International Journal of Humanity, Social Science & Legal Research Vol.2 No.1 2025
ISSN: 3078-8749

LEGAL REGULATION OF PERSONAL INFORMATION LEAKAGE IN THE CONTEXT OF DATA TRADING

Wang Huiling[1], Dong Ying[1,2], Wang Hong[1]

[1] Faculty of Economics & Law, Jingdezhen Vocational University of Art, Jiangxi, China

[2] Faculty of Education, SEGI University, Selangor, Malaysia

Submitted: 2025-01-02 Revised: 2025-01-27 Accepted: 2025-03-02

ABSTRACT

This paper focuses on the protection of personal information in the context of data transactions, with the core objective of exploring the legal regulation of personal information leakage, and endeavors to prevent the leakage of rights holders' information in the process of data transactions. In terms of research method, this paper comprehensively utilizes the literature analysis method and comparative analysis method to conduct in-depth research on the legal regulation of personal information leakage. Through the study, it is found that at the present stage, in the field of legal regulation of personal information leakage, there are still many problems such as insufficient legislation and defective regulatory system. Based on the above problems, this paper proposes a series of targeted solutions, including refining the provisions of personal information protection, formulating the rules of cross-border data flow, clarifying the authority and responsibility of the regulatory body, and strengthening the connection mechanism between judicial and administrative enforcement. Through the above efforts, this paper expects to build a more sound and perfect legal regulation system of personal information leakage, and then provide ideas and directions with reference value for the protection of citizens' personal information security.

Keywords: Personal Information Leakage; Legal Regulation; Personal Information; Protection Data Trading

1. INTRODUCTION

As technology continues to evolve, the world has entered the era of big data, where all kinds of behavioral traces are kept. Operations such as entering personal information when registering for an account or verifying a phone number when logging on to a website inadvertently result in the leakage of personal information. In recent years, with data becoming a key production factor and entering the trading field, the data trading market has continued to expand, and the protection of citizens' personal information is facing serious challenges. From precision marketing to financial and credit fields, from medical and healthcare to social entertainment, personal information is gradually being pushed from the hidden realm to the prominent position of risk under the hidden wave of data trading, which has triggered the public's deep concern about privacy protection and prompted all sectors of the society to attach great importance to and pay in-depth attention to the standardization of data trading and the security of personal information. It has taken about fifty years from the beginning of the information age to the enactment of legislation on personal information in China. In the early days, although China had the awareness of personal information prevention, the relevant laws and regulations were not yet perfect. The earliest legal regulation on personal information protection in China was the Decision on Strengthening the Protection of Network Information, which was passed in 2012, and it was not until the formal introduction of the Personal Information Protection Law in 2021 that a more comprehensive regulation on the protection of personal information was made. Internationally, the U.S. Privacy Act of 1974 is the world's earliest legislation on personal information, followed by Germany's Multimedia Act of 1974 (IuKDG). In terms of regulation, China adopts the model of coordination and division of labor to regulate individuals, enterprises and society; the European Union has set up an independent regulatory mechanism and a strict penalty mechanism; and the U.S. adopts a decentralized legislative model, whereby multiple

departments formulate relevant laws, regulations and regulatory measures according to the characteristics of different industries and fields. This paper proposes solutions to prevent personal information leakage by analyzing the legislative and regulatory approaches of different countries, so as to promote the process of personal information protection.

2. LITERATURE REVIEW

2.1 Domestic Research Status

At present, the research on personal information leakage in China mainly lies in the research on the causes of personal information leakage and the current status of legislation on the protection of personal information.

Regarding the causes of leakage Wang Yongming in "Analysis of Personal Information Leakage Preventive Measures in the Big Data Environment" argues that the main causes of personal information leakage in China are mobile devices, biometrics, and internal reasons of enterprises. Scholars Cheng Pu and Eddie Yang, "Study on the Reasons for the Formation of Personal Information Security and Countermeasures in the Era of Big Data", believe that the reasons for the leakage of personal information are also the hidden nuclear bundled information theft of software and the immaturity of data supervision technology. Scholar Lian Yeying pointed out in "Study on the Protection of Personal Information in the Era of Big Data" that although China has introduced relevant laws and regulations on the protection of personal information, such as "Personal Information Security Law" and "Network Security Law", the promulgation of these laws is still in the primary stage, and it is not possible to comprehensively and systematically regulate and protect personal information, which is an obvious gap compared with other developed countries and regions; at the same time, the technology of information protection is not perfect, and cyber attacks and leaks occur frequently. At the same time, information protection technology is not perfect, and cyber attacks and leaks occur frequently. Scholar Li Wei pointed out in "Study on the Protection of

Personal Information in the Era of Big Data" that there is still the problem of low application of technical means for privacy protection, high cost, and illegal theft by criminals; scholars Feng Zhanying, Chen Rui, Zhang Yu, Wang Yu, Zheng Fei, Zhang Jianping, and Li Lu pointed out in "Analysis of the Current Situation of the Leakage Problem of Citizen's Personal Information and the Countermeasures" that the leakage of personal information is due to the lack of awareness of confidentiality, which makes governmental agencies and public service departments The leakage of personal information is due to the fact that government agencies and public service departments unintentionally disclose citizens' personal information due to a lack of awareness of confidentiality, commercial organizations illegally sell personal information due to a tendency to make profit, and overseas organizations obtain personal information by any means.

To summarize, the causes of information leakage in China's academic circles are: hacker attacks, lax supervision of information within enterprises and governments, defects in the development of application programs, citizens' lack of awareness of personal precautions, information writing for profit, and incomplete legal norms. As for these problems, the academic community has come up with a variety of solutions: from the national side: refining the legal provisions, determining the responsibility of each party and the corresponding penalties, and strengthening legal aid; from the government side: establishing an administratively-led and judicially-assisted system of recourse; from the enterprise side: encouraging self-discipline of enterprises, optimizing the internal compliance system of the enterprise, strengthening the private remedies, and perfecting the remedies after the event.

China's legislative research on personal information protection started relatively late, but the real demand for personal information protection is very strong, and before the implementation of the Personal Information Protection Law and other laws, there were many tragic cases of personal information leakage in China, such as the "Xu Yuyu case" in 2016. Before that, there were many tragic cases of personal information leakage in China, such as the Xu Yuyu case in 2016. For personal information, China's corresponding legal provisions

were put forward in the Decision on Strengthening the Protection of Network Information in 2012, which is also the earliest proposed law on the protection of personal information. For the right to privacy, the 2010 Tort Liability Law was the first legal provision in China to explicitly mention the right to privacy and provide for it.

In On the Status of the Right to Personal Information in the Law of Personality Rights, Wang Liming points out, “The right to personal information does not belong to general personality rights. There is some overlap between personal information and personal privacy in terms of content, but overall the concept of personal information goes far beyond the scope of private information, and the right to personal information should be stipulated separately rather than attached to the right to privacy.” Personal information is presented as a right of citizens, i.e., the right to personal information is protected separately from the right to privacy as the case may be; however, it was not until the promulgation of China's Civil Code in 2021 that the second paragraph of Article 1,034 stipulated, “For private information contained in personal information, the provisions on the right to privacy shall apply; if there are no such provisions, those on the protection of personal information shall apply. ”

Scholar Yang Changquan has combed through China's legal provisions on the legislative regulation of personal information, for example: Article 253 of the Criminal Law provides for the conviction and punishment of the crimes of selling or illegally providing citizens' personal information and illegally obtaining citizens' personal information. Article 285 of the Criminal Law provides for the crimes of illegal intrusion into computer information systems, illegal acquisition of data from computer information systems, and illegal acquisition of personal information from non-citizens. Article 37 of the Network Security Law of the People's Republic of China provides for the rules on the storage of personal information, Article 40 provides for the system of protection for the collection of personal information, Article 41 provides for the principles to be followed in the collection and use of personal information and the rules on the consent of those who have been collected, and Article 42 provides for the rules on the guarantee of information security for network operators. Article 42 stipulates the obligation of network operators to guarantee the security of information, Article 43 grants

right holders the right to delete and the right to rectify, Article 44 regulates the unlawful acquisition, unlawful sale and unlawful provision of personal information, and Article 76(5) specifies the scope of personal information. Conviction and Sentencing of Crimes of Controlling Computer Information Systems by Law. Scholar Lin Xiumei pointed out the existing problems in the Study on Civil Law Protection of Personal Information in the Context of Big Data Era: "The system of civil law protection of personal information is flawed and needs to be further improved; the principle of attribution of responsibility is imperfect; the criteria for determining excessive collection of personal information are unclear, and the determination of 'excessive' depends largely on the judge's discretionary power. The judgment of "excessive" is largely dependent on the judge's discretion, which may easily result in different judgments for the same case, and is not conducive to the full protection of the legitimate rights and interests of personal information rights holders", but at the same time, it also puts forward the improvement methods, 'clarifying the principle of attribution of responsibility for civil tort liability for disputes over personal information, and formulating different attribution principles for personal information of different importance; clarifying the principle of 'excessive" for personal information. The scope of "excessive" to set up a bottom-up clause to increase the latitude of the legislation; improve the corresponding civil remedy mechanism for personal information disputes, and formulate a unified and clear standard for the calculation of damages to fully protect the legitimate rights and interests of the parties concerned."

2.2 Current Status of Foreign Research

At present, there are three main models on personal information protection in foreign countries.

U. S. model: based on the right to privacy, personal information is protected through decentralized legislation and a large number of judicial cases, such as the Privacy Act ("Privacy Act"), the Electronic Communications Privacy Act and so on. Meanwhile, the U.S. attaches great importance to industry self-regulation, such as the privacy protection guidelines published by the American Online Privacy Alliance and the Internet Privacy Certification

Program, which require websites to comply with the rules of data collection practices and accept supervision.

EU model: adopting a harmonized legislative model, such as the Personal Data Protection Directive adopted in 1995 and the General Data Protection Regulation, which came into effect in May 2018 (GDPR for short). The regulation stipulates a number of rights for data owners, such as the right to be informed, the right to be forgotten, the right to data portability, etc. It also clarifies the obligations and responsibilities of data controllers and processors, and imposes severe penalties on non-compliant enterprises, with fines up to 20 million euros or 4% of the enterprise's global annual turnover.

Japan Model: Based on the model of Europe and the United States, the Act on the Protection of Personal Information of 2005 realizes all-round protection, and at the same time focuses on industry self-regulation and the participation of associations, with enterprises formulating internal rules on the protection of personal information, and industry associations issuing relevant guidelines, forming a unique protection model combining government legislation and industry self-regulation. At the same time, it emphasizes industry self-regulation and community participation, with companies formulating internal personal information protection rules and industry associations issuing relevant guidelines.

Legislation on the protection of personal information is also diverse, with the more influential ones being the EU's General Data Protection Regulation (GDPR), which came into force in 2018, the U.S. Privacy Act, Canada's The Personal Information Protection and Electronic Documents Act in Canada, and the Act on the Protection of Personal Information in Japan. All of these Acts regulate, to a certain extent, some of the criminal problems caused by the leakage of personal information.

3. CONTENT AND METHODOLOGY OF THE STUDY

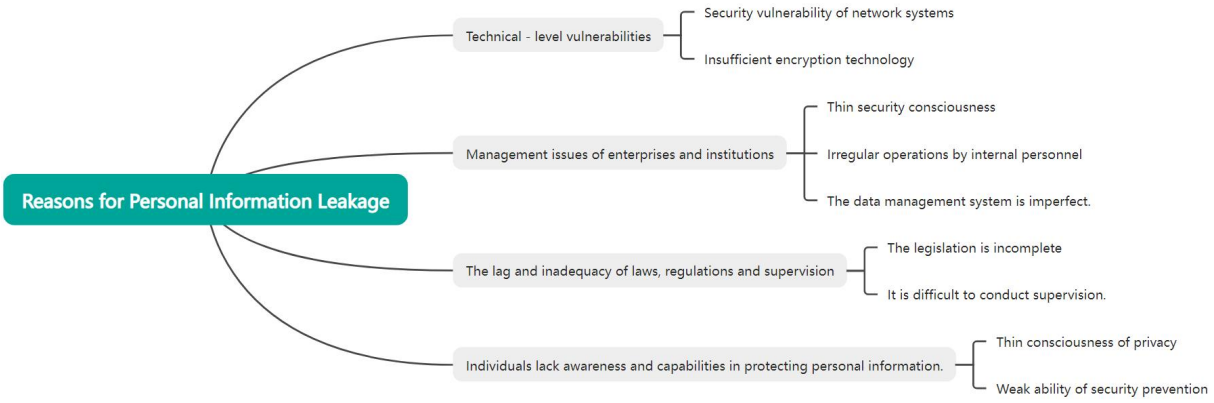
3.1 Research Content

3.1.1 Types of Personal Information and Causes of Personal Information Leakage

Personal information refers to personal data related to an individual that can be recognized

directly or indirectly. It can be categorized into the following categories: direct personal information and indirect personal information, sensitive personal information and general personal information, public personal information and non-public personal information.

According to the literature review, it can be sorted out that the reasons about the leakage of personal information can be organized into four aspects:

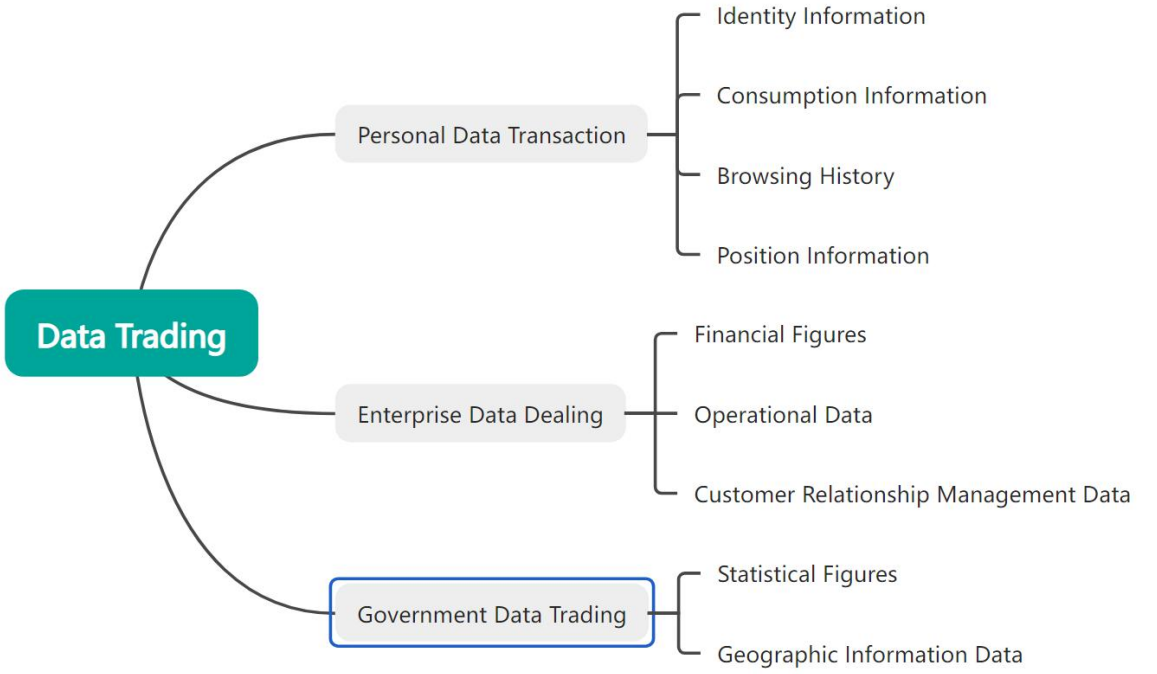


3.1.2 The ways of personal information leakage

The ways of personal information leakage are diversified and complicated. At the network level, hacker attacks utilize all kinds of loopholes to invade databases, malware quietly collects and transmits information, and phishing lures users to actively provide by fraudulent means. Low security awareness of employees within the enterprise, internal staff operating in violation of business secrets leaked, whether unintentional errors or intentional profit-making, the system security loopholes in the neglect and improper handling of personal information will be exposed to risk. At the level of data trading and sharing, unregulated third-party cooperation and chaotic data trading market conditions are likely to cause information in the flow process out of control. Furthermore, the widespread use of mobile devices and Internet of Things (IoT) devices poses new challenges. Excessive collection by mobile apps, unauthorized sharing, and security weaknesses in IoT devices can lead to leakage of personal information when it is used and transmitted for storage. These pathways are intertwined and together constitute a complex network of personal information leakage, seriously threatening the security of personal privacy and the stability of the social information security system.

3.1.3 Data transactions

There are many types of data transactions, as shown in Fig:



And the scope of this paper focuses on the parts of the above types of transactions related to personal information.

3.2 Research Method

Literature analysis method: through the analysis of the existing literature on the legal regulation of personal information leakage, on the premise of understanding the literature, focusing on the literature on the personal information leakage of the existence of all kinds of problems and their corresponding solutions, and these contents are systematically organized and categorized. Through this sorting work, we draw valuable ideas from them to better serve the research of this paper. These extracts from the literature will undoubtedly play an important role in providing constructive guidance for this paper.

Comparative Analysis: The comparative analysis of the domestic and foreign situations in terms of personal information leakage pathways, regulatory methods and the resulting governance consequences will enable us to more intuitively feel the effectiveness of different governance contexts, and then identify the existing problems and propose effective solutions.

4. RESULT

4.1 Presentation of the Problem

Time	Area	Case
2020	USA	In January 2020, an unprotected set of databases at U.S. cosmetics giant Estee Lauder accidentally exposed 440 million internal records to the Internet, where the exposed information included email addresses, internal documents, IP addresses, and information about the company's internal education platform.
		In January 2020, Microsoft said it suffered a data breach of the servers it uses to store customer support analytics.The incident, which occurred in December 2019, involved 250 million records, including email addresses, IP addresses, and detailed descriptions of customer support cases, all of which were accidentally made public without password protection.
	China	In March 2020, it was revealed that the personal information of more than 538 million users of Sina Weibo had been put up for sale on the dark web and other online sites, with the leaked information including the nicknames, genders, places of residence and phone numbers of 172 million users.
2022	Brazil	Brazil experienced the largest breach of personal data in its history, with a database containing names, unique tax identifiers, facial images, addresses, phone numbers, emails, credit scores, salaries and other information for 223 million people. This incident reflects the fact that Brazil's legal framework for the protection of personal information may not be sufficiently robust and lacks comprehensive and strict regulatory mechanisms for the collection, storage and use of personal information on such a large scale, which puts citizens' personal information at high risk.
2023	USA	Neiman Marcus, a high-end department store in the United States, suffered a data breach that affected the information of about 5 million customers, including credit card numbers, names, addresses and so on. This demonstrates that in the commercial sector, despite the existence of personal information protection laws, there is a lack of clarity in defining the responsibilities of enterprises in handling customer data in cooperation with third parties, which makes it easy for security loopholes to occur in the data-sharing process, leading to information leakage.
	China	On August 17, 2023, the Nanchang Public Security Network Security Department discovered that more than 30,000 pieces of personal information of students and faculty members of a university in Nanchang had been sold publicly on the Internet outside of China. The university in question had not established a full-process data security management system and had not taken technical measures to safeguard data security, which led to the illegal invasion of the university's database, which stored more than 30 million pieces of information on faculty, staff, students, and tuition payments, by hackers.
2024	Chinese Tai Wan	In October 2024, the Office of Political Affairs of the Taiwan Defense Department made a major oversight in handling the property declarations of its personnel by transmitting the roster of all personnel within the department who were required to declare their property and their personal declarations via e-mail to the declarant and to the units of each military service, which resulted in the leakage of personal information of all general officers above the rank of colonel, the “Chief

	of Staff" and the head of the Taiwan Defense Department, Gu Lixiong. As a result, all general officers above the rank of colonel, the "Chief of Staff" and the head of Taiwan's defense department, Gu Lixiong, had all their personal information leaked out, including the personal information and real names of all intelligence officers. After the incident, the Taiwan Defense Department urgently recovered the data and carried out damage control.
USA	In 2024, a data breach of Transerve, an electronic travel pass system managed by the U.S. Department of Transportation (DOT), exposed the personal information of approximately 237,000 current / former federal government employees. The system was used to process transportation allowances for government employees, reimburse some commuting expenses, etc. The GAO issued a report stating that the DOT had failed to follow through on its cybersecurity responsibilities and lacked oversight of privacy issues.

4.1.1 Incomplete Regulatory Regimes for Personal Information Leakage in Various Countries

The regulatory system of personal information leakage in each country has its own characteristics, but all of them are incomplete.

China adopts a coordinated regulatory system based on laws and supported by the net information department, but there are inconsistencies in the coordination of various departments, and the results of implementation vary greatly in different regions; the U.S. adopts a combination of industry self-regulation and decentralized legislation, with limitations in industry self-regulation, fragmented laws prone to conflict, and imbalance in the intensity of regulation; the European Union is dominated by uniform and strict regulations, but it faces differences in implementation, high costs for enterprises, and cross-border regulatory problems; the U.K., although it has a comprehensive legal system, has problems in enforcement. Although the United Kingdom has a comprehensive legal system, there is insufficient enforcement of regulations and challenges in keeping up with technological updates; Canada adopts a "middle way" model, but there may be a lag in updating the laws; Japan has enacted a series of laws and set up a supervisory body, but there is a lag in updating the laws, differences in enforcement by enterprises, and limited regulation of leakage caused by negligence on the part of some members of the public.

4.1.2 Incomplete legislation on personal information protection in various countries

Personal information protection laws in various countries have played a positive role in the protection of personal information to a certain extent, but there are still many

incompletenesses, and these incompletenesses have been highlighted in various types of data leakage incidents, reflecting the challenges faced by various countries in different aspects and levels of personal information protection.

Time	Area	Law	Content
2016	China	Cybersecurity Law of the People's Republic of China	The Law stipulates the basic principles and requirements for the collection and use of personal information by network operators, clarifies that network operators shall keep the user information they collect strictly confidential, and establishes a sound system for the protection of user information, etc., providing a fundamental legal framework for the protection of personal information.
2021	China	Personal Information Security Protection Act	This law is China's first systematic and comprehensive law dedicated to the protection of personal information, which comprehensively regulates the handling of personal information, clearly prohibits the excessive collection of personal information and the killing of acquaintances by big data, regulates the handling of sensitive personal information such as face information, and improves the mechanism for complaints and reports on personal information protection, etc., which fully responds to the concerns of the society and provides strong legal protection for cracking the hot and difficult issues in the protection of personal information. It has fully responded to the concerns of the society and provided a strong legal guarantee for solving the hot and difficult problems in personal information protection.
1974	USA	Privacy Act	It regulates the handling of personal information of U.S. citizens and aliens with permanent residency by federal government agencies, specifies the rights of the subject of the information and the obligations of the government agencies, and provides for appropriate civil remedies.
2016	EU	General Data Protection Regulation	Clarifies the definition of personal data and the principles of protection, sets out a number of rights for data subjects, obligations for data controllers and processors, regulates the conditions for cross-border data transfers and the requirements for international cooperation, and establishes a mechanism of penalties for non-compliance in order to safeguard the privacy and security of the personal data of EU citizens.

2003	Japan	Act on the Protection of Personal Information	Provides for the definition of personal information, the rights of data subjects, the obligations of data controllers and processors, as well as the rules, supervisory bodies and penalties for the handling of personal information in order to safeguard the security and privacy of personal information.

The personal information protection laws of some of the above countries regulate the collection, storage, use and transmission of personal information from different perspectives, specifying the rights enjoyed by the subject of the information, such as the right to know, the right to consent, the right to delete, etc., and at the same time stipulating the corresponding obligations of the information processors, such as safeguarding information security and following the principle of lawful and proper handling. These provisions make personal information in the process of handling a clearer legal guidelines to follow, to a certain extent, to curb some of the arbitrary violation of personal information unlawful behavior, and enhance the confidence of citizens in the protection of personal information. However, we must also realize that although these laws have achieved some success, there are still some areas that need to be improved in the actual implementation process.

Scope of Legislation: With the rapid development of science and technology, various new types of personal information continue to emerge, such as genetic data, and the existing legal framework often fails to timely incorporate these special information into a comprehensive and precise scope of protection, resulting in the existence of insufficient legal basis when dealing with this type of information, which puts the citizen's personal information of these new types of personal information at a potential risk of leakage.

With regard to cross-border data transfers: there is a clear lack of harmonization between national laws. In today's increasingly deep globalization, the cross-border flow of data is more and more frequent, and international organizations have introduced some rule systems among themselves, such as the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Cross-Border Privacy Rules System (“CBPR System\), etc., while for individual countries, some requirements are stringent and some are relatively lax in

this aspect of data transfer. This makes it easy for regulatory gaps or conflicting areas to arise when multinational enterprises are involved in handling personal information and when personal information is transferred between different countries, giving lawbreakers an opportunity to take advantage of the situation, and thus threatening the security of citizens' personal information in the cross-border process.

Definition of the responsibility of information processors: although the law stipulates the basic obligations that they should undertake, it still seems to be insufficiently detailed in some complex practical scenarios, that is, the problem of data rightization. Regarding the determination of the principle of attribution of responsibility, it should be applied differently between personal information processors and non-personal information processors. For example, when a large-scale data leakage incident occurs due to a hacker attack, the existing legal provisions often lack clear and operable details as to what specific measures should be taken by the information processor within how long to remedy the situation, and how to accurately assess and compensate for the losses caused to the subject of information due to the data leakage, which to a certain extent affects the timely and effective maintenance of the rights and interests of the subject of information.

To sum up, although the personal information protection laws of various countries have taken important steps forward, in order to realize all-round and dead-end protection of personal information, it is still necessary to continuously adjust and improve them according to the development of the times and the actual situation, so as to better adapt to the increasingly complex information society environment and effectively safeguard the rights and interests of citizens' personal information.

4.2 Research Results

The purpose of this paper is to explore what are the ways of legal regulation of personal information leakage in the context of data transactions, through the literature analysis method, comparative survey method to collect and analyze the required content in order to inspire the author's thoughts, the following is the feasibility of the ways of legal regulation suggestions:

Regulatory system: clarify the authority of each department, establish a coordinating

mechanism, optimize the regulatory system; supervise the implementation of legal provisions, improve the illegal disposal provisions;

Judicial aspects: establish a specialized judicial institution or department, the docking of judicial and administrative law, and improve judicial publicity and education on the protection of personal information.

4.3 Recommendations

4.3.1 In terms of justice

Establish a unified and independent regulatory body. Professional personal information protection courts can be set up, or specialized teams can be formed within the relevant trial courts to focus on various cases involving personal information leakage. The personnel of these professional organizations or departments should have profound legal literacy and understanding of the information technology field, so that they can interpret the cases more accurately facts of the case, accurately apply the law, improve the efficiency and fairness of the trial, and provide stronger judicial protection for the victims.

To focus on the docking of justice and administrative law enforcement. Build a smooth communication bridge between the judiciary and administrative law enforcement, establish an information sharing platform, and realize real-time interoperability of key information such as case clues, investigation and evidence collection results, and penalty decisions. When dealing with cases of personal information leakage, all departments should work together.1290 Administrative law enforcement departments carry out preliminary investigation and evidence collection with their professional technical means and regulatory resources, and transfer the results to the judicial authorities in a timely manner; the judicial authorities conduct in-depth examination based on the law, and hold the infringers legally liable, so as to form a strong synergy in combating such illegal behavior.

Improve judicial publicity and education on the protection of personal information. Through a variety of channels, such as online legal lectures, offline community legal activities, and special media reports, the relevant laws and regulations on the protection of personal information have been widely publicized, typical cases have been interpreted, and the public's

awareness of the law and rights has been raised, so that everyone can better guard the security of their own personal information.

4.3.2 Regulatory framework

It is crucial to clarify the competence of each department and establish a coordinating mechanism. Different departments should have clear and explicit responsibilities in the field of personal information protection supervision, for example, the Internet information department is responsible for coordinating planning and formulating macroscopic policies, while the competent authorities of financial and telecommunication industries carry out specific supervision of personal information processing activities within their own industries. Through the establishment of an effective coordination mechanism, communication and collaboration between departments can be promoted, avoiding regulatory gaps or overlaps caused by unclear responsibilities and forming regulatory synergy.

Supervise the implementation of legal provisions. Supervisory authorities need to adopt various methods, such as regular inspections and irregular spot checks, to ensure that all kinds of information processing entities carry out their activities in strict accordance with the relevant legal provisions on personal information protection, so as to make the law really take effect.

Improvement of illegal disposal provisions. For the violation of personal information protection laws and regulations, the penalty standards should be further refined, according to the severity of the illegal circumstances, clear corresponding administrative penalties, such as the reasonable setting of the amount of fines, ordered to suspend and rectify, etc., constituting a crime should also be investigated according to law for criminal responsibility, so as to improve the cost of violation of the law, strongly curbing the occurrence of personal information leakage and other illegal behaviors.

5. SUMMARY

This paper sets as the core research purpose to explore in depth the legal regulation of personal information leakage in the context of data transactions. In the process of research, a

comprehensive approach integrating literature analysis and comparative method is adopted. Through careful reading and combing of a large amount of relevant literature, as well as in-depth comparative analysis of the practical experience and legal systems of different countries and regions in the protection of personal information, it is finally concluded that a more comprehensive and systematic regulatory framework of personal information leakage can be constructed from the legislative level, the regulatory level and the judicial level.

At the legislative level, it is possible to fill the gaps in existing legislation by improving the content of relevant laws and regulations, clarifying the scope of personal information, the attribution of rights, and infringement liability, so that the protection of personal information has a more solid basis in law. At the regulatory level, it is necessary to build an efficient and coordinated regulatory system, clarify the responsibilities and authorities of each regulatory body, and strengthen the dynamic supervision of each link of data collection, storage, use and transaction, so as to timely detect and stop the risk of leakage of personal information and violation of the law. At the judicial level, specialized judicial relief mechanisms should be established and improved to ensure that when personal information is infringed upon, the right holder can obtain timely and effective judicial assistance, including compensation for damages, and stopping infringement of rights. These research results not only promote the theoretical study of personal information protection, help enrich and improve the relevant academic theory system, but also have great value and significance in practice. They can provide practical operational guidelines for government departments, enterprises and social organizations to formulate personal information protection policies, regulate data processing behaviors and resolve personal information disputes.

In the future, the results of this paper will be used as the cornerstone of the subsequent research to further expand in the direction of refinement and vertical deepening. In the future, we will use the results of this paper as an important cornerstone to further expand in the direction of refinement and vertical deepening, and further optimize the multiple governance model of personal information protection, in order to promote the process of personal information protection to a new level worldwide, and make unremitting efforts to build a

global digital ecosystem that respects and protects the security of personal information.

REFERENCES

"Anmeldung erforderlich." juris.de. Accessed. https://www.juris.de/jportal/portal/page/jurisw.psml.

"Cross Border Privacy Rules System." APEC Cross - Border Privacy Rules System. Accessed . https://cbprs.org/.

"Electronic Communications Privacy Act of 1986 (ECPA)." Bureau of Justice Assistance. Accessed. https://www.bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

"EU Data Protection Directive." Electronic Privacy Information Center. Accessed. https://epic.org/eu-data-protection-directive/.

"General Data Protection Regulation." gdpr - info.eu. Accessed. https://gdpr-info.eu.

"Law Search." e - laws.e - gov.go.jp. Accessed. https://elaws.e - gov.go.jp/document?lawid=343AC0000000057.

"Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)." laws - lois.justice.gc.ca. Accessed. https://laws - lois.justice.gc.ca/eng/acts/P - 8.6/page - 1.html.

"Privacy Act of 1974." US Department of Justice. Accessed. https://www.justice.gov/opcl/privacy-act-1974.

Cheng, Pu, and Yang Yun. "Research on the Causes and Countermeasures of Personal Information Security in the Big Data Era." *Modern Business Trade Industry*, 2020, no. 17, pp. 146 - 147. DOI: 10.19311/j.cnki.1672 - 3198.2020.17.076.

Dai, Wenkui, and Li Xuecheng. "Research on the Ways and Prevention of Personal Privacy Leakage." *Computer Knowledge and Technology*, vol. 17, no. 25, 2021, pp. 57 - 59.

Deng, Hui. "The Legislative Choice of Administrative Supervision over Personal Information Protection in China." *Journal of Shanghai Jiao Tong University Law Review*, 2020, no. 2, pp. 140 - 152.

Feng, Zhanying, Chen Rui, Zhang Yu, et al. "Analysis of the Current Situation and

Countermeasures of Citizen Personal Information Leakage." *Chinese Journal of Medical Library and Information Science*, vol. 31, no. 6, 2022, pp. 9 - 19. DOI: 10.3969/j.issn.1671 - 3982.2022.06.002.

Feng, Zhanying, Zhang Yu, Duan Meizhen, et al. "Research on the Path of Personal Information Leakage and Its Protection Strategy in the Big Data Environment." *Chinese Journal of Medical Library and Information Science*, vol. 29, no. 9, 2020, pp. 7 - 12.

Feng, Zhanying, Zhang Yu, Duan Meizhen, et al. "Research on the Path of Personal Information Leakage and Its Protection Strategy in the Big Data Environment." *Chinese Journal of Medical Library and Information Science*, vol. 29, no. 9, 2020, pp. 7 - 12.

Han, Kewang. "Research on the Dilemma and Optimization Path of Personal Information Protection in Network Platforms." *Women's Daily*, 2024, no. 10, pp. 181 - 183.

Ji, Rongyao, Jiang Zeng, and Wang Chuqiao. "Personal Information Leakage and Protection in the Context of 'Internet +'." *Cooperative Economy & Science*, 2020, no. 9, pp. 184 - 185. DOI: 10.3969/j.issn.1672 - 190X.2020.09.077.

Li, Changchang. "The Dilemma and Countermeasure Path of APP Personal Information Protection Policy." *Journal of Information Security Research*, vol. 10, no. 2, 2024, pp. 177 - 183. DOI: 10.12379/j.issn.2096 - 1057.2024.02.12.

Li, Danni. "Research on the Protection of Citizen Personal Information Based on Judicial Big Data." *Market Weekly*, vol. 36, no. 6, 2023, pp. 164 - 167.

Li, Peijiao. "Research on the Legal Issues of Personal Information Protection." *Zhengzhou University*, 2022.

Li, Wei. "Research on the Protection of Personal Information in the Big Data Era." *New Economy*, no. 1, 2023, pp. 24 - 34. DOI: 10.3969/j.issn.1009 - 8461.2023.01.004.

Lian, Yeying. "Research on the Protection of Personal Information in the Big Data Era." *Xiamen Science & Technology*, vol. 31, no. 2, 2024, pp. 47 - 49.

Sun, Peng, and Yang Zaihui. "The Determination of Fault in Personal Information Infringement and Its Impact on Tort Liability." *Journal of Central South University (Social Science Edition)*, vol. 30, no. 1, 2024, pp. 76 - 86.

Wang, Liming. "On the Status of the Right to Personal Information in the Law of Personality Rights." *Journal of Soochow University (Philosophy and Social Science Edition)*, vol. 33, no. 6, 2012, pp. 68 - 75.

Wang, Yongming. "Analysis of Preventive Measures for Personal Information Leakage in the Big Data Environment." *Cyberspace Security*, vol. 14, no. 1, 2023, pp. 76 - 80. DOI: 10.3969/j.issn.1674 - 9456.2023.01.013.

Wang, Yuwei. "Research on the Protection of Personal Information in the Internet Context." *Telecom World*, vol. 31, no. 3, 2024, pp. 45 - 47. DOI: 10.3969/j.issn.1006 - 4222.2024.03.015.

Yang, Changquan. "On the Legislative Improvement of the Protection and Processing of Personal Information in the Big Data Era." *Journal of Kaili University*, vol. 40, no. 5, 2022, pp. 44 - 49. DOI: 10.3969/j.issn.1673 - 9329.2022.05.008.

Li, Xiaojia. "Research on the Legal Issues of Cross - Border Data Transmission Provisions in RCEP." *Shandong University*, 2022.