QQ number, e-mail address, etc. In addition, the leakage of transaction user data by internal employees due to inadequate platform supervision occurs every year, which fully demonstrates the deficiencies in the protection and supervision of digital information.

4.3.3. The Judicial Remedy Channels are not Perfect

Due to the new situation of data privacy in the context of big data, traditional judicial remedies can hardly meet the relief needs of modern privacy infringers. Regarding the confidentiality of data privacy infringement, many illegal evidences are stored in electronic devices or online clouds. According to the current principle of "who advocates, who provides evidence", it is

ISSN: 2688-9323

difficult for the plaintiff to collect evidence to prove the defendant's infringement. Compared with the trend of prominent economic value of private data in the era of big data, the current way of assuming civil liability for "stop infringement, eliminate obstacles, eliminate danger, compensate for losses, eliminate impact, restore reputation, apologize, etc." is generally a court decision Economic compensation methods such as compensation for mental damage, soothing payments, and medical expenses cannot make up for the economic losses incurred by the infringement of the right to privacy. In short, traditional judicial remedies cannot adapt to the new changes and requirements of the new era.

4.3.4. The Industry has Poor Self-discipline and Lack of Network Supervision

As mentioned above, big data companies are chasing high economic benefits. In the face of interests, citizens' private information becomes a tool for making money. The big data industry does not hesitate to harm the security of citizens' personal information to seek economic development. The government has not established a sound and effective administrative supervision and punishment mechanism, the online platform supervision mechanism is not sound, the duties of law enforcement agencies are ambiguous, and the big data industry has also allowed the infringement of citizens' privacy rights. The trinity of legislation, justice, and law enforcement is indispensable. Without supervision, legislation cannot be perfected, and judicial implementation cannot be implemented. Therefore, the supervision of relevant administrative departments must be strengthened to effectively enforce the law. However, in the era of big data, data application infringement takes various forms, the law enforcement process of privacy protection is correspondingly complicated and cumbersome, and the difficulty of protection is escalating, making the road to data privacy protection difficult.

4.3.5. The Ability and Awareness to Protect Personal Privacy is Lacking

The Regulations on the Protection of Personal Information of Telecommunications and Internet Users promulgated by the Ministry of Industry and Information Technology in 2018 clearly stipulates that user have the right to cancel accounts on various websites and mobile software. QQ account can be cancelled in 2019. This may seem like a simple operation, but in fact it is a huge improvement in the maintenance of network data privacy. In the era of big data, most of the user's account is associated with personal private information. The account can be discarded at will, but the personal information associated with the account will always be stored in the cloud, which can easily be stolen by others. It is our right to cancel the account, but in real life, only a very small number of us will cancel the account. Under normal circumstances, we will directly uninstall the useless or infrequently used software, and there is no sufficient awareness of account cancellation. It demonstrates the lack of citizens' awareness and ability to protect personal privacy.

5. Measures to Protect Personal Data Information under Big Data

5.1. Clarify the Scope of Privacy, Severely Punish and Punish Measures, and Promote the Improvement of Legislation

The law is a weapon for citizens to protect their legitimate rights and interests. If there is no law to rely on, then the protection of privacy infringement will become a piece of paper. Only when the law is enacted and implemented in practice, can citizens' privacy and security be effectively protected.

1. From the perspective of civil legislation, it is necessary to use the opportunity of the compilation of the civil code to clarify the independent legal status of the right to privacy, and clearly stipulate the connotation and extension of the right to privacy in the provisions. Judging from the current privacy protection legislation, privacy protection should focus on personal privacy, physical and residential privacy, personal image privacy, privacy protection of heart

ISSN: 2688-9323

secrets, privacy of private family data or information, privacy of property, privacy of diseases, etc. [11] Therefore, it is necessary to clarify the standards for the collection, utilization and management of citizens' information, strictly distinguish the civil liability of the infringer, improve the defenses, refine the infringement compensation standards, and enhance the operability of civil law protection measures.

2. From the perspective of criminal legislation, the criminal legislation that requires continuous privacy protection, further expands the scope of regulation of citizens' information and data infringement, and incorporates data related to citizens' personal study, work, life and other direct interests into the criminal law system for privacy protection, enriching The way privacy is protected by criminal law. Establish and improve grassroots criminal law laws and regulations, departmental rules, etc., and accelerate the issuance of regulatory documents in various sectors to form a complete legal system. Based on the background of the big data era, the use of Internet technology, cloud processors and other big data technologies to leak citizens' personal information and infringe on citizens' privacy rights can be dealt with based on traditional privacy protection methods. The interpretation is revised, the big data network service system, etc. are included in the monitoring channels for the protection of citizens' privacy rights, specific infringements and punishments for serious circumstances are clarified, and citizens' privacy rights are effectively protected.

With the rapid development of big data today, we should strengthen the formulation of cyber security legislation. In view of the rapid and wide-ranging characteristics of network information, judicial interpretations should be formulated based on the scope of information dissemination, the number of browsing and forwarding, and the click-through rate. Corresponding punitive measures, clarify specific crimes, continuously improve the rationality, authority and scientificity of network security legislation, promote the continuous improvement of the network security legal system, and improve the level of criminal law protection of data privacy. Regarding the extension of data privacy, we can take the new situation of damaging citizens' privacy and property rights as the main object of prevention and control, take the digital extension of benefit crimes against citizens' material property infringement as the object of protection, and take the value of citizens' private information at the social level as the key point of protection. Separate chapters and regulations have been established in China to provide centralized protection for citizens' online privacy information. [12]

5.2. Reform the Judicial System, Enrich Judicial Relief Channels, and Clarify Compensation Standards

"There is no right without remedy". In the era of big data, it is necessary to establish a perfect way of remedying rights, improve judicial standardization, and promote judicial system reform. my country has promulgated and implemented the "Interpretation on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringing Citizens' Personal Information". This document clearly stipulates the scope of protection of personal information and the boundaries of information data transactions, and provides clear standards for the subsequent maintenance of citizens' private information. [13] However, the network environment is complex and privacy protection has a long way to go. Therefore, it is more important to continue to introduce systematic, scientific, and highly operable judicial interpretations and codes of conduct. In addition, it is necessary to enrich judicial relief methods and clarify the property rights relief compensation methods and compensation standards for privacy protection.

ISSN: 2688-9323

5.3. Strengthen Self-discipline in the Internet Industry, Standardize Corporate Behavior, and Shoulder Protection Responsibilities

With the advent of the era of big data, a large number of successful business cases using big data have allowed big data companies to see new business opportunities, and the demand for data mining and processing has increased. Many companies have seen the economic value of them and did not hesitate to violate business ethics. And industry standards to profit by infringing on citizens' privacy. Therefore, we must strengthen corporate integrity education, face up to the economic value of private data, regulate our own behavior, and shoulder the social responsibility of protecting user data privacy. Ensuring the security of citizens' private data is the most basic and most important requirement for companies. Regardless of the size of the company and its rich assets, as long as the citizens' private data are mastered, they must shoulder the responsibility of protecting them. It can guide the establishment of industry self-regulatory organizations, formulate industry self-regulatory conventions, establish an internal disciplinary system within the industry, and increase the cost of violations of laws and infringements.

Enterprises must adhere to the minimum collection of private data from citizens, and must adhere to industry standards and professional ethics for unnecessary data. If they are not collected, they must not collect, and insist on reasonable collection and reasonable use. The industry's "overlord clause" should be reformed and abolished in a timely manner. In addition, it is necessary to improve the company's data security technology, standardize the big data operation process, improve the internal system, increase professional ethics education for employees who have access to the data, increase the awareness of privacy data security protection, and prevent data leakage.

5.4. Increase Investment in Technology Research and Development and Improve Data Privacy Protection Technology

Big data technology is a "double-edged sword". We can't give up on choking and give up the development of the entire network technology in order to protect the security of personal data. With the rapid development of Internet technology, the popularization of big data has become an irreversible trend of the times. The application of big data is inseparable from the advancement of science and technology, economic take-off, and social change. We should face up to the problem, face the challenge, cultivate scientific and technological talents, increase investment in technology research and development, and develop more innovative and safer technologies through data traceability technology, identity authentication technology, data watermark technology, social network anonymity protection technology, and data release anonymity protection technology. Network data protection technology protects privacy and security technically.

5.5. Strengthen Publicity and Education, and Enhance the Subject's Awareness of Privacy

In our country, most citizens are out of the "unconscious" state of privacy protection. The government and relevant social organizations should actively carry out education and publicity activities on the protection of privacy information, and strengthen the ideological education of citizens. Citizens should "start with me and start with the small things" for privacy protection, stick to the first line of defense for privacy protection, develop good habits, and increase their awareness of risk prevention. Log out useless software and accounts in a timely manner; be vigilant before disclosing the content of private information, and carefully read the relevant privacy clauses; frequently conduct security checks on computers and mobile phones to avoid the existence of privacy-infringing virus software; learn about related information Network knowledge, proficient application of network technology, to encrypt their own private

ISSN: 2688-9323

information; raise awareness of rights protection, avoid infringements in time, and use legal weapons to protect their vital interests.

5.6. The Government Should Strengthen Supervision, Strictly Enforce the Law, and Establish a Corresponding Punishment and Protection System

To protect privacy in the era of big data, it is far from enough to rely solely on industry Self-discipline and civic awareness. Legislation needs to be improved and the focus is on implementation. The government must clarify the administrative division of various administrative departments, and the supervisory department must increase supervision, strictly stipulate the market access rules of the big data industry in advance, and improve the entry standards of the big data industry. For example, my country's data protection department can formulate specific balance test guidelines. Then a series of examples were issued to carry out typified analysis, and to provide a certain reference system for the uncertainty of the method of case analysis [14]; The incident severely cracked down on data operators' improper collection and use of private data, strictly monitored the "overlord clause" in the industry, and severely punished them if they were discovered; afterwards, they should promptly stop and impose corresponding administrative penalties if they discover infringements. The disciplinary system for infringement in the data industry increases the criminal cost of infringement by enterprises, effectively implements various legal measures, maintains legal authority, and protects citizens' privacy.

6. Concluding Remarks

In summary, "If all rights are a bunker, which not only protects what people have now, but also preserves them what they cannot have otherwise, then it can be predicted that with the passage of time and people's vision expand, there will be more and more bunkers in the society. Behind the bunkers, we will have more and more specific interests that need to be sheltered." [15] In the era of big data, with the rapid development of the Internet and the economy, data applications have become an inevitable trend of the times, ranging from transportation and medical assistance in life to national governance, chasing crime, combating terrorism, our lives, our era It is destined to be inseparable from the application of data. In this era when data application and leakage are inevitable, we cannot blindly reject the use of data, appropriately transfer individual rights, and take appropriate measures in a timely manner to integrate various subjects, which can not only effectively protect us The data information of the company will not be abused, and the value of data information can be fully utilized to maximize economic benefits, realize mutual benefit, interconnection and interaction between big data applications and personal information protection, and welcome the warm spring of the big data era.

References

[1] Xiong Hao-nan, Zhao Rui-nan. The reasonable boundary of data privacy-the conflict and resolution of privacy protection and data application [J]. Journal of East Liaoning University 2018 (8): 56-59.

[2] Zhang Li. Research on the Protection of Privacy in the Big Data Surveillance Society [J]. Books and Information. 2018: 71-79.

[3] Gartner.IT Glossary: Big Data [EB/OL]. [2017-09-03].http://www.gartner.com/it-glossary/big-data/.

[4] (U.S.) Sanil Soles. Kuang Bin, translated. Big Data Governance [M]. Beijing: Tsinghua University Press, 2018 (8): 3-4.

[5] Cheng Xueqi, Zhang Tieying, Liu Yahui, Jin Xiaolong. Personal privacy protection in the era of big data [J]. Computer Research and Development, 2015 (1): 229-247.

ISSN: 2688-9323

[6] Yuan Xue. Privacy protection in the era of big data [J]. Journal of Shandong Agricultural Engineering College, 2014 (3): 99.

[7] Tian Xinling. The Paradox of Public Data Opening and Personal Privacy Protection [J]. Journalism University, 2014 (6): 57-60.

[8] Zhang Xinbao. From Privacy to Personal Information: The Theory and Institutional Arrangement of Re-evaluation of Interests [J]. China Law, 2015 (3): 41-49.

[9] Deborah N.Pearlstein.Before Privacy,Power:The Structural Constitution and the Challenge of Mass Surveillance [EB/OL].[2017-04-05]. http://ssrn.com/abstract=2947092.

[10] Chen Xu. Exploring the privacy protection in the era of big data from "human flesh search" [J]. Legal Expo, 2019 (2): 128-129.

[11] Fan Jinxue. The Legislative Review and Improvement of Privacy in my country [J]. Law Journal, 2017 (5): 39.

[12] Li Weiwei, Meng Gaozheng. Criminal Law Protection of Privacy Based on the Background of Big Data [J]. Legal System and Society, 2018 (12): 15-17.

[13] Yao Wanqin. How should the criminal law deal with the "anxiety" of digital copyright protection in the era of big data [J]. Journal of Chongqing University of Posts and Telecommunications, 2016: 30-35.

[14] Xie Lin, exemption from legitimate interests in the use of personal information in the era of big data [J]. Politics and Law Forum. 2019(1).

[15] Li Lifeng, The right to be forgotten in the context of localization: the procedural construction of personal information rights [J]. Journal of Wuhan University, 2019(3).