International Journal of Multiphysics
Volume 18, No. 3, 2024
ISSN: 1750-9548

Privacy Protection in the Big Data Era: Judicial Renewal of the Right to be Forgotten Institution of PRC

Cong Sun*
Luoyang Normal University, Henan 471934, China
*Corresponding Author.

Abstract

The Right to be Forgotten, serving as a traditional leniency right, assumes an increasingly pivotal role in upholding democratic values and maintaining order in the era of big data. Nevertheless, the Personal Information Protection Law does not acknowledge this right, but merely stipulates the Right to Delete, assigning it a singular attribute of private law. From a legal theoretical perspective, the Right to Delete corresponds to instrumental value, emphasizing 'control' and inheriting the attribute of public law; the Right to Be Forgotten aligns with normative value, stressing 'communication' and 'dialogue', and possessing an attribute of private law. Functionally, the prevailing Right to Delete essentially amalgamates the aspects of deletion and forgetfulness, thereby failing to fully harness the combined efficacy of both. It is recommended to adopt a path of judicial reconstruction, formulating a system for the Right to Be Forgotten that caters to China's indigenous needs within the framework of Article 47 of the Personal Information Protection Law. In individual case adjudications, the applicable contexts for the Right to Be Forgotten, as well as the execution and safeguards of forgetting measures, should be explicitly identified across three dimensions of logical argument and evidence, by imposing limitations on purpose and necessity. This approach would facilitate the realization of the normative articulation of the Right to Be Forgotten. In the era of big data, the establishment of the Right to be Forgotten legal institution will serve as a powerful guarantee for the effective implementation of privacy protection technologies.

Keywords: Big data, personal information protection act, right to delete, right to be forgotten, judicial renewal.

1. Introduction

In the era of big data, computer technology has played an irreplaceable role in enhancing information processing efficiency and driving socio-economic development. However, accompanying this progress are increasing concerns about privacy breaches and misuse of personal information, posing serious threats to individual rights. Despite achievements in privacy protection through technologies like encryption and anonymization, these measures are limited and fail to fully address privacy concerns. [1] Against this backdrop, the role of legal frameworks becomes significantly important. They not only supplement technical measures, offering a more robust safeguard for privacy protection but also deter violations and repair victim's rights through penalizing illegal acts and upholding victim's interests.

In China, the enactment of the Personal Information Protection Law provides a solid legal basis for the protection of personal information. Particularly, the provision on the right to deletion offers individuals an effective remedy, enabling the possibility of being "forgotten" in the digital realm. However, to fully leverage this provision, it's necessary to clarify its scope of application, operational procedures, and other key issues in practice. This requires judicial interpretation and supplementation, or judicial construction, where courts interpret and supplement legal provisions during case adjudications, thereby constructing a right to be forgotten system that aligns with China's

national conditions. The establishment of such a system would not only better protect individual privacy but also promote social fairness and justice, enhancing people's trust and participation in the digital economy.

Therefore, this paper aims to explore the achievements and challenges of computer technology in privacy protection during the big data era, and analyze the vital role of legal systems therein. Specifically, this paper will focus on discussing how China can rely on the right to deletion provision in the Personal Information Protection Law, through judicial construction, to establish a right to be forgotten system that not only meets international norms but also suits domestic realities, providing stronger legal support for the protection of individual privacy.

2. The Nature of the Right to Delete Personal Information in the Domestic Legal System

In China's current legal system, the right to delete personal information (after this referred to as the "right to delete") is one of the rights in the protection of personal information, and it belongs to the system of personality rights as a whole, which has the attributes of private law. However, in the context of Article 47 of the *Personal Information Protection Law*, the right to delete has specific public law attributes. The contradiction in the attributes of the right stems from the mixing of the functions of the right to delete and the right to be forgotten under the current law. However, it also provides a premise for the continuation of the native right to be forgotten.

2.1 The private law orientation of the right to delete under the systemic interpretation

The right to delete in China's current civil legal system has obvious private law attributes. From a doctrinal point of view, the right to delete is a power of personal information. Currently, the relevant provisions of the *Civil Code* assume the general provisions for protecting personal information in China.

First, from the perspective of legislative history, China's legislature and academia have included the personal information protection system in the legislative plan of the *Civil Code* since the beginning, thus confirming the private law attribute of the right to delete at the legislative level. 2016, the emergence of the *"Xu Yuyu"* case directly prompted the personal information protection provisions to be included in the *"General Rules of the Civil Law (Draft)"* (Second Review Draft). In 2017, the *General Rules of the Civil Law* finally adopted the personal information protection provisions in the draft. They provided a more detailed description, including Article 111: "The law protects personal information of natural persons. Any organization or individual that needs to obtain another person's personal information shall obtain it by the law and ensure the security of the information and shall not unlawfully collect, use, process or transmit another person's personal information or unlawfully trade in, provide or disclose another person's personal information." After enacting the *Civil Code*, the articles above were retained. Article 111 is categorized under the "Civil Rights" chapter and is a general provision. Articles 1034 to 1039 are special provisions on "Privacy and Protection of Personal Information" under the "Title of Personal Rights." The right to delete is stipulated in Article 1037, paragraph 2.

Secondly, from the perspective of systemic interpretation, the right to delete also has obvious private law attributes. The right to delete is a subordinate concept to the right of personality in the logic of civil law and is a substantive right. In nature, the right to personal information is the basis of the right to delete. From the perspective of the *Civil Code*, personal information and the right to privacy are stipulated in the Title of Personality Rights, which is a legally recognized and protected personality right. Therefore, from a normative point of view, the right to delete is a right to personal information. However, the legislature has treated it as a right from the context of the Code and its words. For example, Article 1037 (2) provides for the right to delete by using the expression "the right to request," which shows that the *Civil Code* has recognized the right to delete as a right. [2] At the same time, as a specialized law on protecting personal information, the *Personal Information Protection Law* explicitly states in Chapter 4 that personal information includes the right to delete, access, copy, correct, and supplement. The previous provisions constitute a "bundle of rights," and each protects personal information. Among these, the institutional function of the right to delete is to protect the integrity of personal information in the context of relevant processing activities and the subject's right to information self-determination. Regarding the language used in the provisions, the *Personal Information Protection Law* recognizes the above rights in the title of the chapter "Rights of Individuals in Personal Information Processing Activities" and the corresponding provisions, which use the word "rights." Accordingly, although the right to delete is a personality right in the normative sense, it has been recognized as a substantive right in the actual legislation.

2.2 The public law orientation of the right to delete under a contextual interpretation

Although in the current legislative system, the right to delete is a substantive right of personality in civil law and therefore has the attributes of private law recognized by national law. However, let us look deeper into the context of the legal provisions. The right to delete has a clear public law orientation, which is mainly manifested in the following aspects.

2.2.1 The public nature of the object of protection

As one of the main elements of personal information rights and interests, the right to delete protects personal information, i.e., "all kinds of information recorded electronically or by other means relating to an identified or identifiable natural person, excluding anonymized information." From the legislative provisions, personal information is a somewhat generalized concept in which all "identified" and "identifiable" information about a specific natural person is included, and thus its scope goes far beyond traditional privacy. Based on everyday life experience, defining personal information by the provisions of the *Personal Information Protection Law* and requiring the processor of personal information to obtain consent for all activities would completely block regular social interactions. The object of the right to delete, which the current law seeks to protect, has a particular public nature because it involves forming social interactions. Therefore, if the right to delete is to consistently maintain its private law attributes in the current legal system, the following two elements should be introduced to realize the restriction of the scope of the object, i.e., the data controller and the processing activities. In other words, the objects protected by the right to delete should be the personal information involved in the data controller's data processing activities, and no personal information other than that involved should fall within the scope of the objects protected by the right to delete. [3]

The above argument can also be supported from the perspective of comparative law. From the current practice of personal information protection legislation in significant economies worldwide, the essence of "personal information protection" is "personal information processing protection," i.e., the protection of personal information is realized through regulating personal information processing behavior. Therefore, the target of the right to delete is the "personal information processor," i.e., the "organization or individual who independently decides the purpose and method of processing personal information." In light of current legislation and practice, the purposes and methods of processing personal information involve social interaction or public opinion and thus have a certain degree of public nature. As such, the objects protected by the right to delete and the objects to which they are directed have a certain degree of public character. The most common example is where a particular natural person's personal information is freely available to others when they are in or out of a public place. However, it is only where, for example, the operator of a closed-circuit television system collects information about them for a particular purpose that they are subject to the protection of personal information law.

2.2.2 The public nature of the subject of the obligation

According to the *Personal Information Protection Law*, the subject of the obligation to delete is the processor of personal information, which is a unique subject, not "any organization or individual." The provision mentioned contradicts the nature of the right of personality, a right erga omnes. Since the right to personality is a temporal right, the subject of its obligation should be universal and general, i.e., no organization or individual can infringe upon it. Therefore, as an essential content of the right to privacy, due to its nature of not wanting to be known, any organization or individual is the subject of the obligation not to disseminate. In contrast, the subject of the right to delete is a specific "processor of personal information," which is a specific subject of obligation and has the nature of a personal right. The reason for this is that personal information itself has specific attributes of social interaction, and the actions of those who process it often determine whether or not social interaction and public opinion can be successfully realized or formed, thus assuming certain obligations of a public nature. Therefore, the subject of the obligation of the right to delete is not only of a unique nature but also of a public nature.

A generalized definition of the obligatory subject of the right to delete based on the internal logic of the right to personality would dissolve the public nature of its mandatory subject. In everyday social communication, inter-subjective interaction is the natural process of leaving a specific impression on each other. In this process, each participant is always consciously or unconsciously exchanging personal information with the person he or she

interacts with. In other words, personal information is not so much "acquired" as it is naturally generated by the "impressions" of the social actors in their daily interactions. Therefore, the generation and dissemination of personal information as an "impression" belongs to the realm of private life and social autonomy, and not only does it not require the intervention of the law, but it is also unnecessary to use the law to define the meaning of "consent" "obtained by the law" "unlawful collection" and "illegal collection" There is no need to define by law such behaviors as "consent" "acquisition by law" "illegal collection and use". However, civil legislation follows the conventional sense of including the right of deletion in the category of personality rights and constructing the relevant legal system based on the concept of the right to privacy. This situation undoubtedly contradicts the intent of the *Personal Information Protection Law*, which in turn denies, to a certain extent, the public nature of the subject of the obligation of the right to delete.

2.2.3 The public nature of the right to delete itself

By nature, personality rights are negative rights, defensive and prior, so legislation usually does not list their rights. Professor Liang Huixing summarizes the mode of protection of personality rights in civil law of various countries as "type confirmation + tort liability", i.e., "through legal provisions or jurisprudence to confirm the type of personality rights, ... will infringe on the victimization of personality rights into the scope of application of tort law, and the perpetrator will be punished for the infringement. incorporate the infringing behaviors that violate various personality rights into the scope of application of tort law, and hold the infringers liable for the infringement of tort." [4] In contrast, personal information is not handled in the same way, and it is impossible to accurately identify whether a specific act of control infringes on the subject of the information. Therefore, the text of Article 47 of the *Personal Information Protection Law* directly sets out the particular rights and uses them as a legal basis for information subjects to counteract information processors' processing behavior to maintain everyday social interactions and public opinion. Accordingly, the right to delete is given the attributes of a new type of public law right. It becomes a legal obligation for information controllers, the violation of which constitutes an infringement of the rights of the subject of the information, thus ultimately realizing the legislative value of the subject of the information's self-determination.

In addition, regarding the mechanism of rights protection, the context of Article 47 of the *Personal Information Protection Law* also indicates that the right to delete has a public law orientation. Civil rights are usually protected by "ex post facto relief + tort compensation." Among them, civil liability mainly stops infringement, removes obstruction, eliminates danger, compensates loss, eliminates influence, restores reputation, and apologizes. This mode contains two meanings. One is that the subject of civil rights confrontation is equal civil subjects, and the second is that the public power will not protect them beforehand. However, in the asymmetric structure of information subjects and information processors in the network era, the right to delete, if purely civil, will be difficult to exercise effectively due to the lack of public power intervention. The dilemma will be further amplified if the information processor is a public authority. The result would be that the right to delete would become a dead letter. The situation above would defeat the purpose of Article 47. The right to delete should therefore be a public law right. Only in this way can the subject of information use this right to overcome the disadvantages caused by the asymmetric structure of the network era, realize the legislative purpose of self-determination of personal data, and give practical significance to Article 47.

In conclusion, in the current system, the right to delete is not a purely private law right but a new type of right with specific public law attributes. The personal law attribute of the right to delete mainly comes from the legal system in which it is located, which is mandatorily given by the legislative behavior led by the traditional civil law theory. However, only in terms of its textual language and internal logic, the right to delete cannot be a purely private law right; otherwise, in the era of big data on the Internet, it will lose the significance of being included in the *Personal Information Protection Law* due to the lack of exercisability. Therefore, the right to be forgotten should be a "new right in positive law" with public and private law attributes. [5] Only with this in mind can we continue to explore the renewal of the right to be forgotten in China.

3. The Relationship between the Right to be Forgotten and the Right to Delete

From a temporal perspective, the right to be forgotten and its conflation with the right to delete originated from European legislative practice. The Article 47 of China's *Personal Information Protection Law* only provides for the right to delete without mentioning the right to be forgotten, similar to the legislative model of the *European Union's General Data Protection Regulation* (GDPR, referred to as "the *Regulation*"). This combined legislative model has compounded the public and private attributes of the right to delete in China's legislation.

However, the right to be forgotten and the right to delete are two different rights in the pursuit of value and the scope of application. The right to be forgotten is mainly applied in the field of public discourse, which is an essential means to maintain modern democratic order; the right to delete is primarily applied in personal information protection, which is the leading way to safeguard the self-determination of personal information. Therefore, it is necessary to adhere to the legislative model of the dichotomy between the right to delete and the right to be forgotten. In China's current legislative model, which only provides for the right to delete, the two should be restricted at the jurisprudence level so that the judiciary can effectively resolve disputes over personal information based on different value pursuits in the public and private spheres through judicial renewal.

3.1 Deficiencies in the google spain judgment

The controversial 2014 judgment of the Court of Justice of the European Union (after this referred to as the CJEU) in *Google Spain SL v. Agencia Española de Protección de Datos* led directly to the adoption of a combined legislative model for the right to be forgotten and the right to delete in the *Regulation* (2016). In its judgment, the CJEU held that both Article 7 of *Directive 95/46/EC* (starting now referred to as the *Directive*) and Article 8 of *the Charter of Fundamental Rights of the European Union* (after this referred to as *the Charter*) authorize "data subjects" to request search engine operators to "remove" them from the list of results displayed for searches based on their name to links to web pages legitimately published by third parties and containing truthful information about him, because he would like that information to be 'forgotten' after a certain period. [6] In its judgment, the CJEU eschewed judicial judgment on Google's collection and processing of customers' personal information, focusing instead on restrictions on Google's public dissemination of public information. To this end, the Court introduced the right to be forgotten in its judgment. The case was decided based on Article 8 of *the Charter* and the *Directive*, and in the course of its reasoning, the Court significantly expanded the scope of application of the principle of "fair information practices."

The *Regulation* issued in 2016 reaffirmed the expansive interpretation in the *Google Spain Case*, and on May 25, 2018, made it official legislation in all EU member states. The *Regulation* has since replaced the *Directive* and incorporated the right to be forgotten into formal EU legislation. In the *Regulation*, the EU legislature named Article 17 "the right to delete ('right to be forgotten')" thereby conflating the right to delete and the right to be forgotten at the verbal level. The situation mentioned is because the legislature and the courts need to understand the legal tradition, thus confusing the institutional starting point of the right to be forgotten and deleted. As a result, the *Regulation* provides for the right to delete and be forgotten in the same provision in an ambiguous manner, causing severe confusion between the two.

In the EU legal tradition, privacy has been categorized into two distinct types based on value. One is data privacy protected by the "fair information practices" in the *Directive*. The primary purpose of this rule is to regulate the handling of personal information to ensure that such information is collected by lawful means for a specific purpose. Data privacy operates based on an instrumental logic that gives citizens the "right to control" their data. In this institutional framework, data subjects do not need to prove the existence of damage when claiming infringement of their data privacy. Another category is dignity and privacy. This type of privacy is usually protected under section 7 of *the Charter* at the level of human dignity, i.e., it should not be degraded, humiliated, or used as a right to insult others in social interactions. Protecting dignity and privacy follows a normative logic intended to protect against damage to another person's personality caused by violating civil norms. [7] However, the decision in the *Google Spain Case* confuses these different types of privacy.

The *Google Spain Case* was first heard by the Spanish data protection authority (Agencia Española de Protección de Datos et al., AEPD) in 2010 and then appealed by Google to the Spanish High Court of Justice. In its judgment,

the High Court of Justice took Articles 7 and 8 of *the Charter* as the basis for its reasoning, citing the relevant interpretation of the CJEU. An examination of the text of the judgment shows that the central issue in the *Google Spain Case* was whether Google's processing of the data contained in the La Vanguardia website was contrary to the requirement that "the search engine operator carries out the processing in question intending to make it inappropriate, irrelevant or no longer relevant, or excessive". The CJEU has made it clear in relevant judgments that a violation of the *Directive* does not require "bias against the data subject." [8] The basis of the judgments above is that data privacy is compromised whenever a data controller processes personal data in a manner unrelated to the specific purpose for which the information was obtained, regardless of whether or not there is collateral physical or material damage. In short, according to the logic of the CJEU's reasoning, there should be a "specific purpose" for any data processing. Therefore, the logic of the argument invoking data privacy cannot be justified without a specific purpose for processing personal data.

Given the above deficiencies in the argumentation, it is necessary to restate the basic concepts of "personal data" and "processing" involved to clarify the basic logic of the reasoning in the judgment of the case. The *Directive* applies to the "processing" of all "personal data," which refers to all kinds of information relating to an identifiable person. Accordingly, "personal data" has two qualities: it is not limited to private information, and it is information that, if disclosed, would cause damage to the data subject. The *Directive* defines "processing" in similarly broad terms: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Accordingly, the text of the *Directive* suggests that it should not be confined to a specific domain constructed on the basis of a narrow instrumental logic, but should be applied to the broader social sphere. In reality, however, it is possible for anyone to "process" their own or another person's "personal data" without having a "specific purpose." This scenario creates a fundamental conflict with the personal data protection regime that the legislator of the *Directive* intended to build. As noted above, the "processing" the *Directive* recognizes is necessarily linked to a "specific purpose." The underlying cause of this conflict stems from the provisions of Article 8 of *the Charter*. The text of this article suggests that its normative character is relevant only in the context of the accumulation and use of large-scale data by governmental or commercial organizations. In other words, Section 8 of *the Charter* makes a value claim. It is protecting the control of individuals over their data who are in a weaker position compared to government and commercial organizations. In the case of government agencies, data is processed for "mass surveillance." In the case of commercial organizations, data is also collected for "mass surveillance" to determine credit ratings or to minimize costs. The textual structure of Article 8 is, therefore, successful in ensuring that, in the cases mentioned above, the processing of personal data is limited to the appropriate purposes and is accountable to the legitimate concerns of the data subject.

However, there needs to be more clarity between the internal logic of Article 8 and people's everyday practical experience. For example, both the *Directive* and the *Regulation* stipulate that the mere "processing" of personal data through the retention of "filing systems" that are not "solely" for personal or family activities constitutes "processing" of personal data. In reality, substantial government *Regulation* is necessary for the large quasi-bureaucratic organizations that the *Directive* and the *Regulation* are intended to regulate. Nevertheless, in the everyday lives of ordinary people, such formal obligations are clearly out of place. In sum, the fatal error in the *Google Spain* decision was the Court's attempt, through interpretive techniques, to isolate certain positive information from the social practices that gave rise to it.

3.2 The essence of the relationship: integration of public and private law based on the pursuit of the value of self-determination of personal information

The legislator of the *Directive* and the *Regulation* was aware of the contradiction between the above norms and the reality and therefore excluded from both laws the *Regulation* of the processing of data "by natural persons in the course of purely personal or family activities." However, this remedial measure did not allow the *Google Spain Case* to avoid the errors that had been foreseen since the fundamental aim of the *Directive* and the *Regulation* is to "de-embed" specific information processing behaviors. The scenario above runs counter to the laws of human interaction in social practice, distorting the relationship between the right to delete and the right to be forgotten,

blurring the boundaries of their respective fields of application, ultimately resulting in legislative confusion.

In practice, by virtue of their social interactions, human beings construct a public discourse/information sphere at the societal level, which may include both individual data processing with a specific purpose and a large number of data processing acts that lack a clear purpose. In this complex social subsystem, the "specific purpose" of a data processor's processing should have been carefully scrutinized to determine whether the *Directive* and the *Regulation* should regulate the processing. However, the CJEU in the *Google Spain* judgment not only ignored the identification of "specific purposes" but also asserted that a data processor's actions achieve the factual status of online data capable of being accessed by an unspecified majority of persons. The *Directive* should regulate the factual situation because it goes beyond "personal" or "family" use.

The normative and analytical framework in Article 8 of the *Directive* is incompatible with the exchange of data-based public discourse. As the overriding fundamental principle of Article 8, "fair information practices" allow ordinary citizens to "control" their personal data. At the same time, the *Regulation* also explicitly states that "natural persons shall have the right to control their data." Based on the value of fairness in the principle of the rule of law, personal data generated in a mass surveillance structure should, subject to certain exceptions, be controlled by natural persons in a vulnerable position rather than by public authorities or quasi-bureaucratic organizations that can exert direct influence over them. [9] However, the emphasis on "control" of personal information in EU legislation is misplaced if one looks beyond the dichotomy of organized institutions and atomized individuals and considers social interaction in the network age as an ongoing dialogue between people. Thus, "control" means, in a sense, that a particular person "owns" personal information. This view is at odds with the social practices of the Internet age. In the context of sustainability dialogues, individual citizens' "control" of personal information is no longer at the top of the value hierarchy, and legitimate public order concerns will be visible in the value sequence of personal information protection. Attention to the value of "control" will partly shift to promoting sustained public discourse to maintain a democratic public order. In essence, the "control" theory of personal data will be unsustainable when the underlying values of personal information protection are constructed to enable sustained public dialogue.

The text of Article 8 of the *Directive* is written in a regulatory rationality that completely excludes the mode of social interaction of public discourse based on a pluralistic mesh structure. The legal conceptual structure embodied in the text of Article 8 would therefore eliminate the possibility of democratic legislation. Moreover, in order for Article 8 to be implemented in a way that does not contradict *the Charter*'s provision on "freedom of expression," the *Directive* also has to choose to exclude certain public discourses from its scope of *Regulation*. Thus, at the heart of the relationship between the right to delete and the right to be forgotten is the harmonization of "data privacy" with "freedom of expression and information." Both the *Directive* and the *Regulation* need to provide clear instructions. In EU practice, when there is a conflict between the two, law enforcers usually adopt a "balance between data privacy and freedom of expression" approach to harmonize the relationship. However, this approach fails to achieve an effective balance because it is based on norms that divide data privacy and freedom of expression into two mutually exclusive social subsystems. In other words, the very basis of public discourse is undermined by the processing of personal data under the regulatory logic of data privacy. At the same time, the principle of "fair information practices" cannot be justified if public discourse is not subject to that logic and can freely express its ideas and interests. In sum, current European Union law cannot protect data privacy while preserving the formation of public discourse because data privacy exists in a dichotomous world picture incompatible with the social interactions that form public discourse.

At this level, the right to delete (the right to be forgotten) constructed by the *Directive* and the *Regulation* contrasts with the right to be forgotten in the traditional sense. In traditional legal systems, the right to be forgotten is often used to reconcile the conflicting values of personality-based privacy and public discourse. In essence, the traditional right to be forgotten concerns whether a particular social interaction is offensive because it contradicts the "customs of the community": if it is offensive, the particular social interaction can be forgotten; if it is not, it cannot. Thus, at the legal level, social interactions that violate privacy rules are recognized as causing humiliating damage, and the right to be forgotten should not apply. It is thus clear that the traditional right to be forgotten does not focus on the personal data itself but only on the damaging consequences of a particular behavior. In applying

the traditional right to be forgotten, courts typically examine whether the particular conduct of the interaction is consistent with the "civil rules" that define the identity of individuals and communities. Rather than focusing on the personal data itself, this approach seeks to determine whether particular interactions are consistent with the "civil rules" that mutually define the identity of individuals and communities. In other words, courts rely on these rules to examine the appropriateness of the interaction, i.e., whether it conforms to a "carefully calibrated system of social norms ..... that define and sustain essential activities and key relationships and interests." [10] In short, the right to be forgotten should be a right that can be integrated into public discourse.

The relationship between the right to delete and public discourse differs from the right to be forgotten. The reason why the right to delete cannot be reconciled with public discourse is not only that people do not always participate in social interactions with a predetermined 'precise purpose' but also that the 'control' of personal data subjects over their personal information may impede the formation of public discourse, which may conflict with democratic values. By contrast, while the right to be forgotten may create tension with freedom of expression by limiting social interaction, it does not necessarily conflict with the democratic function of public discourse.

Freedom of expression gives people the right to participate in the formation of public opinion and to visualize the feedback of opinion from the State. Freedom of expression is, therefore, often seen as essential to the democratic order. However, suppose the sphere of public discourse is rendered uncommunicative, even abusive and hostile, due to the "control" of various personal information. In that case, people cannot use it as a possible medium for forming public opinion. As a result, public discourse will no longer legitimize democracy, thereby undermining the validation of democratic values for freedom of expression. The results in the so-called "paradox of public discourse," whereby public discourse preserves democratic legitimacy on the premise that it can operate in a minimally civilized manner, but where the imposition of civilization restricts freedom of expression. This paradox suggests that the right to be forgotten can be reconciled with the democratic function of public discourse in a way that the right to delete cannot.

4. The Institutional Renewal of the Native Right to be Forgotten

4.1 The need to renew the right to be forgotten

The right to be forgotten and the right to delete do not protect the same values. The leading institutional goal of the former is to realize the forgotten values of traditional society in the network environment to benefit personal development, maintain regular social interaction, guarantee the usual construction of public discourse and social consensus, and effectively safeguard democratic values. In real society, the forgotten value is one of the key factors to guarantee the free development of individual personality, which is related to whether the wrongdoer can reintegrate into society. The inability to be forgotten may hinder the sound development of an individual's personality, making it difficult for him or her to pursue life goals independently. [11] For example, contemporary developed countries with the rule of law have established a system of sealing the criminal records of juveniles at fault, using a strict sealing system to achieve a state of oblivion in the public discourse and to give juveniles at fault a chance to reform themselves, to safeguard their re-socialization and personality interests. In essence, being forgotten is one of the concrete manifestations of the value of social tolerance, implying the community's forgiveness of the perpetrator's faults, allowing him or her to remove the negative label through anonymous life and get a fresh start. From a functionalist perspective, being forgotten is a catalyst for the formation of forgiveness, which can shorten the process of forgiveness for the wrongdoer and make it easier for him or her to re-enter everyday social interactions. However, big data technology has sharply increased the cost of realizing the value of being forgotten. Therefore, it is necessary to respond to the new challenges posed by new technologies by establishing the right to be forgotten.

First, the "Internet memory" of long-term storage undermines the value and function of traditional forgetting. In the pre-Internet society, members usually "forget" because of their limited memory. However, the virtual Internet environment creates convenient conditions for permanently tracing individual social behaviors, thus forming the so-called "Internet memory." In such an environment, the negative information or faulty behaviors of an individual will be retained entirely in cyberspace so that the "label" assigned to him or her at a particular time cannot be erased by the passage of time, thus making him or her more prone to social prejudice or negative evaluations by

others.

In addition, data mining, collection, storage, and analysis in the era of big data have further exacerbated the impact of "Internet memory". At the present stage, based on big data, any desired trajectory of network activities can be obtained through algorithmic information surveying, intelligent aggregation, and data recovery, resulting in serious misuse of information. Meanwhile, the data crawling and analysis process is characterized by opacity and unpredictability. This behavior can take very little information as a clue and gradually put together a "portrait" of a specific individual, thus creating a de facto state of privacy leakage.[12] These situations may reinforce the effects of "Internet memes" by making it more difficult to forget, as the public passively receives specific information about others repeatedly.

Second, the traditional legal framework's safeguard mechanism centered on the right to privacy and the right to reputation cannot respond to the erosion of forgotten values by technologies such as big data. Firstly, the traditional rules of privacy protection cannot respond to the needs of the big data environment. The current law stipulates that "information voluntarily disclosed by an individual in a public place is not private." However, the public sphere in cyberspace today is gradually blurring the public-private boundary due to technological advances' constant erosion of the private sphere. [13] In other words, advances in data technology may confer privacy interests on private information in the public sphere, thereby weakening the protection of the right to privacy under traditional law. In addition, the diversity of information collectors and users, on the one hand, enhances the difficulty of management and control and, on the other hand, blurs the causal relationship between the act of dissemination and the consequences of damage. Secondly, it is difficult to effectively deal with "reputation damage caused by the collation of fragmented information" under the rules of protecting the right to reputation. The information provided by search engines and online information platforms may be one-sided or false, thus failing to present a complete and objective picture of a particular individual's reputation. An individual's image may be created based on false information, which biases public opinion. As a result, a person's reputation may be damaged, and he or she may suffer unfair treatment and financial losses. However, the current legal system for protecting the right to reputation does not effectively regulate such situations. In addition, the persistence of information can also lead to the mutation of the consequences of reputation infringement, which leads to a significant reduction in the effectiveness of the existing protection rules. As mentioned earlier, cyberspace gives information searchability and permanence, which eliminates the expectation of "forgetting over time" in traditional societies and makes information that damages a person's reputation evidence that will not disappear over time. [14] Ultimately, individuals are permanently tied to their past wrongs, rendering claims for damages or rehabilitation meaningless.

4.2 Compatibility of the right to be forgotten with the right to delete

Legislation on the right to be forgotten is a response to the crisis of forgotten values in the context of big data era. China also faces a crisis of forgotten matters arising from "Internet memory." The *Google Spain Case* shows that the interactive combination of a country's rule of law, social economy, traditional culture, and other factors jointly determines the construction of the right to be forgotten. Therefore, the introduction of the right to be forgotten in legislation should be cautious and prudent.

In the Chinese context, the need for legislation to introduce the right to be forgotten has arisen. A series of judgments, such as the*"Ren Jiayu Case"* and the triggered debates, have shown that theoretical and practical circles have had to respond to real social needs. After the *"Ren Jiayu Case"*, there were views in the theoretical and practical communities that the judiciary in China had rejected the introduction and application of the right to be forgotten. Such statements are questionable because of their one-sidedness. The judgment of the case mentioned above is the court combined with the particular circumstances of the file to make a more reasonable decision. Its background and the right-to-be-forgotten system are only partially compatible. In other words, the interest that Ren Jiayu intended to remedy must be consistent with the core value of the right to be forgotten. For this reason, some scholars in China have made a careful and persuasive comparison between the Ren Jiayu and the Gonzalez cases. [15] These two cases differed in two aspects: first, the purpose of the information processor's use of the personal information involved in the case is different; second, the interests of the subject of the data differ. From the perspective of judicial practice, the application of the right to be forgotten depends on the court's

realization of justice in individual cases, i.e., the analysis and consideration of the dispute in a particular case. To summarize, the conditions for applying the right to be forgotten in individual circumstances should be that, on the premise of ensuring that the function of public discourse in shaping democratic values is not compromised, the fundamental rights of the subject of the information should be applied if they will be safeguarded by the application of the right to be forgotten; conversely, the right to be forgotten should be applied with caution.

In conclusion, Article 47 of the *Personal Information Protection Law* implies the right to be forgotten at both the textual and functional levels, and the scope of application of the right to be forgotten is relatively single from the perspective of competence. Therefore, the renewal of the right to be forgotten in China should be based on and framed by the Article 47, adopting the approach of "case analysis + determination of elements."

4.3. Normative expression of China's system of the right to be forgotten

4.3.1 Possibility of renewal of the right to be forgotten under current law

Article 47 of the *Personal Information Protection Law* implies the right to be forgotten, leaving room for judicial renewal and application. As mentioned above, the right to be forgotten corresponds to the democratic value of public nature, emphasizes "communication" and "dialogue," and upholds the democratic value based on the order of public discourse, which corresponds to self-governing thinking. Therefore, the right to be forgotten should be applied to the scenario where the disputed personal information, although legally obtained in compliance with the law, gradually shows non-necessity and non-relevance after being made public, adversely affecting the subject of the data. In contrast, the right to delete is for cases where the disputed information has been violated from the outset or after the fact and corresponds to a regulatory mindset emphasizing "control." Accordingly, the Article 47 of the *Personal Information Protection Law* contains the conditions for the application of the right to be forgotten, namely subparagraphs (i) and (v), while subparagraphs (ii), (iii), and (iv) are more in line with the "control" function of the right to delete.

In addition, from a textual point of view, the wording of the Article 47(a) of the *Personal Information Protection Law* is the same as the scope of "inappropriate, irrelevant or no longer relevant or excessive information" defined in the *Google Spain* judgment. This article is also highly similar to the 17.1.a in terms of the textual structure of the *Regulation*. It can be argued that the right to be forgotten can be exercised by the subject of personal information when "the purpose of processing has been achieved, cannot be achieved, or is no longer necessary for the achievement of the purpose of processing" and the information becomes inappropriate, obsolete, or detrimental to the subject of data due to the passage of time.

4.3.2 Elements and limitations of the application of the right to be forgotten in individual cases

First, the limitation of purpose and necessity. According to the analysis above, the prerequisite for applying the right to be forgotten is that the information processing behavior is legal and compliant; otherwise, the right to delete will be used and adjusted. Consolidating the provisions of Article 6 and Article 47 of the *Personal Information Protection Law*, the application of the right to be forgotten shall follow the principles of purpose and necessity. The direction of purpose means that personal information should be handled for a clear and reasonable goal. In individual cases, if the deletion of undesirable information involving the subject of the information would affect the informed interests, personal and property safety of others, then the act of processing does not meet the purpose requirement. If deleted, it will hinder communication and dialog in the public sphere and affect the formation of consensus. In short, the right to be forgotten should be realized on a case-by-case basis, based on the principle of the purposefulness of the act of information processing and the criterion of whether it impedes the formation of public discourse.

The principle of necessity means that the handling of personal information should be directly related to the purpose of the handling, and that personal information should be collected and handled in a manner that minimizes the impact on the rights and interests of individuals. The application of the right to be forgotten shall likewise follow the requirements of this principle. In the course of processing information, the court may apply the right to be forgotten if the purpose of the processing has been achieved, cannot be reached, or is no longer necessary to achieve the purpose of the processing, as well as for other reasons provided for by the law, and if it hurts the subject of the information and the court is unable to achieve a remedy by exhausting other means of redress.

Second, the qualifying conditions and application scenarios of the right to be forgotten. The fundamental function of the right to be forgotten lies in eliminating or restricting the use and disclosure of past negative information on the subject of information through technical means to realize the freedom of remodeling citizens' identity and surrounding public opinion to ensure the usual construction of public discourse. In terms of the way, the forgotten system is a typical after-the-fact relief. At present, the exploration of the right to be forgotten in China's theoretical and practical communities has become increasingly conservative. At the academic level, there are many alternative rules to the right to be forgotten in China's current legal system, which is sufficient to safeguard the right to personality effectively; [16] At the level of judicial practice, the courts usually take the theory of personality right as the standard of judicial decision. The judicial renewal of the right to be forgotten should follow two restrictions: (1) there is necessary to protect the disputed interest of the subject of information involved in the case; second, applying the right to be forgotten can realize that interest. Accordingly, if the court wants to use the right to be forgotten in individual cases, its legitimacy should follow two steps: firstly, it should judge whether the disputed information has caused unnecessary negative impacts on the subject of the data; (2) it should further argue that the elimination of the negative information will not affect the realization of other rights and interests, i.e., it will not hinder the formation of public discourse. It should be especially emphasized that when applying the right to be forgotten to realize relief, the court should strictly follow the principle of necessity, i.e., the right to be forgotten can only be applied to provide relief after exhausting other means to effectively safeguard the rights and interests of the subject of the information. This circumstance above constitutes the basic scenario for the application of the right to be forgotten by the courts in China.

In addition, the EU's experience in applying the right to be forgotten can also provide a valuable reference for the scenario-specific application of the above restrictions. First of all, the judiciary can consider applying the limits to the field of data market. In the EU, on the one hand, the *Regulation* has set strict compliance standards and high fines for big data industry entities represented by search engine service providers, and on the other hand, the *Google Spain Case* has inspired the public to exercise the right to be forgotten, which has led to an increase in the number of related lawsuits. The phenomenon has created a conflict between industrial development and rights protection. At present, China's big data industry has just started, and the application of the right to be forgotten may cause a significant increase in the cost of compliance, which in turn affects the performance of enterprises, and ultimately impedes the benign development of China's related industries. [17] Therefore, if the right to be forgotten is not applied following the above steps, the scope of application may be too broad, ultimately increasing social communication costs. The result will not only affect the development of the industry but also the protection of democratic values. Secondly, the legislature needs standardize the retention period of data. The retention period provisions for data in China's legal system still need to be further standardized. The *Cybersecurity Law* stipulates that the retention period of weblogs by network service providers is more than six months, while the statutory period of the *Conditions for the Administration of the Credit Collection Industry* is five years. The *Measures for the Supervision and Administration of Network Transactions* stipulates that the retention period for transaction information shall be at least three years from the transaction's completion date. According to the preceding laws and *Regulation*s, as long as the statutory period of information retention is in place, regardless of whether the purpose of personal information processing has been achieved, the information controller will be able to legally defend the deletion or forgotten request made by the subject of the information. This not only directly affects users' rights but also impedes the application of the right to be forgotten by the courts. Therefore, it is necessary to rationalize and standardize the data retention period at the legislative level.

Third, the enforcement and safeguarding of measures of being forgotten. The right to be forgotten can only realize its value through corresponding enforcement measures; that is, under the premise of preserving public discourse and democratic order, it can promote reasonable interactions between the subject of the information and the information processors, controllers, and other members of the public. However, there is a lack of judicial practice in China, so the enforcement measures of the European Union have particular reference value. The *Belgium Google Case*'s judgment provides a reference for measuring the effectiveness of forgetting measures. In 2019, Google Belgium refused to delete the internet information related to the party concerned. Subsequently, the person involved complained to the Belgian personal data protection authorities. The Belgian authorities not only imposed a fine of €600,000 on Google Belgium under the *Regulation* but also required it to clearly articulate the division

of responsibilities for the supervision of the right to be forgotten within the company. The dispute was so contentious that both parties went to the European Court of Justice (ECJ). In the end, the court made the following rulings: (1) Google Belgium's de-listing information was incomplete, non-transparent, and inaccurate, and failed to fulfill the safeguard obligations of search engine service providers effectively. (2) Google Belgium's deletion procedure was misleading, even though the parties mistakenly believed that the realization of the right to be forgotten must be premised on the consent of the original web page administrator. This practice harms the parties' active use of the right to be forgotten to safeguard their rights and interests. In short, the practices mentioned above violate the requirements of Article 5 of the *Regulation*, which stipulates that "the handling of personal information shall be lawful, fair, and transparent."

Then, in the *EU Guidelines on the Protection of the Right to be Forgotten in Search Engine Cases* published in July 2020, the European Union Information Commission (EDPB), based on summarizing the practical experience since the entry into force of the *Regulation*, has further refined the rules on the protection of the right to be forgotten, which mainly include the following aspects: (1) it clarifies the grounds for the information subject to request the processor of the personal information to delete/forget. The document describes in detail the meaning of Article 17 of the *Regulation*, which provides that a request for erasure may be made in cases where data held by a company about an individual is deleted from publicly available information, where a link on a company's website contains the contact details of the data subject of an employee who has left the job, or where personal information has been stored online for a while longer than the legal period. In addition, personal data processors are required to notify a third party of the deletion request, aiming to provide further responsibility to the original controller. (2) the circumstances in which deletion/forgetting can be refused are further clarified, including tasks performed fulfilling legal obligations, the public interest, or in exercising public authority.

As noted above, the realization of the right to be forgotten in the EU is characterized by two main features. (1) In terms of the means of implementation, the primary purpose is to "hide the summary of information" rather than "completely delete information." In this way, when realizing the goal of the right to be forgotten, the information subject does not need to resort to the problematic means of completely deleting the relevant information in cyberspace. Still, it only needs to ask search engines and other personal information processors to take more feasible ways such as deleting the search link, hiding the summary of the information link, and blocking the identity of the information subject. With the help of the "hidden" way, realizing the information subject's right to be forgotten will not cause uncontrollable disturbance to the free flow of information, the construction of public discourse, national security, and other social public values. In other words, the hidden way of realizing the right to be forgotten is more in line with the objective law of human society. Being forgotten has been a relative state since the beginning, and absolute forgetting has never existed. In cyberspace, due to the role of technical factors, the relativity of forgetting has been dramatically weakened. Therefore, the means of "hidden information summarization" is essentially to restore the degree of relativity of forgetting in real society so that the subject of information can be free from unnecessary troubles caused by "Internet memory" due to the natural loss of time. (2) Protecting personal information is prioritized in the trade-off of outcomes. In EU practice, the realization of the right of the information subject to be forgotten generally takes precedence over the economic interests of the processor of the personal information, as well as the interests of the public in accessing information in cyberspace. This prioritization is also more prominently reflected in the case of legal and compliant publication of data on the original webpage. Although this is conducive to safeguarding the rights and interests of the subject of the information, it may not only undermine the order of the data trading market. However, it may also jeopardize the democratic order by impairing the formation of public discourse. Therefore, the use of what kind of forgetting to protect different information involved in the case should be combined with the specific application scenarios in individual cases and be judged by the standard of the most minor damage to the interests involved in the case.

Acknowledgement

This work was supported by Annual Program of Philosophy and Social Science Planning of Henan Province “Research on the Generation and Realization of the Right to be Forgotten in Digital Transformation” (2023BFX018).

References

[1] Qian Wenjun, Shen Qingni, Wu Pengfei, Dong Chuntao, & Wu Zhonghai. (2022). Research progress on privacy-preserving techniques in big data computing environment. Chinese Journal of Computers, 45(4), 669–701.
[2] Wang Liming. (2022) On the right to delete personal information, Oriental Law, 1, 38-52.
[3] Zhou Hanhua. (2020). The legal positioning of personal information protection. Studies in Law and Business, 37(3), 44-56.
[4] Liang Huixing. (2018, May, 18). The protection of personality rights has formed the Chinese experience. Legal Weekly.
[5] Wang Linghao. (2021). The right to be forgotten and its purpose: A critical examination of the normative basis of the right to be forgotten. ECUPL Journal, 24(5), 41-54.
[6] Squires, J. (2014). GOOGLE SPAIN SL v AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (EUROPEAN COURT OF JUSTICE, C-131/12, 13 MAY 2014).
[7] Post, R. C. (2018). Data privacy and dignitary privacy: google Spain, the right to be forgotten, and the construction of the public sphere. Duke Law Journal, 67(5), 981-1072.
[8] Floridi, Luciano. (2015). Should you have the right to be forgotten on google? nationally, yes. globally, no. New Perspectives Quarterly, 32(2), 24-29.
[9] Solove, D. J. (2001). Privacy and power: computer databases and metaphors for information privacy. Stanford Law Review, 53(6), 1393-1462.
[10] Nissenbaum, H. (2020). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
[11] Wang Yikun & Liu Jinxiang. (2022). The path choice and normative remodeling of the localization of the right to be forgotten: Focusing on article 47 of the personal information protection law. Law and Economy, 3, 96-109.
[12] Solove, D. J. (2007). The future of reputation: Gossip, rumor, and privacy on the Internet. Yale University Press.
[13] Zhang Xinbao. (1996). The development of information technology and the protection of the right to privacy. Law and Social Development. 5, 16-25.
[14] Yang Lixin & Han Xu. (2015). The localization and legal application of the right to be forgotten in china. Journal of Law Application, 2, 24-34.
[15] Wan Fang. (2016). The right to be forgotten eventually: Reflections on the introduction of the right to be forgotten in China. Law Review, 34(6), 155–162.
[16] Jiang Su. (2020). Automated decision-making, criminal justice and arithmetic rulemaking: Reflections on the lummis case. Oriental Law, 3, 76-88.
[17] Breznitz, D. (2011). Delete: The virtue of forgetting in the digital age. The Review of Policy Research, 28(3), 307-309.