




ORIGINAL

Research on the Issues and Paths of Citizen Privacy Protection in China in the Era of Big Data

Investigación sobre los temas y caminos de la protección de la privacidad de los ciudadanos en China en la Era del Big Data

Wuguang Wei¹  , Nazura Bt. Abdul Manap¹  , Mohamad Rizal Bin Abd Rahman¹  

¹Faculty of Law, Universiti Kebangsaan Malaysia (UKM). Bangi, Selangor Malaysia, 43600.

Cite as: Wei W, Nazura Bt. AM, Bin Abd Rahman MR. Research on the Issues and Paths of Citizen Privacy Protection in China in the Era of Big Data. Salud, Ciencia y Tecnología. 2024;4:.1208. <https://doi.org/10.56294/saludcyt2024.1208>

Submitted: 01-02-2024

Revised: 21-05-2024

Accepted: 14-08-2024

Published: 15-08-2024

Editor: Dr. William Castillo-González 

ABSTRACT

The development of big data technology has brought great impact and changes to social governance, and poses a great threat to personal privacy security, but it also effectively promotes the intellectualization of lifestyle, personalized service and scientific decision-making. At present, due to the imperfect legal system, the non-standard management of practitioners, and the weak awareness of personal privacy protection, cases of information security infringement occur from time to time. This paper analyzes the existing problems in the field of privacy protection and the reasons for privacy disclosure in the era of big data, and summarizes the important enlightenment of foreign privacy protection experience to the protection of privacy rights of Chinese citizens at this stage by drawing lessons from the successful practical experience of American industry self-regulation model, European Union legislative protection model and British technology control model. This paper puts forward specific measures to establish and improve the protection mechanism of citizens' privacy in the era of big data in China, that is, to strengthen legislative supervision and system formulation, to protect personal privacy through data desensitization, data encryption, data access control and data security audit technology; Improve the awareness and ability of personal privacy protection and other governance methods.

Keywords: Citizen Privacy Protection; Big Data; Similarities and Differences; Comparative Perspective.

RESUMEN

El desarrollo de la tecnología big data ha traído un gran impacto y cambios a la gobernanza social, y plantea una gran amenaza a la seguridad de la privacidad personal, pero también promueve efectivamente la intelectualización del estilo de vida, el servicio personalizado y la toma de decisiones científicas. En la actualidad, debido al sistema legal imperfecto, la gestión no estándar de los profesionales, y la escasa conciencia de la protección de la privacidad personal, los casos de violación de la seguridad de la información se producen de vez en cuando. Este artículo analiza los problemas existentes en el campo de la protección de la privacidad y las razones para la divulgación de la privacidad en la era del big data, y resume la importante ilustración de la experiencia de protección de la privacidad extranjera para la protección de los derechos de privacidad de los ciudadanos chinos en esta etapa, extrayendo lecciones de la experiencia práctica exitosa del modelo de autorregulación de la industria estadounidense, el modelo de protección legislativa de la Unión europea y el modelo de control tecnológico británico. Este documento propone medidas específicas para establecer y mejorar el mecanismo de protección de la privacidad de los ciudadanos en la era del big data en China, es decir, para fortalecer la supervisión legislativa y la formulación del sistema, para proteger la privacidad personal a través de la desensibilización de datos, el cifrado de datos, el control de acceso a datos y la tecnología de auditoría de seguridad de datos; Mejorar la conciencia y la capacidad de la protección de la privacidad personal y otros métodos de gobierno.

Palabras clave: Protección de la Privacidad Ciudadana; Big Data; Similitudes y Diferencias, Perspectiva Comparativa.

INTRODUCTION

With the rapid development of Internet technology, big data has become an indispensable part of modern society. Businesses, government agencies and even individuals are seeking value in the growing amount of data, which brings unprecedented convenience and efficiency. However, with the advent of the era of big data, the issue of citizen privacy protection has become increasingly prominent and has become an urgent social problem to be solved.⁽¹⁾ The frequent leakage of personal information not only violates the privacy of citizens, but also causes widespread social concern and legal disputes. For example, personal information collected through Internet search, social media, e-commerce and other channels, if not properly protected, can easily be illegally obtained and abused, thus causing serious harm to individuals.

At present, China has formulated a series of relevant laws and regulations on the protection of personal privacy, but there are still some problems such as difficult implementation and insufficient supervision. In addition, the public's awareness of personal privacy protection is relatively weak, lacking the necessary protective measures and capabilities. Therefore, exploring the problems and paths of privacy protection in the era of big data is not only the need of law and policy, but also the necessary condition to improve the public's awareness and ability of privacy protection. The purpose of this study is to deeply analyze the challenges of privacy protection of Chinese citizens in the era of big data, and to propose corresponding solutions.⁽²⁾ By formulating and improving relevant laws and regulations, establishing data protection management system and industry norms, and strengthening the supervision of data collection, processing and use, the public's awareness and ability of personal privacy protection can be improved in order to achieve the purpose of effectively protecting citizen's privacy. The research on the problems and paths of privacy protection in the era of big data will not only help to improve the legal system of privacy protection in China, but also promote the awareness of personal information security of citizens, and provide theoretical support and practical guidance for building a safer and healthier network environment.

Privacy in the era of big data

Right of privacy

The right of privacy refers to the right of a natural person to enjoy the peace of his private life and the protection of his private life information according to law, and not to be disturbed, known, used, disclosed and made public by others. The main meaning of the right of privacy includes: the subject of the right of privacy can only be a natural person; the content of privacy includes the information of private life and private sexual life; The ways of violating the right to privacy usually include disturbing the peace of natural person's life, probing into the secrets of natural person's private life, disclosing, publicizing to others, or using without permission after knowing the privacy of others. The main contents of the right to privacy include: the right to live in peace, the right to keep personal life information secret, the right of personal communication secret and the right of personal privacy use.⁽³⁾ The right of privacy is a kind of basic personality right. At present, the right of privacy is not perfect in our country's law, and it is still a controversial topic. Privacy paradox refers to the phenomenon that although Internet users perceive the existence of privacy risks, they will not take effective privacy protection actions, and there is a general contradiction between user's perception of privacy risks and their uploading of a large number of personal information. The study found that web users are not ignorant of these threats, but rather are very concerned about their privacy.

Privacy risks brought about by the development of big data technology

With the development of big data technology, the automation and intelligence of data processing has become an important factor to promote the progress of the industry.⁽⁴⁾ This trend not only improves the efficiency of data processing, but also changes the way and strategy of personal privacy protection to a great extent. The application of automation and intelligent technology makes the process of data collection, processing and analysis faster and more accurate. Through algorithms and machine learning models, the system can automatically identify and classify large amounts of data, thus reducing the need for human intervention. This automated approach greatly reduces the risk of data leakage and improves the efficiency of data processing. However, automation and smart technologies also bring new privacy challenges. Because algorithms may be biased and erroneous, the results of automated processing may lead to injustice or invasion of personal privacy. In addition, the application of intelligent technology may also be used to monitor and track personal information, raising concerns about privacy.⁽⁵⁾ In the era of big data, there are many kinds of privacy violations.

table 1 illustrates some common privacy violations.

Serial number	Type of problem	Parties involved	Scope of influence
1	Data breach	Individual users, enterprises,	Extensive
2	Identity theft	Individual users, enterprises,	Extensive
3	Misuse of ad targeting	Individual users, advertising companies,	Specific groups
4	Social engineering attacks	Individual users, enterprises,	Extensive
5	Privacy violations of smart devices	Individual user	Extensive
6	Deep forgery technology	Individual user	Extensive
7	Abuse of personal information	Individual user	Extensive
8	Illegal surveillance	Individual user	Specific groups
9	Third-party data sharing	Individual users, enterprises,	Specific groups

Data leakage is one of the most common types of privacy violations. According to Apple’s recent data breach report, a staggering 2,6 billion personal records were leaked worldwide in 2021 and 2022, and about 1,5 billion personal records were leaked in 2022 alone. In 2023, the scale of global data leakage will reach a record high, with sensitive data of 360 million people being leaked in the first nine months, 20 % higher than in the whole year of 2022. On May 1, Verizon’s Data Breach Investigation Report 2024 showed that DBIR had analyzed 30 458 data security incidents in 2024, of which 10 626 were confirmed to have data breaches, with the most serious data breaches in education (1537) and professional science and technology services (1314). Medical and health industry (1220 cases), financial and insurance industry (1115 cases), public administration (1085 cases).

The education industry has become the most serious area of annual data leakage incidents, with internal mis-operation, misconfiguration, external leakage, external attacker’s blackmail intrusion, vulnerability attacks and other problems intertwined, which are the main culprits of data leakage in the industry. The number of data leakage incidents in different industries is shown in figure 1.

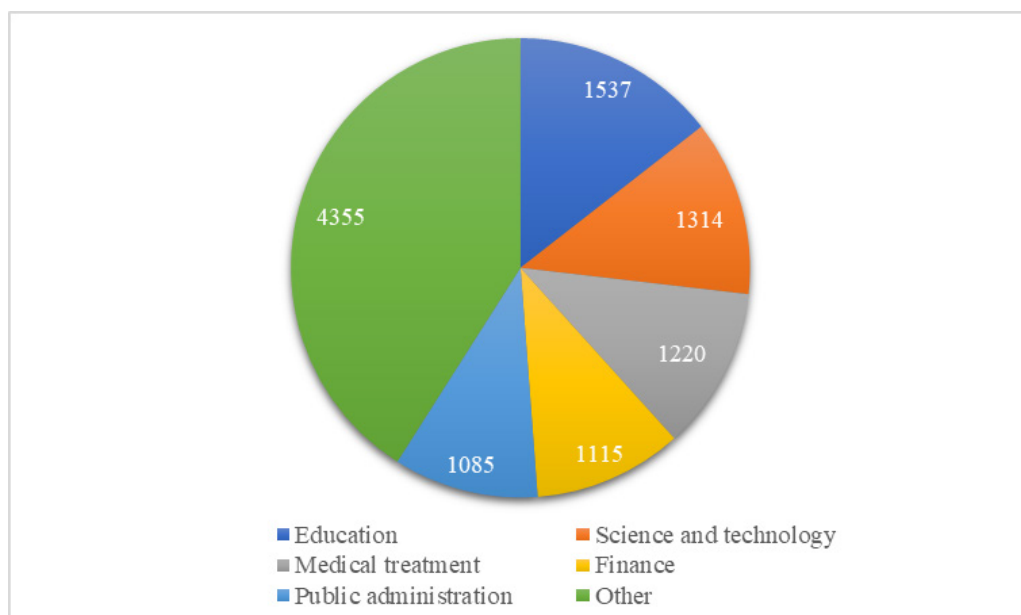


Figure 1. Number of data leakage incidents in different industries

New features of privacy in the era of big data

In the era of big data, privacy infringement will exist as “senseless harm”. The so-called senseless harm means that the violation of citizen’s privacy exists objectively, but the subject of privacy does not perceive the harm. The generation of senseless injury is based on the objective characteristics of the existence of big data. On the one hand, in the era of big data, almost all the words and deeds of citizens will leave data traces and become part of the database. On the other hand, after the data is retained in the database as an objective existence, the parties do not know whether and how it is used. In a sense, the social harm caused by the injury without feeling is more serious. Because of the immediate feeling of the injury, the feeling injury can be terminated as soon as possible and reduce the consequences of the injury. Due to the senselessness of

the injury, the non-feeling injury makes the injury lag and continue, and eventually leads to the expansion of the consequences. In the era of big data, under the impact of the change of communication mode, privacy is constantly squeezed and frequently lost, which leads to fundamental changes in the subject, mode and consequences of privacy infringement. In the era of big data, under the impact of the change of communication mode, privacy is constantly squeezed and frequently lost, which leads to fundamental changes in the subject, mode and consequences of privacy infringement.

Foreign models of citizen privacy protection

Industry self-discipline model

Industry self-regulation mode is a self-management mode that reduces the government's management and control of the industry, establishes self-regulatory organizations independently within the industry, formulates self-regulatory treaties, and is observed within the individual organizations of the industry. This mode has been fully developed in the United States. Because the development of the internet industry in the United States is in the leading position in the world, and the rapid development of the Internet industry also makes it inconvenient to be rigidly managed by the government. The United States is divided into two areas in the protection of citizens' online privacy. One is aimed at the public sphere, such as communication, health care, education, etc. In order to protect citizen's information and privacy in the public sphere and prevent them from being infringed by the government, the United States has formulated a relatively perfect departmental protection law to protect them in the form of legislation. The other is the non-public sphere. The Internet industry in the United States is developing rapidly, and technological innovation is also very fast. It is impossible to formulate laws and regulations to match its speed. Therefore, in this field, there are basically no compulsory government management measures.

Therefore, corresponding to the division of the protection of citizen privacy by the state, the self-discipline model of the industry in the United States is also divided into two aspects. The first is that the industry consciously abides by the relevant laws and regulations of the state.⁽⁶⁾ The United States is a pioneer in the implementation of industry self-regulation model in the Internet industry, which is determined by the national conditions of the United States advocating freedom, and based on the idea of free economic model, the development environment of the United States from top to bottom is more relaxed, practitioners are unwilling to be more interfered, and the government is willing to delegate power to enterprises and individuals. However, the premise for the government to allow industry self-regulation is to retain the government's ability to control it. The relatively perfect legal system and conscious industry consciousness of the United States have become the object of study in the process of protecting citizen's privacy rights.⁽⁷⁾

Legal regulation model

For the protection of citizens' privacy rights, there are significant differences between the legal regulation model and the industry self-regulation model, and the legal regulation model is more complete in the European Union. The mode of legal regulation is to clarify the legal system of the Internet industry and the norms for the protection of citizen's network privacy in the form of legislation. Compared with the development of the Internet industry, the European Union pays more attention to the privacy rights of citizens, so this legal regulation model has been produced and developed well in the European Union (Aho & Duffield, 2020). At the same time, the model has made detailed provisions for specific judicial procedures and remedies after the event, which can be clearly understood by practitioners and citizens, thus regulating the behavior of organizations in the industry in collecting, using and processing data, and also enabling users to know whether the organization's behavior is legal, judge right and wrong, and provide information, which is conducive to the protection of citizen's network privacy rights.

EU countries also advocate the establishment of a special committee to protect network privacy, and urge its member States to formulate laws in line with the interests of ordinary EU citizens based on the basic spirit of EU legislation and in accordance with their own national conditions, so as to protect the privacy of all citizens of member States in the network. Most member States have their own personal network privacy laws and regulations, which are all based on the consensus of the European Union on the protection of citizen's network privacy rights, and can protect all citizens of member States from illegal infringement of personal privacy. Because of historical reasons, after the Nazi dictatorship, the European people attach great importance to the protection of human rights after national independence, and Europeans believe that the most basic human right is the right to privacy. Therefore, immediately after the end of the war, Europe wrote the protection of personal privacy into the law, so Europe became the first region to use legal regulation to protect the right of network privacy, and also the first region to propose the protection of personal data into legislation. After a long period of development, the EU's laws on the protection of citizen privacy rights on the Internet have become more comprehensive and specific, leading the world.

Technical control model

The technical control model, as its literal meaning, refers to the protection of citizen's online privacy through technology, which is the most typical development in the United Kingdom. The technical control model, through the use of privacy data protection software, allows citizens to decide for themselves whether to accept the services of the organization and whether to provide them with personal privacy data.⁽⁸⁾

Britain's network coverage and network infrastructure construction are at a very high level, and the high quality of the people makes the Internet technology in Britain develop continuously. At the same time, the UK has been highly forward-looking and leading in digital strategy and digital construction for a long time, and has achieved great results.⁽⁹⁾ The UK's e-government construction has also been in the world's leading level, so it has a certain inherent advantage in the development of advanced network technology. When a user installs and uses a specific network privacy protection software, every time the website or application is ready to start collecting the user's personal privacy data, the software will immediately prompt the user that the website is collecting your privacy data, and prompt the content and types of data that may be exposed next, so that the user can follow the prompt. Whether to provide information and whether to continue to accept the services of the organization are judged according to the necessity of the collected information and the risk of information leakage. In addition, the software can also preset the scope and content of privacy permission collection, that is, which personal privacy information can be provided under what circumstances, and which personal information cannot be collected.

Enlightenment of the three models to China

We list the advantages and limitations of the above three modes, and obtain table 2.

Model	Area	Main features	Advantage	Limitations	Field of application
Industry self-discipline model	America	Reduce government intervention and industry self-management	High flexibility, quickly adapt to industry changes	Lack of uniform standards, regulation may be inadequate	Internet and technology industry
Legal Regulation Model	European Union	To clarify privacy protection norms in the form of legislation	Legal protection is complete, Strong protection of civil rights	Regulatory updates may lag behind technological developments	Industry-wide, with special emphasis on personal data protection
Technical control mode	The UK	Protecting privacy through technological means	Strong user control and wide technical adaptability	Strong dependence on technology, requires knowledge of the user	Information technology, digital services

Considering the actual situation of our country, we should adopt the protection mode based on legal regulation, learn from the industry self-discipline mode, and supplemented by the technology control mode, so as to form a collaborative governance mode of government, institutions and individual citizens, and give full play to the advantages of different governance subjects.

First, the legal regulation mode is the main mode. In the current situation of our country, the perfect legal system will play an important supporting role in the protection of citizens' privacy rights, clarify the personal privacy and network privacy that citizens do enjoy, and refer to the current legal system of other countries in the world to formulate a special network privacy protection law. To stipulate the rights and obligations of different subjects, to clarify the legitimate principles and legal means for industries and organizations to collect and process citizen privacy information, and to improve the management and supervision system to ensure the implementation of laws and regulations are effective ways to govern the protection of citizen privacy rights in China at this stage. At present, China's Consumer Rights and Interests Protection Law has relevant provisions for operators to protect consumer personal information rights.⁽¹⁰⁾

Second, learn from the industry self-discipline model. This model avoids too much state intervention and restriction, gives the industry more room for development, and can promote and supervise the rapid and healthy development of the industry.⁽¹¹⁾ When formulating privacy protection clauses, different industries can more closely integrate their own industry characteristics to make privacy protection clauses more targeted. Therefore, when constructing the industry self-discipline mechanism of privacy protection in China, on the one hand, we should pay attention to discovering the new characteristics of big data and provide reference for the improvement of the law. On the other hand, we should pay more attention to the self-discipline of

various industries and use flexible industry self-discipline to make up for the temporary vacancies in laws and regulations. At the same time, we should strengthen the training of information protection skills and awareness of network service providers and related practitioners, and cultivate a high-quality team of law-abiding, honest and self-disciplined.

Third, supplemented by technical protection mode. Continuously update network technology and protection technology, so that users can control the initiative to protect network privacy and choose whether to use data services provided by the government or agencies. Clearly inform the rules of using personal information, such as the purpose of forming user portraits and portraits, whether they are used to push commercial advertisements, etc. Clearly inform users of the right to access, delete and correct their personal information, the way to achieve, restrictions, etc. This action has played a certain role in supervising the rectification of the industry, which is conducive to strengthening the protection of citizen's information, but because it is still prone to problems such as untimely technological updates and weak awareness of the protection of citizens' privacy rights, so this model can play a relatively limited role in protection.

Legal and institutional measures to protect personal privacy

Improve the legal framework for privacy protection

In the era of big data, personal information protection is facing unprecedented challenges. In order to cope with these challenges, China needs to further improve the legal framework of personal information protection. This includes formulating and amending relevant laws and regulations, establishing clear legal responsibilities and obligations, and establishing a sound regulatory mechanism. It is necessary to strengthen the legal norms for the collection, processing and use of personal information. At present, China has the Network Security Law and Personal Information Protection Law and other relevant laws, but there are still some loopholes and shortcomings in the actual operation.⁽¹²⁾ Therefore, it is necessary to further improve these laws, clearly stipulate the rights of data subjects and the obligations of data processors, strengthen the supervision of the data processing process, and ensure that the security and privacy of personal information are effectively protected. We need to establish a sound data protection management system and industry norms.

In addition to the legal provisions, it is also necessary to establish a complete set of data protection management system within the organization, including data classification, data access control, data encryption and other provisions. At the same time, it is also necessary to promote the establishment of unified data protection standards and norms within the industry to promote the orderly development of data protection work.⁽¹³⁾ At the same time, the regulation of data collection, processing and use needs to be strengthened. This includes the review and supervision of data processing activities to ensure that data processing activities meet the requirements of laws and regulations. At the same time, it is also necessary to strengthen the punishment for violations of data protection regulations, and enhance the legal responsibility and normative awareness of data processors. Only by establishing a sound regulatory mechanism and means of law enforcement can we ensure the effective implementation of the law. For example, a special personal information protection regulatory body can be set up to supervise and inspect the personal information processing activities of enterprises and organizations, and to punish illegal acts. At the same time, we can also carry out public education and publicity activities to raise public awareness and awareness of personal information protection, and form an atmosphere of personal information protection in which the whole society participates.

Establish a management system for privacy protection

In the era of big data, the protection of personal privacy has become an important issue. To this end, the establishment of data protection management system and industry norms is an essential step. These measures aim to ensure that the security and privacy of personal information in the process of data collection, processing, storage and transmission are effectively guaranteed.⁽¹⁴⁾ First, existing data protection laws and regulations need to be reviewed and revised to adapt to emerging challenges in the big data environment. For example, we should strengthen the definition of the sensitivity of personal data, clarify the responsibilities and obligations of data processors, and the procedures and principles to be followed in the processing of personal data under specific circumstances. Second, develop industry specifications specifically for data protection. This includes, but is not limited to, data classification criteria, data access control policies, data encryption technology requirements, etc.

Through these specifications, specific operational guidelines can be provided for various industries to help enterprises better implement data protection measures in their daily operations. Establishing a regulatory body or commission for data protection is essential. These institutions are responsible for monitoring and evaluating whether the data protection measures of enterprises conform to laws, regulations and industry norms, and imposing penalties for violations.⁽¹⁵⁾ At the same time, regulators should also play a guiding and advisory role to help enterprises solve problems encountered in data protection practices. In order to promote exchanges and cooperation in data protection at home and abroad, it is also very important to promote the formation

of unified data protection standards and norms. By participating in international organizations and forums and drawing on mature international experience and practices, we can speed up the improvement of data protection laws, regulations and industry norms in China.

Optimize regulatory mechanism for privacy protection

Firstly, government departments should not only give full play to the advantages of administrative supervision, but also clarify the supervisory responsibilities of other departments from the system, and establish an accountability mechanism for administrative responsibility tracing, so as to achieve the effective protection of citizen privacy by combining the three modes of pre-examination, in-process examination and post-examination. Among them, pre-examination can be achieved by setting permission, in-process examination and post-examination can be achieved by irregular spot checks, special reports, social supervision and other ways.

Secondly, a special and unified department should be set up to take charge of data security supervision. A special and unified data security supervision department is conducive to the combination of several forces, the unified performance of regulatory responsibilities, the exercise of regulatory power, and the effective protection of data in a more orderly manner.

Thirdly, we need to strengthen the regulation of Internet service providers, especially websites. Avoid the situation that network users are forced to agree to contracts because they need to use services, and ensure that citizens can effectively control their personal information.

Fourthly, the relevant government departments should strengthen supervision, at the same time, because the work really needs to collect personal data of citizens, organizations and institutions should also establish a standardized management system, self-management, in the process of obtaining and using information to ensure the security of information, in particular, attention should be paid. Without the consent of the parties, the personal information of the parties shall not be provided to the relevant data agencies without authorization.

Fifthly, after the occurrence of security incidents such as personal information leakage, law enforcement and investigation should be strengthened, and enterprises with violations of laws and regulations should be punished and the final punishment results should be publicized.

In the process of supervising and dealing with the protection of citizen privacy rights, we can use a variety of ways, such as notification interviews, credit scoring and so on, to further enhance the cost of enterprises' violations of laws and regulations, and to effectively supervise enterprises, so that they can more actively assume the responsibility of protecting personal information and fulfill the obligation of protecting personal information.

Technical means and measures to protect personal privacy

Data desensitization technology

Data desensitization technology refers to the processing of sensitive data to ensure that business needs and data analysis purposes can be met without revealing personal privacy. This technology mainly includes data mask, data replacement, data forgery and other methods. Data masking is the partial or complete replacement of sensitive information with other characters or random numbers to prevent sensitive information from being directly identified and acquired. For example, separate the last and first name letters in a name, or replace the middle four digits of a phone number with an asterisk.⁽¹⁶⁾ Data replacement replaces sensitive information with non-sensitive values, but still retains some business logic. For example, replace the date of birth in the ID number with the age, or replace the email address with an anonymous email address. Data forgery is the replacement of sensitive information with fictitious data that still conforms to business rules and logic. For example, replace a name with a randomly generated dummy name, or replace a phone number with a dummy phone number.

In the era of big data, data desensitization technology plays an important role in protecting personal privacy. First of all, it can effectively reduce the risk of data leakage. By desensitizing sensitive information, even if the data is illegally obtained, it is impossible to directly identify individuals. Secondly, data desensitization technology can also guarantee the commercial value of data. Through desensitization, the data can still be used for data analysis and decision support without revealing personal privacy. In practical applications, data desensitization technology needs to be selected and adjusted according to specific business scenarios and data characteristics. For example, for financial data involving personal privacy, more stringent desensitization measures can be adopted, such as data encryption and data desensitization. For data related to public safety, more relaxed desensitization measures can be adopted to facilitate the rapid transmission and processing of data.

Data encryption technology

Data encryption technology is one of the important means to protect personal privacy. It encodes and decodes data so that it cannot be read or tampered with without authorization. Data encryption technology is

divided into two main categories: symmetric encryption and asymmetric encryption. Symmetric encryption is the most common encryption method, and its principle is to use the same key to encrypt and decrypt data. The advantage of symmetric encryption algorithm is that it is fast and suitable for the encryption of large amounts of data. However, symmetric encryption has a problem, that is, the distribution and management of the key is more difficult, if the key is leaked, then the encrypted data will be cracked. Asymmetric encryption technology is another commonly used encryption method, which uses a pair of public key and private key to encrypt and decrypt data. The public key can be made public, and anyone can use it to encrypt data, but only the person who holds the private key can decrypt the data.⁽¹⁷⁾ The advantage of asymmetric encryption technology is to solve the problem of key distribution and management in symmetric encryption, but its disadvantage is that the computing speed is relatively slow, which is not suitable for large-scale data encryption processing.

In practical applications, in order to give consideration to both encryption efficiency and security, hybrid encryption technology is often used. Hybrid encryption technology combines the advantages of symmetric encryption and asymmetric encryption, which can not only ensure the security of data, but also improve the efficiency of encryption. For example, when transmitting sensitive information, you can use asymmetric cryptography to generate a temporary symmetric encryption key and then use symmetric cryptography to encrypt the data. This not only ensures the security of data, but also improves the efficiency of encryption. In addition to symmetric encryption and asymmetric encryption, there are also some new encryption technologies, such as quantum encryption and block chain encryption. These new encryption technologies have higher security and efficiency, but they are still in the stage of research and application, and have not been widely used in practical scenarios.

Data access control technology

With the advent of the era of big data, data access control and permission management have become an indispensable technical means to protect personal privacy. In this session, focus on how to effectively restrict access to sensitive data and ensure that only authorized users can obtain, use, or modify this information. To achieve this goal, we need to take a series of measures and strategies. Data access control first requires clear classification and labeling of data. According to the sensitivity and importance of the data, it is divided into different levels, and the corresponding access rights are set for each level. In this way, you can ensure that access to high-sensitivity data is strictly limited and that access to low-sensitivity data is more relaxed.

It is also crucial to establish a fine-grained permission management mechanism. This means not only differentiating the access rights of different roles and positions, but also customizing the scope and depth of data access for each user's specific job needs. For example, a project manager may need access to data for the entire project, while an ordinary employee may only have access to a portion of the data that is directly related to his or her work. Data access control and privilege management is one of the key technical means to protect personal privacy. Through the implementation of meticulous rights management, combined with advanced technical means and strict legal policies, the risk of personal privacy disclosure can be effectively reduced, so as to safeguard the privacy rights and interests of citizens in the era of big data.

Data security audit technology

The Marrakesh Treaty requires Parties to place appropriate limitations on technical measures in copyright laws to facilitate the production and use of accessible formats by beneficiaries. China's copyright law focuses more on copyright protection and the legitimate use of technological measures. This provision in the Marrakesh Treaty is actually seeking a balance between copyright protection and the rights and interests of people with reading disabilities. It allows, in certain circumstances, the restriction or circumvention of technical measures of a work in order to provide a work in an accessible format for the dyslexic. Such exceptional measures help to ensure that dyslexics have equal access to cultural and intellectual outcomes, while also encouraging the development and use of technological solutions adapted to the needs of dyslexics.

In contrast, China's copyright law takes a more cautious stance on copyright protection and the legitimate use of technological measures. Chinese law emphasizes the protection of the legitimate rights and interests of copyright holders, including through technological measures to prevent unauthorized copying and dissemination.⁽¹⁸⁾ At the same time, China's copyright law also recognizes the special needs of people with reading disabilities, and has introduced corresponding provisions in the revision to allow the production and provision of works in accessible formats under certain conditions. Chinese copyright law pays more attention to balancing the rights and interests of copyright owners and public interests when implementing restrictions on technological measures. This means that while ensuring the effective protection of copyright, it also provides a legal way for people with reading disabilities to obtain works. In this way, China's copyright law aims to maintain a fair and reasonable copyright environment, which not only protects the legitimate rights and interests of creators, but also meets the needs of special groups and promotes the overall interests of society.⁽¹⁹⁾

Comparison of several technologies

At the technical level, data encryption and desensitization technology provide basic support for data security audit. Encryption technology ensures the security of data during transmission and storage, while data desensitization reduces the risk of data leakage by replacing or masking sensitive information. At the same time, the implementation of strict data access control and permission management is also an important means to ensure data security. Data security audit and risk assessment are necessary to protect citizens' privacy in the era of big data. Through scientific and reasonable audit and evaluation process, we can effectively find and solve the security risks in the process of data processing, and protect the security and privacy rights of citizen personal information. We compare the above techniques and get table 3.

Technical name	Application scenario	Advantage	Limitations
Data encryption	Online banking, email, cloud storage, etc.	Strengthen data security to prevent unauthorized access	The encryption and decryption process may affect performance; Key management is required
Data desensitization	Data sharing, testing, development environment	Protect privacy while retaining the analytical value of your data	Complex logic may be required to ensure data consistency
Access control	Enterprise internal system and network resource management	Refined access management to reduce the risk of data leakage	Complex configuration, requiring periodic review of permission settings
Data security audit	Enterprise Data Management, Risk Assessment, Compliance	Timely detection and correction of security vulnerabilities to improve data management transparency	Need for expertise and tools; There may be audit blind spots.

Improvement of the Awareness and Ability of Personal Privacy Protection

Enhance the awareness of personal privacy protection

In order to better implement the Marrakesh Treaty and harmonize it with domestic laws, one of the suggestions for improvement of China's copyright law is to clearly define the scope of application of the treaty. Marrakesh Treaty is the first international intellectual property treaty in the world with copyright limitations and exceptions as its main content. Its core purpose is to achieve human rights through copyright law and policy tools, especially to ensure that people with print disabilities, including people with visual disabilities, can enjoy works and receive education equally. When implementing the treaty, China should face up to the theoretical disputes, coordinate the objectives of copyright protection and human rights promotion according to its national conditions, and make corresponding institutional arrangements.⁽²⁰⁾ This includes defining the types of works to which the treaty applies, clarifying the definition of beneficiaries, and establishing specific requirements for the production and availability of accessible formats.

In addition, China's copyright law should take into account the mandatory obligations of the treaty, establish clear provisions on copyright restrictions and exceptions for people with reading disabilities, and ensure that these restrictions and exceptions will not cause unreasonable damage to the legitimate rights and interests of copyright owners. It is important to recognize that the treaty's promotion of international exchange of accessible format publications has not been fully implemented. Consequently, proposals for the enhancement of China's copyright law should encompass measures that address cross-border dealings, with the aim of advancing the global exchange and distribution of publications in accessible formats.⁽²¹⁾

Strengthen the legal popularization of privacy protection

At present, Chinese citizens' awareness of data protection laws and regulations is generally not high, which not only affects the personal information security of citizens, but also restricts the effective implementation of data protection laws and regulations. It is necessary to strengthen legal publicity and education for citizens through multiple channels. Government departments should strengthen the publicity of data protection laws and regulations, make use of media resources such as television, Internet, newspapers and periodicals, popularize data protection related knowledge, and raise citizen's awareness of data protection laws and regulations. At the same time, various lectures, seminars and other activities can be held to invite experts and scholars to interpret data protection laws and regulations in depth and shallowly, so that citizens can better understand and master relevant legal knowledge.⁽²²⁾

Strengthen the content of legal education in school education. The school is an important place to cultivate the quality of citizens, and the education of data protection laws and regulations should be incorporated into

the school education system, through classroom teaching, extracurricular activities and other forms, so that students can establish a correct concept of personal information security from an early age, and enhance their awareness and understanding of data protection laws and regulations. Through online articles, videos and other forms, the knowledge and skills of personal privacy protection are popularized to the public, and the public's awareness of privacy protection is raised.⁽²³⁾

At the same time, experts and scholars can be invited to write relevant articles or publish books to discuss in depth the problems and solutions of personal privacy protection, and guide the public to correctly understand and protect personal privacy. In addition, government departments should strengthen cooperation with enterprises and social organizations to jointly promote the popularization of data protection laws and regulations. As the main body of data collection and processing, enterprises should assume the responsibility of educating employees, strengthen their training and education on data protection laws and regulations, guide them to abide by relevant laws and regulations in their daily work, and protect user's personal information security. At the same time, social organizations can also give full play to their professional advantages, provide advisory and guidance services for citizens on data protection laws and regulations, and help them better safeguard their rights and interests.

Improve personal information security literacy

It is particularly urgent to enhance the public's awareness and ability of information security. Education and training are effective ways to improve personal information security literacy. By offering courses related to information security, holding public welfare lectures and seminars, we can help the public understand the risks and preventive measures of personal information leakage, and learn how to protect their privacy. In addition, the government and enterprises should also assume social responsibility, popularize information security knowledge to the public, and provide practical protection guidelines and tools. Individuals should take the initiative to protect their own information security. For example, change passwords regularly, use complex and unique password combinations, and avoid sensitive operations in insecure network environments. At the same time, we should be alert to all kinds of phishing emails and fraudulent information, and not easily click on unknown links or download attachments from unknown sources.⁽²⁴⁾

On social media and other platforms, privacy rights should be set reasonably to control what information can be made public. In addition, it is also necessary to use technical means to improve personal information security. For example, the use of virtual private networks to access the Internet can encrypt network communications and protect personal data from theft. Installing and updating anti-virus software can prevent malicious software from entering personal devices and stealing information. Technologies such as digital signature and digital certificate are used to ensure the authenticity and integrity of data transmission. Only when everyone realizes the importance of information security and takes active measures to protect their privacy, can we ensure the security of personal information while enjoying convenient services in the era of big data.

Encourage professional institutions to carry out services

In the era of big data, personal privacy protection is facing unprecedented challenges. In order to meet these challenges, it is particularly important to encourage professional institutions to carry out privacy protection consulting services. Professional organizations can help enterprises and individuals better understand and deal with privacy protection issues by providing expertise and technical support. Professional organizations can provide targeted privacy protection advisory services. This includes conducting privacy risk assessment for enterprises, formulating privacy protection strategies, and optimizing data processing processes. Through professional consulting services, enterprises can better understand their privacy protection needs and formulate privacy protection measures that meet the requirements of laws and regulations. Professional organizations can also provide privacy protection training services.⁽²⁵⁾

Through training, employees can improve their awareness and awareness of privacy protection and learn how to better protect personal privacy in their daily work. At the same time, professional organizations can also provide relevant technical training for enterprises to help them master data encryption, desensitization and other technical means, so as to improve the level of data security. Professional organizations can also provide privacy protection audit services for enterprises. Through auditing, enterprises can find problems and shortcomings in privacy protection, and timely rectify and optimize them. At the same time, professional organizations can also provide privacy protection compliance assessment services for enterprises to help them ensure that their data processing activities meet the requirements of relevant laws and regulations. Encouraging professional institutions to carry out privacy protection consulting services can also promote the development of privacy protection industry. With the increasing demand for privacy protection, the role of professional institutions in the field of privacy protection will become more and more important. This is not only conducive to promoting the innovation and application of privacy protection technology, but also conducive to the formation of a sound privacy protection service system, providing more professional and efficient support

for personal privacy protection.

CONCLUSIONS

This article points out the existing problems of privacy protection in the era of big data, including the imperfect legal system, non-standard management of professional institutions, and weak awareness of personal privacy protection. The existence of these problems has led to frequent cases of information security infringement, which has attracted widespread social attention. The article draws on the successful practical experience of the United States, the European Union, and the United Kingdom in privacy protection issues, and summarizes the important insights of foreign privacy protection for China. On this basis, this article proposes specific measures such as strengthening legislative supervision, data desensitization, data encryption, data access control, and data security auditing, aiming to establish a sound mechanism for protecting citizens' privacy rights.

Through education and training, the public should understand the risks and preventive measures of personal information leakage, and learn how to protect their privacy. At the same time, the government and enterprises should also assume social responsibility, popularize information security knowledge, and provide practical protection guidelines and tools. Encouraging professional institutions to provide privacy protection services can not only help enterprises and individuals better understand and respond to privacy protection issues, but also promote the development of the privacy protection industry and promote innovation and application of privacy protection technologies.

REFERENCES

1. Aho, B., & Duffield, R. . Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 2020:49(2), 187-212. <https://doi.org/10.1080/03085147.2019.1690275>
2. Andrew J , Baker M .The General Data Protection Regulation in the Age of Surveillance Capitalism[J]. *Journal of Business Ethics*, 2021, 168.DOI:10.1007/s10551-019-04239-z.
3. Habrelian H .LEGAL PROTECTION OF MEDICAL PERSONNEL DURING ARMED CONFLICTS[J]. 2020. DOI:10.32518/2617-4162-2020-1-139-145.
4. Deepa N , Pham Q V , Nguyen D C ,et al.A survey on blockchain for big data: Approaches, opportunities, and future directions[J].*Future generations computer systems: FGCS*, 2022(131-):131. DOI:10.1016/j.future.2022.01.017
5. Elkawkagy M, Elwan E, Alsumayt A, et al. Elevating Big Data Privacy: Innovative Strategies and Challenges in Data Abundance[J]. *IEEE Access*, 2024. DOI:10.1109/access.2024.3357943
6. Fu A, Zhang X, Xiong N, et al. VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT[J]. *IEEE Transactions on Industrial Informatics*, 2020, 18(5): 3316-3326. <https://doi.org/10.48550/arXiv.2007.13585>
7. Hassan J, Shehzad D, Habib U, et al. [Retracted] The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR)[J]. *Computational intelligence and neuroscience*, 2022(1): 8303504. <https://doi.org/10.1155/2022/8303504>
8. Josphineleela R, Kaliappan S, Natrayan L, et al. Big Data Security through Privacy-Preserving Data Mining (PPDM): A Decentralization Approach[C]//2023 Second International Conference on Electronics and Renewable Systems (ICEARS). *IEEE*, 2023: 718-721. doi: 10.1109/ICEARS56392.2023.10085646.
9. Keshk, M., Moustafa, N., Sitnikova, E., & Turnbull, B. (2022). Privacy-preserving big data analytics for cyber-physical systems. *Wireless Networks*, 28(3), 1241-1249. <https://doi.org/10.1007/s11276-018-01912-5>
10. Lv Z, Qiao L, Hossain M S, et al. Analysis of using blockchain to protect the privacy of drone big data[J]. *IEEE network*, 2021, 35(1): 44-49. doi: 10.1109/MNET.011.2000154.
11. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era[J]. *BMC Medical Ethics*, 2021, 22: 1-5. DOI:10.1186/s12910-021-00687-3
12. Nair A K, Sahoo J, Raj E D. Privacy preserving Federated Learning framework for IoMT based big

data analysis using edge computing[J]. *Computer Standards & Interfaces*, 2023, 86: 103720. DOI:10.1016/j.csi.2023.103720

13. Nguyen T, Gosine R G, Warriar P. A systematic review of big data analytics for oil and gas industry 4.0[J]. *IEEE access*, 2020, 8: 61183-61201. doi: 10.1109/ACCESS.2020.2979678.

14. Ogbuke N J, Yusuf Y Y, Dharma K, et al. Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society[J]. *Production Planning & Control*, 2022, 33(2-3): 123-137. doi: 10.1080/09537287.2020.1810764

15. Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data privacy laws and their impact on financial technology companies: a review. *Computer Science & IT Research Journal*, 5(3), 628-650. <https://doi.org/10.51594/csitrj.v5i3.911>

16. Ramachandra M N, Srinivasa Rao M, Lai W C, et al. An efficient and secure big data storage in cloud environment by using triple data encryption standard[J]. *Big Data and Cognitive Computing*, 2022, 6(4): 101. <https://doi.org/10.3390/bdcc6040101>

17. Rizi M H P, Seno S A H. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city[J]. *Internet of Things*, 2022, 20: 100584. <https://doi.org/10.1016/j.iot.2022.100584>

18. Robertson, V. H. (2020). Excessive data collection: privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, 57(1). DOI: 10.54648/cola2020006

19. Sousa, S., Kern, R. How to keep text private? A systematic review of deep learning methods for privacy-preserving natural language processing. *Artif Intell Rev* 56, 1427-1492 (2023). <https://doi.org/10.1007/s10462-022-10204-6>

20. Talukder M S R. Digital Constitutionalism in Bangladesh to Protect Right to Privacy in the Big Data Regime[M]//*The Constitutional Law of Bangladesh: Progression and Transformation at its 50th Anniversary*. Singapore: Springer Nature Singapore, 2023: 317-334. https://doi.org/10.1007/978-981-99-2579-7_18

21. Tan L, Shi N, Yang C, et al. A blockchain-based access control framework for cyber-physical-social system big data[J]. *IEEE Access*, 2020, 8: 77215-77226. doi: 10.1109/ACCESS.2020.2988951.

22. Wang X, Guo Y, Zhao Y, et al. The New Progress and Methods of Privacy Protection on Medical and Health Big Data[C]//2022 14th International Conference on Software, Knowledge, Information Management and Applications (SKIMA). IEEE, 2022: 73-78. doi: 10.1109/SKIMA57145.2022.10029494.

23. Widanage C, Liu W, Li J, et al. HySec-Flow: privacy-preserving genomic computing with SGX-based big-data analytics framework[C]//2021 IEEE 14th International Conference on Cloud Computing (CLOUD). IEEE, 2021: 733-743. doi: 10.1109/CLOUD53861.2021.00098.

24. Wu X, Zhang Y, Wang A, et al. MNSSp3: Medical big data privacy protection platform based on Internet of things[J]. *Neural Computing and Applications*, 2022: 1-15. doi: 10.1007/s00521-020-04873-z

25. Zhao, B., Fan, K., Yang, K., Wang, Z., Li, H., & Yang, Y. (2021). Anonymous and privacy-preserving federated learning with industrial big data. *IEEE Transactions on Industrial Informatics*, 17(9), 6314-6323. doi: 10.1109/TII.2021.3052183.

FINANCING

No financing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Supervision: Nazura Bt. Abdul Manap.

Writing - proofreading and editing: Wuguang Wei.
Methodology: Mohamad Rizal Bin Abd Rahman.