ISSN: 2710-0170

The local construction of the right to be forgotten

Shuwen Zheng

Law School, Beijing Normal University, Beijing, China

Abstract

With the emergence of Internet technology and big data technology, the remembering and forgetting of personal information have gradually become unbalanced, and the permanent memory ability of big data has brought more and more important impacts on people's lives. While the browsing history and shopping history of websites bring convenience to people, there is also the fear of being monitored and recorded at all times. It is an inevitable trend for people to seek ways to control their own data information to deal with the drawbacks brought about by the development of big data technology. Therefore, many countries have introduced the right to be forgotten to remedy this situation and protect the right of individuals to control their data information. Comparing the series of legislation in China with the extra-territorial right to be forgotten, identifying the right to erasure and the right to be forgotten in China as different expressions of the same right, analyzing the right to be forgotten from the perspective of the structural system of rights, clarifying the subject, object and content of the right to be forgotten, and proposing ways to further optimize the right to be forgotten in China in terms of both substantive and procedural law.

Keywords

Personal information protection, right to be forgotten, localization.

1. Creation of the right to be forgotten

The right to be forgotten is derived from the French "Le droit à l'oubli" in 1974. It is usually used for criminals to request the deletion of their criminal records in the public domain after serving their sentences in order to obtain equal opportunities for development in social life, so as to facilitate their re-socialization.[1] However, in the context of the rapidly changing era of the emerging industry of information network technology services, the laws of countries around the world have a tendency to focus on and strengthen the protection of citizens' personal information, and the system of the right to be forgotten is more widely used in the field of the Internet industry. Western countries represented by Europe and the United States were the first to set off the wave of Internet technology. As a result, these countries and regions took the lead in exploring the institutional setting and practice of the right to be forgotten.

1.1. The practice of the right to be forgotten in the European Union

At the end of 1995, the European Union passed the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter referred to as the Personal Data Protection Directive). This directive stipulates that when personal data is no longer needed, the data subjects can apply to modify or delete personal data in order to protect personal digital information. Although the Personal Data Protection Directive does not directly stipulate the right to be forgotten, this directive is considered to be the prototype of the right to be forgotten. The directive also has a significant impact on the subsequent legislation in the field of information protection in the EU.

In the 2014 Google-González case, the "right to be forgotten" was established as a civil right of the information subjects in the form of a precedent.The case occurred in 2009 when González,

ISSN: 2710-0170

a Spaniard, was searching for his first name and last name using the Google search engine and the first search result on the page was an auction notice published in the Spanish daily newspaper La Vanguardia in 1998, which referred to an auction of a property that belonged to González and mentioned his social security debt arrears. By this time, however, his social security debt had been settled years earlier.

After negotiations with La Vanguardia and Google Spain did not achieve the desired results, González filed a complaint with the Spanish Data Protection Agency (AEPD), requesting La Vanguardia to remove or change the newspaper content involving his personal information so that his personal information could not be accessed through the search engine, and requesting Google Spain or Google's headquarters to remove the link involving his personal information in the search engine to prevent the information from being viewed through the link.

The AEPD held that La Vanguardia's disclosure was made in accordance with the order of the Ministry of Labor and Social Affairs. It ruled to dismiss González's claim against La Vanguardia, but supported his lawsuit against Google Spain and Google's headquarters, ordering the defendants to remove the links to the relevant information in the search results.

Google Spain and Google headquarters appealed the case in the Spanish National High Court, which then referred the case to the European Court of Justice. The European Court of Justice ruled that Google's processing of personal data complied with Article 2(d) of the Personal Data Protection Directive, and that it should be deemed a "data processing controller" as provided for in this paragraph, and that its actions violated the obligation of a data processing controller to remove or block non-compliant data as provided for in Articles 12(b) and 14(a) of the Personal Data Protection Directive. It ultimately ruled that Google Spain and Google's headquarters should remove the link to the relevant information as requested by González.

This case established the "right to be forgotten" as a civil right of information subjects in the form of a precedent, which is of milestone significance for promoting legislation on the right to be forgotten.

In 2018, the EU officially enacted the General Data Protection Regulation, which codified the "right to erasure (right to be forgotten)" in Article 17. It detailed six conditions under which the right applies and five exceptions. A series of regulations promulgated by the EU have gradually established a relatively advanced right to be forgotten system in the region. The right to be forgotten systems in other regions have also borrowed from the EU. The EU's concept of legislation on the right to be forgotten has had a profound impact on a global scale.

1.2. The practice of the right to be forgotten in the United States

Compared with Europe's legislative philosophy, the United States places greater emphasis on protecting citizens' freedom of speech rather than their personal information.

The right to be forgotten, which allows individuals to demand that search engine operators delete "harmful, irrelevant, or excessive" personal links from search results through legal means, is seen as conflicting with the first provision of the First Amendment to the U.S. Constitution that "Congress shall make no law abridging the freedom of speech, or of the press".[2] As a result, the U.S. has taken a cautious approach to the right to be forgotten, focusing primarily on the personal information of minors. However, since the EU officially legislated the right to be forgotten, the U.S. has also made efforts to explore its application.

One such effort is the "Eraser Law," enacted in California in 2013, formally known as the Business and Professions Code. This law represents a compromise between protecting personal information and upholding freedom of speech. The Eraser Law is particularly focused on safeguarding minors by granting them the right to delete their personal information from social networking platforms.

ISSN: 2710-0170

The code protects minors' right to be forgotten by stipulating the obligations of network service providers. [3]The obligations stipulated can be divided into four aspects. The first is to allow minors to delete data content that is actively disclosed on the Internet. The second is to clearly inform minors that they have the right to delete or request network operators to delete the information they actively publish on the Internet. The third is to let minors know the way to delete or request deletion. The fourth is to promptly inform the minors who apply for deletion when it is impossible to delete.

However, for the purpose of protecting the freedom of speech of others, the rights of the code are limited to the content or information posted on the Internet by the underage network users who implement the deletion behavior or apply for deletion. It explicitly prohibits minors from requesting the deletion of data information posted by others. Although the "Eraser Law" is still very limited in terms of geographical scope and applicable subjects, and its objects are limited to personal information voluntarily posted on social platforms by underage users in California, the effective area is California, where many technology companies are concentrated. Therefore, it is still a major attempt by the U.S. government to legislate in the field of the right to be forgotten. It also protects the personal privacy of minors in a targeted manner, and at the same time has considerable reference significance for the legislation of other states in the United States.

2. The Construction of the Right to be Forgotten in China

2.1. The Necessity of Establishing the Right to be Forgotten System in China

The 55th "Statistical Report on the Development of Internet in China" released by the China Internet Network Research Center in January 2025 shows that as of December 2024, China's Internet penetration rate is as high as 78.6%, and the number of Internet users has reached 1.108 billion. Although the vigorous development of Internet technology has facilitated people's lives, when people's personal information such as geographic location, mobile phone number and even ID number is requested by various websites and apps for various reasons, Internet users will be in a panic that the massive amount of personal information stored in the virtual space may be leaked or sold at any time. Therefore, the right to be forgotten system should be established in China based on the following purposes.

Firstly, national information sovereignty should be protected at the national level. When the data of individuals reaches a certain amount, it will form a collection of data in the unit of the country, and once leaked, it will have a very bad negative impact on the national information security. Moreover, in the era of big data, information has also become a valuable resource, which is fought over by Internet companies in various countries. If the security of information cannot be guaranteed, China will be at a disadvantage in the competition, and national information sovereignty, as an important part of national sovereignty, will also face great threats.

Secondly, from the perspective of protecting individual citizens, the construction of the right to be forgotten is not only a protection of the right to self-determination of personal information, but also a protection of personality. Personal information stored on the Internet has the possibility of being leaked or used illegally, and illegal acts such as "cyber violence" and "doxxing" occur more frequently. Allowing the information subject to independently decide which information can be retained by the website can reduce the occurrence of such illegal acts from the source. In addition, when the amount of personal information stored on the Internet reaches a certain amount, through analysis and reorganization, a person's digital personality can be formed, but the process of analysis and reorganization is determined by the personal information processor, so the formed digital personality cannot fully and truly reflect the original personality image of the information subject.[4]

ISSN: 2710-0170

Therefore, in order to achieve the purpose of protecting national network security and safeguarding personal dignity and the right to self-determination of information, it is necessary to construct a system of the right to be forgotten in China.

2.2. Judicial Practice of the Right to be Forgotten System in China

The 2015 case Ren Jiayu v. Beijing Baidu Netcom Science and Technology Co., Ltd. marked the first instance where the right to be forgotten was addressed in Chinese judicial practice. In this case, the plaintiff, Ren, requested that Baidu cease infringing upon his rights, including his right to reputation and right to name. Of particular interest to legal scholars was the plaintiff's third claim—that of the "right to be forgotten" as part of general personality rights.

Ren demanded that Baidu not link search results for his name with entries like "Tao Education Ren," citing the poor reputation of "Tao Education" and its potential negative impact on his personal image. He also sought economic compensation. All of Ren's claims were dismissed by the trial court, and the appellate court upheld the decision. While the disputes over reputation and name rights are not elaborated upon here, the court's handling of the right to be forgotten was significant.

The court acknowledged that Chinese law does not explicitly recognize the right to be forgotten as a legal right or concept and that it originated in European jurisprudence. However, rather than dismissing Ren's claim solely on this basis, the court examined whether the right to be forgotten could fall under the umbrella of general personality interests.

The court concluded that Ren's claim implied two intentions: to assert that Tao Education had a negative reputation, and to conceal his work experience with the company. However, business reputation is itself a legal interest protected by law, and courts cannot evaluate it positively or negatively. Furthermore, Ren's work history was relevant information for potential business partners and thus could not be arbitrarily deleted. Since Ren entered into his employment with full legal capacity, he was not part of a legally vulnerable group requiring special protection. Consequently, the court rejected his claim based on the general personality right to be forgotten.

2.3. Legislative Practice of the Right to Be Forgotten in China

Although China's legal system has not explicitly defined the "right to be forgotten" as a legal right or category, several existing laws and regulations already contain elements or counterparts of this concept.

Article 36 of the Tort Liability Law, which came into effect in 2010, established obligations such as deletion, blocking, and disconnection of links. It allowed individuals who were harmed by online torts facilitated through internet service providers to request takedowns via a "notice-and-takedown" mechanism. Article 1195 of the Civil Code later expanded and refined these provisions, specifying how individuals may exercise the right to notify, the penalties for false notices, and the corresponding obligations of network service providers.

In December 2012, the Standing Committee of the National People's Congress passed the Decision of the Standing Committee of the National People's Congress on strengthening the network information protection. Article 8 of the decision stipulates that citizens can request network service providers to delete information that infringes on their legitimate rights and interests and commercial electronic information intrusions. In this decision, the objects to be deleted are no longer limited to infringing information, but also include intrusive commercial electronic information.

In February 2013, the Guideline for personal information protection within information system for public and commercial services, issued by the Ministry of Industry and Information Technology, came into effect. This guideline is China's first national standard for personal information protection. Section 5.1 of the guideline stipulates that the deletion link is one of the four important links in the processing of personal information in the information system.

ISSN: 2710-0170

Section 5.5 of the guideline stipulates that only under the premise of "legitimate reasons" can the information subject achieve the purpose of requesting the deletion of personal information in the information system. After the purpose of using personal information notified is achieved or the explicit storage period of personal information is exceeded, the personal information manager should delete it in a timely manner even if the information subject does not request deletion. It also stipulates the exceptions to the deletion of personal information, namely "when it may affect the investigation and evidence collection of law enforcement agencies."

In March 2013, the Credit Reporting Industry Regulations came into force. Article 18 stipulated that negative credit records must be removed five years after the termination of the adverse behavior or event.

Article 18 of the Regulations on the Administration of Credit Reporting Industry, which was officially implemented in March 2013, stipulates that five years after the bad behavior or incident ceases, credit reporting agencies shall stop storing negative information on citizens.

China's Cybersecurity Law, enacted in 2017, granted individuals the right to request deletion of personal data collected illegally, improperly, or in breach of agreements. Article 43 of this law also detailed the procedures that network operators must follow to delete or correct data. Although it did not explicitly use the term "right to be forgotten," it closely aligns with its underlying principles.

In 2017, the Cybersecurity Law was passed and came into effect, and Article 43 stipulates that the subject of information has the right to request the deletion of personal information when it is collected by network operators in violation of the law, violation of the law, or breach of contract, and specifies the procedures that network operators should follow to delete or correct it. This provision formally grants citizens the right to deletion in the form of legislation, and although it does not provide for the right to be forgotten, it is already very much in line with the concept of the right to be forgotten.

In 2019, the Cyberspace Administration of China adopted the Measures for Data Security Management, whose Article 8 stipulates that the collection and use rules of a website or application should focus on marking the ways in which the subject of the information can delete personal information; and Articles 20 and 23 stipulate that after a user logs out of an account or refuses to accept targeted push information, the network operator should delete the information that has been collected.

The Personal Information Protection Law was passed and implemented in 2021. Article 47 of the law clarifies several circumstances under which personal information processors should delete personal information, and stipulates that when personal information is not deleted, the information subject can request deletion. The deletion circumstances stipulated by the law include "the purpose of processing has been achieved, cannot be achieved, or is no longer necessary", "the personal information processor violates the law or breaches the contract", and "the retention period expires", and also include "individual withdrawal of consent", which increases the autonomy of individuals in deleting online information.

In summary, China's current laws have provided a legal basis for the construction of the right to be forgotten. However, with the implementation of the Personal Information Protection Law, a controversy has arisen among domestic scholars as to whether the right to erasure provided for in the Law is another expression of the right to be forgotten, and whether the right to be forgotten should be provided for separately. Scholars who support the equivalence of the two believe that the essence of the right to be forgotten is the right to erasure, i.e., individuals are given the right to decide on the handling of their personal information, and have the right to demand that the processor of personal information delete the personal information it has handled in certain circumstances[5], and that the right to be forgotten and the right to erasure both fulfill the requirements of controlling the information of the individual as well as erasing

ISSN: 2710-0170

the historical information in order to protect the dignity of the human being. However, some scholars believe that the two rights are similar but not equivalent. In this regard, it is important to compare the provisions on the right to be forgotten in foreign countries and carefully consider whether the right to be forgotten is equivalent to the right to erasure, and how to better realize the pursuit of the values contained in the right to be forgotten.

3. The local construction of the right to be forgotten

3.1. The personal information protection law as the foundation for local construction of the right to be forgotten

Through comparative analysis with foreign approaches, this paper argues that the deletion right specified in China's Personal Information Protection Law should be regarded as equivalent to the right to be forgotten, for the following reasons:

According to the theory of "the right to self-determination of personal information" put forward by the German scholar Steinmüller, the essence of personal information is that it is the individual's self-determination of his or her personal information, and it is the medium of self-expression and communication with the social environment. [6]Based on this right, the subject of the information has the right to control and consent to his or her own data on an equal basis. In terms of the legislative purpose, both the EU's GDPR and the Personal Information Protection Law provide for defensive rights, which are established to protect the subject's control over his/her personal information from being infringed upon by others, so that the subject can make his/her own decisions and dispose of his/her personal information independently, and to achieve the legislative purpose of protecting the subject's right to personal information.

From the perspective of the applicable circumstances of the rights, the EU's GDPR stipulates six situations in which data controllers must fulfill the obligation to delete relevant personal data, while the Personal Information Protection Law stipulates five. Both laws regard "data is no longer necessary for the purpose of collection", "authorization for personal data processing is withdrawn", and "personal data processing is illegal" as situations in which rights are applicable. In addition, the GDPR also includes two applicable circumstances: "data subject's right to refuse use" and "data processor clears personal data in accordance with the obligations of EU or member state law". However, the Personal Data Protection Law also generally stipulates "other circumstances stipulated by laws and administrative regulations" as applicable circumstances for the right to delete, which can better adapt to new situations that may infringe on the data subject's right to control personal data as technology develops. In addition, both laws stipulate that when the information processor fails to actively terminate the state of retention and storage of information in accordance with regulations, the information subject can exercise the right to delete personal data by applying.

Therefore, in the legal context of China, the right to be forgotten and the right to erasure should be considered as different names for the same right. "Being forgotten" is the state to be achieved by exercising the right, while "erasure" is the method used to exercise the right.

3.2. The concept of the right to be forgotten

Article 3 of the General Provisions of the Civil Code stipulates that in addition to personal and property rights, other legitimate rights and interests of civil subjects are also protected by law. Article 1,164 of the Tort Liability of the Civil Code stipulates that civil relations arising from infringement of civil rights and interests are regulated by this law. The two provisions can serve as the basis for the right to request legal protection. Article 47 of the Personal Data Protection Law stipulates the right to be forgotten, which gives this right a more solid foundation. At the same time, by comparing the foreign right to be forgotten theory, the attributes of the right to be forgotten in China can be defined.

ISSN: 2710-0170

As for the subject of the right to be forgotten, it can be divided into two types: right subject and obligation subject. The right subject of the right to be forgotten is the information subject. When exercising the right to be forgotten, the legal effect of personal information being forgotten can be achieved. It is a consensus reached by the academic community that the right subject of the right to be forgotten only includes natural persons. From the word "individual" used in the provisions of the Personal Data Protection Law, it can be seen that Chinese legislation also limits the right subject of the right to be forgotten to natural persons. As to whether legal persons and unincorporated organizations should be protected by the right to be forgotten, most scholars hold a negative opinion. Although legal persons and unincorporated organizations have some personality rights, the data of legal persons and unincorporated organizations, compared with the personal data of natural persons, focuses more on economic interests rather than personality interests, and does not have general personality rights similar to natural persons. Therefore, legal persons and unincorporated organizations can achieve the maintenance of their information through different paths such as maintaining the right to honor and the right to reputation, and should not be protected by the provisions of the right to be forgotten. When the subject who is able and obliged to process the data does not actively clear the personal information, the data subject requests deletion, and the data belongs to a minor, according to Article 72 of the Law on the Protection of Minors, in addition to the minor himself, the parents or other guardians of the minor can request the data controller to completely clear the data information of the minor user. Article 49 of the Personal Information Protection Law also stipulates that the close relatives of the deceased also have the right to delete the personal information of the deceased, but it is a necessary prerequisite for the purpose of safeguarding the legitimate interests of the close relatives themselves. In addition, the right to be forgotten should have more restrictions on the public figure as a right holder. Because compared with ordinary citizens, public figures often publicize by revealing some relatively private personal information to achieve the purpose of increasing popularity and gaining attention. If public figures are allowed to exercise the right to be forgotten to maintain their personal image after their purpose is achieved, the right will be abused and contrary to the original intention of the legislation. And the knowledge of the information of public figures, especially the information of politicians, is the basic prerequisite for ensuring democratic politics.

The obligor of the right to be forgotten is generally defined as "data controller" in GDPR, while the concept of "personal information processor" is adopted in the Personal Information Protection Law. The so-called personal information processor is an organization or individual who independently determines the purpose and method of processing.[5] Personal information processors include three requirements.[7] First, personal information processors mainly include organizations and individuals. The impact of the right to be forgotten is mainly reflected in the two aspects of information archiving and information acquisition. Therefore, personal information processors should be composed of two major entities: network service operators and search engine operators. Secondly, personal information processors can be either individual processors or joint processors. When personal information processors are joint processors, multiple joint processors shall bear the responsibility of deleting information. In addition, according to the first paragraph of Article 20 of the Personal Information Protection Law, even if there is an agreement between joint processors on the purpose and method of processing data information, it cannot be a reason for the joint processors to refuse to delete personal information. The right holder's right to delete is not affected by the agreement between the obligated subjects.

The exercise of the right to be forgotten by the information subject does not mean that the network data can be deleted at will. First of all, the object of the right to be forgotten must be legally published, correct, and cannot be deleted by autonomous behavior. If the information is false or illegally published, the personal information processor is of course obliged to delete

ISSN: 2710-0170

such information. If the information subject has the ability to delete it autonomously, there is no need to request the personal information processor to delete it by exercising the right to be forgotten. Secondly, there must be a legitimate purpose for deletion. The Personal Information Protection Law clearly stipulates that the personal information processor should delete or the information subject can apply to choose what kind of personal information to be forgotten, that is, the object of the right to be forgotten. According to Article 47 of the Personal Information Protection Law, four types of information can be used as the processing object of the personal information processor when performing its obligations, which can be attributed to the loss of processing purpose, service suspension or expiration of retention period, withdrawal of consent by the information subject, and illegal or breach of contract processing of information by the personal information processor. The four conditions are parallel to each other. If one of them is met, the right to be forgotten can be applied, and it is not necessary to meet them at the same time. Compared with the GDPR's provisions that the object of the right to be forgotten is "incorrect, irrelevant, and outdated" personal information, my country's regulations are more specific and more practical. Whether in the EU, the US or my country, the right to be forgotten is only applied in the civil field, and there is no provision in the criminal field that the right to be forgotten can be applied to past criminal records. It can be concluded that the laws of the above-mentioned regions regard collective interests represented by public interests as more important interests than the right to control personal information. Therefore, the laws of various regions should determine what kind of information can become the object of the right to be forgotten from the perspective of maintaining social public interests.

The right to be forgotten consists of two aspects: on the one hand, the review and deletion obligations of personal information processors, and on the other hand, the request right of the information subject. Personal information processors should actively review whether personal information meets the conditions for being forgotten as stipulated by the law, and delete it in a timely manner when the conditions are met, so as to fulfill the legal obligation to protect the interests of the right holder. When the personal information processor fails to delete the data information that meets the regulations, the information subject can exercise the right to request the personal information processor to fulfill the obligation to delete. In addition, according to Article 44 of the Personal Data Protection Law, personal information processors should guarantee the information subject's right to know about the storage and deletion of their personal information, which is the premise for the realization of the right to be forgotten. However, information processors shall not delete information without the permission of the information subject. From the perspective of reasonably restricting the extension of the concept of the right to be forgotten, the legal application of Article 47 cannot be interpreted in an expanded manner. Whether the personal information subject exercises the right to delete personal information or the information processor actively deletes the information, it should be subject to the five circumstances stipulated by the law. The personal information subject cannot claim to exercise the right to self-determination of personal information and expand the scope of deleting information.[8] After the right to be forgotten is applied, the information that should be deleted cannot be retrieved or accessed by any information network user. At the same time, the "Personal Information Protection Law" stipulates restrictions on the exercise of the right to be forgotten, which can be summarized into two situations. When the deadline has not expired and the technology cannot be realized, the personal information processor is exempted from the obligation to delete. Such regulations urge the right holder to actively exercise their rights and the information processor to take the initiative to assume obligations, so that the actual application of the right to be forgotten can be realized. The exemption situation also avoids excessive requirements on the obligated subject and excessive constraints on the development of the Internet industry.

ISSN: 2710-0170

3.3. Optimizing the Right to Be Forgotten

China's right to be forgotten system should be optimized from both the substantive law and procedural law levels.

From the perspective of substantive law, firstly, since mobile communication devices are commonly and frequently used by minors, minors are more likely to access the Internet than before. However, due to their lack of experience, minors are relatively lacking in awareness of the protection of personal information in virtual space, and their personal information is more likely to be leaked, requiring greater protection of the right to be forgotten. Therefore, we can learn from the special protection of minor Internet users in the United States "Eraser Act". Compared with the conditional forgetting of personal information data of persons with full capacity for conduct, the right to be forgotten should be applied to all personal data information of minors on the Internet, prohibiting personal information processors from storing and applying minors' personal information or significantly reducing the retention period of minors' information, so as to avoid minors leaving negative information and bringing negative impacts on their future development.

Secondly, a sound information classification system should be established to determine what kind of personal information can be subject to the right to be forgotten under what circumstances, so as to achieve more efficient protection of personal information. Personal information can be divided into several categories. First, personal information is collected by personal information processors without the consent of the data subject. The collection of such information is illegal in itself. Therefore, the data subject can also request the right to be forgotten for their personal information at any time without other reasons. Then, for relatively private personal information such as ID card number and home address that are passively published on the Internet by the personal data subject at the request of the website, such information is legal, and whether the right to be forgotten should be applied and the scope of application of the right to be forgotten should be determined in combination with actual conditions. Finally, for information that the personal information subject actively publishes in the virtual space, the right to be forgotten should be applied without affecting the national interest, public interest or the legitimate interests of third parties, and no other conditions should be attached.

A complete procedural law is an important guarantee for the implementation of substantive law. According to the provisions of the Personal Information Protection Law, the national cybersecurity and informatization department and relevant departments of the people's government at or above the county level are the personal information protection supervision and management departments.[9] However, compared with information processors who are often legal persons, information subjects as natural persons are often in a relatively weak position. It can be stipulated in the procedural law that the people's court where the information subject is located has jurisdiction over the case, so as to ensure that the information subject can more fully exercise the right to be forgotten to defend his or her legitimate interests.

In addition, as international trade becomes more frequent, a considerable portion of information processors are overseas companies, so disputes over the right to be forgotten involve extraterritorial jurisdiction. my country can refer to the EU's General Data Protection Regulation, which stipulates that the applicable objects are any entity that provides network information services to the EU, and include overseas companies in the jurisdiction of my country's laws related to the right to be forgotten, so as to safeguard the personal information security of Chinese network users worldwide and safeguard my country's information sovereignty.

ISSN: 2710-0170

References

[1] Chen Jianzhang. Considerations on the right to be forgotten in the era of big data[J]. Journal of Southeast University, 2022, 24(S1): 50.

[2] Yang Lixin, Han Xu. The localization and legal application of the right to be forgotten in China[J]. Applicable Law, 2015, (02): 24~34.

[3] Pei Honghui. The US pushes for an "eraser" bill to erase minors' online mistakes[J]. Law and Life, 2014, (01): 42~43.

[4] Hong Danna. The legitimacy of the right to be forgotten in the era of big data[J]. Journal of South China University of Technology, 2021, 23(01): 73~83.

[5] Cheng Xiao. On the right to deletion in the personal information protection law[J]. Social Science Journal, 2022, (01): 103~113.

[6] Wang Liming. On the right to delete personal information[J]. Eastern Law, 2022, (01): 38~52.

[7] Lian Zhiying. The impact of the right to be forgotten on information archiving and information acquisition in libraries and archives[J]. Library and Information Work, 2021, 65(16): 35~41.

[8] Liu Honghua. The american model of right to be forgotten legislation and its egislative enlightenment--Based on the research background of california's right to be forgotten legislation[J], 2022, 20(01): 93~105.

[9] Chen chen. The legal research path of the right to be forgotten in the digital age——Based on personal information protection and data security[J]. Journal of Yancheng Institute of Technology, 2022, 35(01): 23~27.