

Rules for Personal Information Processing in Bankruptcy Proceedings: A Perspective Based on Bankruptcy Administrators

Yule Zhao

Beijing Institute of Technology, Beijing, China

Corresponding author, E-mail: zhaoyule1016@163.com

Abstract

With the advancement of big data technologies and the rise of the digital economy, the legal status of corporate data assets has garnered increasing attention. The bankruptcy case of “Xiaoming Bike” has sparked public concern over the rules governing the handling of personal information in bankruptcy proceedings. However, the traditional legal framework falls short in addressing the legal challenges posed by data—particularly personal information—as a novel type of asset. Currently, Chinese laws and regulations neither provide a clear classification of personal information nor determine whether it constitutes part of the bankruptcy estate. At the same time, the role of the bankruptcy administrator, a key figure in bankruptcy proceedings, lacks legal guidance regarding their obligations and principles when processing personal information. Therefore, it is necessary to clarify the legal nature of personal information before examining whether and to what extent such information should be included in the bankruptcy estate. Building on this foundation, and drawing upon foreign experience, differentiated rules for handling various categories of personal information should be developed from the perspective of the bankruptcy administrator, with an aim to balance the interests of all parties involved.

Keywords

personal information; bankruptcy estate; bankruptcy administrator; proprietary nature

1 Problem Statement

Against the backdrop of the rapid development of big data technologies and the proliferation of digital enterprises, data is becoming a valuable corporate asset, an important factor of economic input, and the cornerstone of new business models[1]. China’s first bankruptcy case involving a bike-sharing company—the “Xiaoming Bike” bankruptcy case[2]—has attracted widespread public attention; however, both media coverage and popular discussion have largely focused on the issue of how user deposits should be refunded[3].

Data assets are data resources that are lawfully owned or controlled by a specific entity, can continuously function, and are capable of generating direct or indirect economic benefits; they are characterized by intangibility, diversity, and volatility in value[4]. With respect to whether corporate data can constitute an object of property rights, the academic community is divided into three main positions, namely the “affirma-

“negative”view[5],the“negative”view[6],and the“differentiated”view[7].Although these debates persist,the continuous promulgation of laws and policies has largely removed the doubt over treating data as a new type of property,and data enterprises are recognized as having the right to dispose of data they have lawfully collected,for example by transferring it to other private-law subjects or granting them licenses for use[8].Notwithstanding the fact that the Personal Information Protection Law of the People’s Republic of China(hereinafter the Personal Information Protection Law)came into effect in 2021,issues concerning data assets in the field of bankruptcy law have received limited attention in Chinese theoretical and practical circles,and studies specifically addressing personal information are even more scarce[9].

In traditional bankruptcy proceedings,the bankruptcy estate predominantly consists of tangible assets or more conventional property rights,the scope and criteria of which are relatively well established in both legal doctrine and judicial practice.However,with the rapid development of the digital economy,data has become a critical resource for corporate operations,and,in particular,the personal information held by enterprises is increasingly emerging as a core element of their competitive advantage.As a novel type of asset,personal information exhibits legal characteristics that differ fundamentally from those of traditional tangible property.This particularity lies not only in its close linkage with data assets,but also in its dual legal nature,combining both personality attributes and proprietary attributes.

Article 22 of the Personal Information Protection Law and the Administrative Measures for Personal Information Protection Compliance Audits,promulgated on 12 February 2025(hereinafter the Administrative Measures),both address the manner in which personal information handlers,namely bankrupt enterprises,may process personal information in the context of bankruptcy.Nevertheless,the traditional legal framework is inadequate to respond to the legal challenges posed by data—particularly personal information—as a novel type of asset.Classical property law theories are premised on core concepts such as physical possession,exclusivity,and exclusive control,whereas corporate data assets are marked by their immateriality and by the wide sharing and fluid circulation of data,which fundamentally differentiates them from traditional forms of property and corresponding modes of legal protection[7].The approach adopted in the Personal Information Protection Law also gives rise to new issues;for example,the provision that allows the transfer of personal information upon mere fulfillment of the duty of notification,without requiring user consent,raises the question of whether it contravenes the principle of consent as a fundamental principle of personal information protection.Consequently,although the Civil Code of the People’s Republic of China(hereinafter the Civil Code),the Personal Information Protection Law,and the Administrative Measures set forth certain general rules that bankrupt enterprises,in their capacity as personal information handlers,should observe when processing personal information,these instruments lack more detailed and specific provisions and do not clearly define or differentiate categories of personal information.

In addition,under the Enterprise Bankruptcy Law of the People’s Republic of China(hereinafter the Enterprise Bankruptcy Law),the bankruptcy administrator bears the statutory duties of managing and disposing of the debtor’s property.However,when dealing with corporate data and personal information,the legal basis for the administrator’s authority and the scope of his or her responsibilities remain unspecified in the relevant legislation,and existing research on these issues is extremely limited.It is therefore necessary to clarify



the legal nature of personal information, to examine whether corporate data assets—especially personal information—should be included in the bankruptcy estate, and, on this basis and from the perspective of the bankruptcy administrator, to construct differentiated rules for handling various categories of personal information while balancing the interests of all stakeholders.

2 The Nature and Classification of Personal Information in Bankruptcy Proceedings

2.1 *The Dual Attributes of Personal Information*

Personal information, as a special type of informational resource, inherently combines both personality attributes and proprietary attributes. The duality of these attributes means that its treatment in bankruptcy proceedings cannot be approached in a uniform manner. When disposing of personal information, it is necessary not only to recognize its economic value, but also to strictly comply with relevant laws and regulations so as to safeguard the personality rights of the data subject. Only by achieving an effective balance between these two attributes at the level of legal rules and practical operation can the overall interests of all parties involved in bankruptcy proceedings be maximized.

2.1.1 *Personality Attributes*

Personal data possesses both personality attributes and proprietary attributes, yet its personality attributes should be given priority [11]. Although the proprietary dimension of personal information has long been evident, its most important attribute remains its function as a personality right. Personality attributes emphasize the uniqueness and irreplaceability of personal information; it is not merely a simple aggregation of numbers and characters, but rather relates to multiple dimensions of an individual's existence. Accordingly, the design of rules governing the processing of personal information should be grounded primarily in considerations of its personality attributes [12].

From the perspective of personality attributes, personal information is not only an important vehicle for the expression of individual identity, the right to privacy, and personal dignity, but also directly implicates the fundamental rights of the data subject. Article 109 of the Civil Code of the People's Republic of China expressly provides that the personal dignity of a natural person shall be protected by law, and this principle provides a solid legal basis for the personality attributes of personal information. Personal information naturally reflects the personality attributes of natural persons [13]. Personality attributes highlight the internal characteristics and social relationships of the individual as revealed through information; its uniqueness and non-substitutability mean that it must never be simply equated with ordinary property assets under any circumstances. At the same time, the Personal Information Protection Law requires that the processing of personal information comply with the principles of legality, propriety, and necessity, and that the data subject's right to be informed and right of decision be respected. Therefore, in bankruptcy proceedings, any treatment of personal information purely as an economic object may seriously infringe upon the rights of the data subject. Moreover, although personal information is often processed for the purpose of obtaining economic

benefits, personality interests rank higher than property interests in the hierarchy of civil rights and interests; when the two come into conflict, personality interests should be accorded priority[14].

2.1.2 Proprietary Attributes

On the other hand, with the development of the digital economy and big data technologies, the economic value of personal information has become increasingly prominent, and its use in commercial activities has become an important means by which enterprises generate profits. Personal information, while bearing personality attributes, also inherently contains a “gene” of proprietary value and exhibits characteristics such as utility, scarcity, controllability, and tradability[15]. In bankruptcy proceedings, the maximization of the debtor’s estate, under the premise of satisfying the interests of all stakeholders to the greatest extent possible, is a core objective[16]. Achieving this objective requires that the property owned by the debtor be converted into bankruptcy assets to the greatest possible extent.

Personal information has proprietary attributes. The property right in personal information refers to the right of the individual to control the commercial use value embedded in his or her personal information, as distinct from personality interests; such a right can and does exist only within an environment of commercial exploitation of personal information[17]. In practice, users typically provide their information to enterprises or personal information controllers on the basis of certain agreements in order to obtain goods or services, and data controllers transform such personal information into data assets with proprietary attributes through processing. Articles 41 to 45 of the Cybersecurity Law of the People’s Republic of China (hereinafter the Cybersecurity Law) place particular emphasis on the protective measures that network operators must adopt with respect to personal information. On the premise of legality and compliance, enterprises may create significant economic benefits by integrating, analyzing, and utilizing personal information. This, at the operational level, reflects the proprietary attributes of personal information and its economic value.

An analysis and comparison of the personality attributes and proprietary attributes of personal information reveals that the two are not mutually exclusive, but rather interwoven and mutually reinforcing. In bankruptcy proceedings, whether it is the debtor-enterprise or the administrator disposing of the enterprise’s assets, there is, on the one hand, a need to take into account the economic value of personal information and to treat it as an asset capable of realization for the purposes of valuation and disposition; on the other hand, there is an obligation to prevent any infringement of the lawful rights and interests of data subjects in the course of asset disposition. In protecting the interests of creditors, equal emphasis must be placed on respecting and safeguarding the personal dignity of the data subjects.

2.2 Classification and Legal Definition of Personal Information

In the digital economy era, personal information, as an important component of corporate data assets, raises classification issues that are directly relevant to how bankruptcy proceedings can balance the protection of the fundamental rights of data subjects with the goal of maximizing creditor recovery. In bankruptcy proceedings, the classified protection of personal information is not only necessary for implementing the requirements laid down in the Personal Information Protection Law and the Cybersecurity Law, but also a crucial precondition for reconciling the basic rights of data subjects with the property interests of creditors.



Given that the relationship between personal information and personal privacy involves overlap and intersection[18],scholars have expressed divergent views on this issue[19].This article will therefore not engage in a detailed discussion of the similarities and differences between sensitive personal information and personal privacy.Instead,it will,based on the degree of sensitivity,roughly divide personal information into“general personal information”and“sensitive personal information”[20],and explore the practical significance and legal value of this categorization.

2.2.1 General Personal Information

General personal information primarily refers to information widely collected in the course of routine business activities that is related to individual identity but does not involve highly private or sensitive content,such as name,gender,date of birth,contact information,and address.Because such information is ubiquitous in commercial activities,its collection,processing,and transmission have become relatively mature,and it has,to a certain extent,already received the initial authorization of the data subject.Moreover,Article 22 of the Personal Information Protection Law provides that where a personal information handler needs to transfer personal information due to reasons such as bankruptcy,and the receiving party does not change the original purpose and method of processing,the personal information handler only needs to fulfill the duty of notification to users.Accordingly,in bankruptcy proceedings,when an enterprise disposes of general personal information as part of its data assets,the associated legal risks are relatively low.As long as the administrator ensures data security and that the fundamental rights and interests of data subjects are not infringed,such information may be more flexibly included within the scope of the bankruptcy estate for purposes of valuation and transfer.

Although general personal information enjoys relatively more relaxed conditions of disposition under the law,its potential privacy risks should not be overlooked.Compared with sensitive personal information,the direct harm caused by the leakage or misuse of general information may appear smaller.Yet in the information age,even the abuse of basic personal information can trigger secondary risks such as identity theft and harassment.Therefore,in evaluating and disposing of such information,the bankruptcy administrator must strictly comply with the Personal Information Protection Law,the Cybersecurity Law,the Administrative Measures for Personal Information Protection Compliance Audits,and other relevant norms,so as to prevent the rights and interests of data subjects from being compromised due to data circulation.

2.2.2 Sensitive Personal Information

In China,the concept of sensitive personal information first appeared in the Personal Information Protection Law[21].The Information Security Technology—Personal Information Security Specification(GB/T 35273–2020)(hereinafter the Personal Information Security Specification)further clarifies the concept and criteria for determining sensitive personal information and,in its annex,provides examples of sensitive information,including personal financial information,personal health and physiological information,personal biometric information,and personal identification information,among others.Of course,information not explicitly listed is not automatically categorized as general personal information;rather,a comprehensive assessment is required in specific contexts,taking into account the identity of the user,the purpose and meth-

od of use, and the potential privacy risks, with appropriate adjustments made in light of changes to the data subject, the data user, and the usage environment[22]. Compared with general information, sensitive personal information entails higher privacy risks and is subject to stricter legal protection. Section 2, Subsection 2 of Chapter II of the Personal Information Protection Law imposes more stringent safeguards for the processing of sensitive personal information, requiring handlers to obtain the separate, explicit consent of the data subject in advance and to clearly inform them of the purpose, method, and potential risks of processing. From the perspective of legal attributes, sensitive personal information possesses pronounced privacy characteristics and special protective value. Because it directly concerns fundamental aspects of the user's physical, psychological, and social life, the leakage or abuse of such information often causes irreparable harm to the data subject and may even trigger a chain of consequences such as identity theft and credit risks. For these reasons, the State adopts higher standards for the legal protection of sensitive personal information.

In corporate bankruptcy proceedings, the disposition of sensitive personal information is particularly complex. On the one hand, sensitive information may have become an important data asset for achieving targeted marketing, risk control, and service optimization during the course of enterprise operations, and its economic value cannot be ignored. On the other hand, due to the stringent protection requirements for sensitive information, administrators must act with great caution when disposing of assets containing such information, so as to avoid infringing upon the privacy rights and personality rights of data subjects through improper handling[23]. Consequently, the treatment of sensitive personal information in bankruptcy proceedings must adhere to more rigorous standards. Personal information handlers or administrators, in processing such information, should take into account its inherently high-risk nature and adopt appropriate technical measures such as data desensitization and encryption to prevent misuse or leakage, thereby ensuring that the commercial value of data assets is realized while fully protecting the privacy and personal dignity of the data subjects.

2.2.3 Significance and Practical Application of Classification

In ordinary scenarios involving the transfer of personal information, both legal norms and national standards distinguish between general personal information and sensitive personal information[24]. Classifying personal information according to whether it is sensitive not only facilitates the accurate determination of the legal attributes of different types of data at the theoretical level, but also provides concrete operational guidance for bankruptcy administrators in implementing the disposition of data assets in practice. From the perspective of legal application, differentiating between general and sensitive information reflects the principle of differentiated protection in China's current data protection regime. When collecting personal information in the course of ordinary business activities, enterprises typically obtain authorization and provide notice within a certain scope, whereas the processing of sensitive personal information requires more stringent procedural safeguards.

In addition, the scientific classification of personal information contributes to risk prevention and allocation of liability. By clearly distinguishing between general and sensitive information, administrators can verify, prior to transfer, whether the data subject has granted lawful authorization, and can establish security protection mechanisms for each stage of data transmission, storage, and disposal, thereby effectively reducing the legal risks associated with information leakage.



From a broader perspective, the differentiation of personal information is not only an operational requirement for data disposition in bankruptcy proceedings, but also has far-reaching implications for the advancement of China's data governance and the improvement of its legal system. At present, China is in a process of continuous refinement in such areas as the disposition of data assets and information protection. The classification of personal information helps to clarify the legal attributes and protection requirements of different categories of data, thereby promoting the ongoing development of regulatory policies and judicial practice.

3 Legal Basis for Treating Personal Information as Bankruptcy Estate

3.1 Personal Information Should Be Included in the Bankruptcy Estate

3.1.1 Definition and Basic Characteristics of the Bankruptcy Estate

The Enterprise Bankruptcy Law of the People's Republic of China broadly defines the bankruptcy estate as the debtor's property. However, the provisions of the Enterprise Bankruptcy Law also implicitly contain further requirements and conditions regarding the constitution of the bankruptcy estate. First, the property must be capable of realization and distribution, that is, it must possess proprietary attributes and be convertible into proprietary interests. Second, it must conform to Article 30, namely that it is property belonging to the debtor at the time when the people's court accepts the bankruptcy petition and property obtained by the debtor after acceptance of the petition and before the conclusion of the bankruptcy proceedings.

Article 1 and Article 2 of the Several Provisions of the Supreme People's Court on Issues Concerning the Application of the Enterprise Bankruptcy Law of the People's Republic of China (II) (hereinafter the Judicial Interpretation (II) on the Bankruptcy Law) respectively define the scope of the bankruptcy estate from the affirmative and negative dimensions. From the affirmative perspective, the bankruptcy estate includes property or property rights and interests such as currency, tangible assets, claims, and equity interests. From the negative perspective, property that does not fall within the bankruptcy estate may be roughly categorized as property belonging to others but in the debtor's possession, property for which ownership has not yet passed to the debtor, and property that is exclusively owned by the State and is not transferable. In addition, Article 71 of the Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Enterprise Bankruptcy Cases (hereinafter the Provisions on Several Issues in Bankruptcy Cases) enumerates nine categories of property that do not belong to the bankruptcy estate.

Synthesizing the above statutory provisions, the bankruptcy estate can be summarized as having the characteristics of "proprietaryness," "disposability," and "realizability." The characteristic of "proprietaryness" requires that the property included in the bankruptcy estate be capable of being converted into economic benefits and, under the administrator's disposition, participate in the realization and distribution process in bankruptcy. The requirement of "proprietaryness" also inherently embodies the objective of maximizing the value of the bankruptcy estate, which can effectively alleviate conflicts among interested parties [25]. The characteristic of "disposability" requires that, once under the control of the bankruptcy administrator, enterprise property can lawfully be transferred or disposed of through mechanisms such as sale or auction. "Re-

alizability” is a combination and extension of the foregoing two characteristics and constitutes the ultimate objective: where enterprise property has economic value and can be disposed of, it can naturally be converted into monetary funds to satisfy creditors’ claims. These characteristics and elements form the basic theoretical framework for the bankruptcy estate and provide the conceptual foundation for determining whether data assets, including personal information, should be included in the bankruptcy estate.

3.1.2 Policy and Legal Support

The State’s emphasis on data assets has been fully reflected on multiple levels, and relevant policy and legal instruments collectively provide robust support for treating personal information as part of the bankruptcy estate.

The State’s attitude toward whether data possesses proprietary elements is embodied in the Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Basic Data System to Better Play the Role of Data as a Factor of Production, issued at the end of 2022 (hereinafter the “Twenty Data Measures”). The Twenty Data Measures not only clarify, at the macro level, the positioning of data as a fundamental factor of production and a new driving engine of the digital economy, but also explicitly propose the need to “establish and improve mechanisms for the circulation of proprietary rights and interests in data in accordance with statutory provisions or contractual agreements. Where a data handler undergoes merger, division, dissolution, or is declared bankrupt, relevant rights and obligations shall be transferred concurrently in accordance with laws and regulations.” These policies and provisions collectively demonstrate the State’s affirmative stance on recognizing data as a proprietary factor of production, while at the same time directly drawing attention to the need to address the disposition of enterprise data in bankruptcy scenarios.

This recognition is also reflected in the Civil Code. The legislature places “data” alongside “network virtual property” in the Civil Code [26], thereby acknowledging, to a certain extent, that data possesses proprietary attributes. Once personal information has been collected by an enterprise, it is transformed into enterprise data through integration, analysis, and big data algorithms; the enterprise then possesses and controls this data, and in the processes of use, sharing, and circulation, its proprietary value is further highlighted. In the course of business operations, enterprises conduct systematic management and commercial exploitation of personal information, turning it into an assessable and transferable proprietary resource. The Personal Information Protection Law likewise contains provisions addressing situations where personal information handlers need to transfer personal information for reasons such as bankruptcy [27]. These provisions not only emphasize the importance of protecting personal information in the context of corporate bankruptcy, but also indirectly confirm the possibility that personal information may be incorporated into the bankruptcy estate.

Accordingly, both State policy and statutory law support the view that personal information lawfully collected and commercially utilized by enterprises is subject to the same conditions of disposition as other assets, thus providing a sufficient legal basis for its inclusion in the bankruptcy estate.



3.1.3 Personal Information as Property

Through big data technologies, enterprises transform personal information—which originally merely reflected individual identity and privacy—into a resource that progressively releases its intrinsic economic value through processes of collection, integration, processing, and commercial exploitation, thereby acquiring proprietary characteristics analogous to those of traditional assets. This proprietary nature is evidenced not only by the economic benefits and market tradability of personal information, but more fundamentally by the transformation of its internal rights attributes, namely the “release” of “active” proprietary rights from “dormant” personality interests[28].

Enterprises typically obtain lawful disposal rights over personal information data by securing users’ consent to privacy policies, thereby legitimizing their use of such data and laying the legal groundwork for its subsequent transformation or disposition. The process of commercial exploitation of personal information is precisely a process in which its inherent proprietary attributes are separated from personality interests and endowed with the ability to circulate, be traded, and be monetized. By subjecting personal information to systematic management, enterprises process data into quantifiable and assessable commercial assets, whose economic benefits are fully manifested in targeted marketing, risk management, and the construction of user profiles. In order to maintain a competitive advantage, enterprises often seek a stable and exclusive position in the exploitation of personal information. Judges, for their part, increasingly treat enterprise data rights as assets and examine related disputes from the perspective of competition law[29].

All intangible assets are, in principle, susceptible to monetary valuation. Although the valuation of personal information may be challenging, this does not mean that such information cannot be appraised as part of the bankruptcy estate[30]. Common valuation methods include the market approach, income approach, and cost approach, among others, and valuation may also take into account specific characteristics of personal information, market conditions, social environment, and other factors[31]. Of course, not all personal information is suitable for inclusion in the bankruptcy estate. Generally speaking, it should possess characteristics such as economic value, tradability, and controllability. Certain information involving privacy rights—such as biometric data—as well as information that cannot circulate due to statutory provisions or ethical constraints, is not appropriate to be treated as bankruptcy estate.

From the perspective of “disposability,” enterprises typically obtain rights to the lawful use and commercial exploitation of personal information in the course of business operations on the basis of user agreements, privacy policies, and similar instruments. This means that enterprises are entitled not only to store and process user information, but also, under certain conditions, to transfer or otherwise dispose of such information. From the perspective of “realizability,” personal information, as a form of digital asset, is already traded within mature market structures and can realize its proprietary value through lawful transactions, transfers, or licensing. Therefore, whether viewed from the standpoint of relevant legal provisions, from the definition of the bankruptcy estate, or from the proprietary attributes of personal information itself, personal information meets the basic conditions for inclusion in the bankruptcy estate. In bankruptcy proceedings, commercially exploited personal information should be incorporated into the bankruptcy estate and, through scientifically sound valuation and disposition mechanisms, its asset value should be maximized.

3.2 Foreign Experience

3.2.1 Lessons from European and American Statutory Law

The United States is among the earliest countries to legislate for the protection of personal information privacy and has paid considerable attention to cases in which bankruptcy proceedings intersect with personal information and privacy interests. The Federal Trade Commission (FTC), as the government agency specifically tasked with protecting consumer rights, has gradually developed rules governing the transfer of personal data in bankruptcy through its enforcement actions in specific cases. In U.S. bankruptcy practice, when consumer personal information is to be sold, a privacy ombudsman must be appointed to prepare a special report regarding the legality of the proposed data sale[32].

To protect consumers, Section 363(b) of the U.S. Bankruptcy Code imposes restrictions on the sale of “personally identifiable information” when a debtor intends to sell personal data. These restrictions apply under the following preconditions: (1) at the time of collection, the debtor explicitly promised in its privacy policy that personal data would not be transferred upon the commencement of bankruptcy proceedings; and (2) the privacy policy remains in force at the time of bankruptcy[33]. Thus, when the debtor’s privacy policy at the time of the bankruptcy filing prohibits the sale of personal data, or when the policy fails to clearly disclose that the debtor may sell personal data, the debtor must satisfy one of the following two conditions in order to proceed with the data sale: (1) the sale is consistent with the privacy policy that remains effective at the time of the bankruptcy filing; or (2) a court-appointed consumer privacy ombudsman submits a report assessing the proposed sale, and if no evidence is found that the sale violates applicable non-bankruptcy law, the court will approve the transaction[34].

In addition, the U.S. Digital Consumer Rights Act clarifies consumers’ rights over their personal data, thereby strengthening the protection of consumer interests. California’s enactment of the California Consumer Privacy Act (CCPA) further reinforces data subjects’ control over personal data and provides more detailed safeguards for the clarification and protection of data-related rights.

In 2014, the Court of Justice of the European Union, in the Google Spain case[35], established the “right to be forgotten,” holding that individuals, under certain conditions, have the right to request websites to delete personal information about them. On 13 May 2014, the Court rendered its final judgment, finding that the defendant, as the operator of the Google search engine and thus an information controller, was obliged to delete search results concerning the data subject that were “inadequate, irrelevant, or no longer relevant,” thereby granting the plaintiff González’s request for deletion. This judgment constituted the first judicial interpretation and application of the right to be forgotten as provided in the 2012 draft of the General Data Protection Regulation (GDPR), thus rendering the right operational in practice and marking a major breakthrough in its development. In April 2016, the Council of the European Union and the European Parliament successively voted to adopt the GDPR[36], in which the right to be forgotten is prominently enshrined. Pursuant to Article 17 of the GDPR, users have the right to require enterprises to promptly erase their personal data where the data is no longer necessary for the purposes for which it was collected or processed, where consent has been withdrawn, or where the processing is unlawful. Moreover, when personal data has been made public, enter-



prises must take reasonable measures, including deleting relevant links and copies, to ensure effective erasure.

In some European countries such as Germany, a balance has been sought between safeguarding data rights and enabling the exploitation of data value. Requirements under EU law have been implemented through instruments such as the Treaty of Lisbon and amendments to the Telecommunications Act, while the legal regulation of data monopolies has been strengthened through the GDPR, the Anti-Unfair Competition Act, and other statutes that specify legal liability in cases of infringement[37].

A comparative analysis of U.S. and EU cases and policies concerning the treatment of personal data in bankruptcy indicates that, in the United States, the introduction of a privacy ombudsman into bankruptcy proceedings serves to ensure the legality and security of personal information transfer and focuses primarily on whether the administrator of a bankrupt enterprise may sell customer personal data. By contrast, the EU, through the GDPR and related regulations, clarifies the respective rights and obligations of data subjects and personal data controllers, with particular emphasis on the right of erasure (right to be forgotten), thereby providing a clear legal basis for the protection of personal information. Although these governance approaches are not identical, both attach considerable importance to the protection of personal information in the context of corporate bankruptcy, offering useful comparative insights and theoretical support for the treatment of personal information in Chinese bankruptcy proceedings.

3.2.2 U.S. Case Law Experience

In the United States, the sale of personal information in corporate bankruptcy proceedings is relatively common, and the legislative framework addressing data processing by bankrupt enterprises developed comparatively early. Section 363 of the U.S. Bankruptcy Code provides that, if a company's privacy policy clearly authorizes the sale of customer data, the company may sell such data. However, if the privacy policy does not authorize the sale of customer data, a consumer privacy ombudsman (CPO) must be appointed to review the proposed sale in light of applicable non-bankruptcy law[38]. As a common-law jurisdiction, the United States has gradually established rules governing the treatment of personal information in bankruptcy through specific cases. This article focuses on two classic cases, Toysmart and XY, and, by comparing their differing approaches to personal data in bankruptcy proceedings, seeks to draw lessons for the development of China's regulatory framework.

Toysmart was an online toy retailer that, in its privacy statement, promised not to share user information with third parties. In 2000, the company entered bankruptcy proceedings and ultimately sought to sell user data from its database. The FTC took the view that this conduct violated the Federal Trade Commission Act and therefore brought an action before the court. The parties eventually reached a settlement. Although Toysmart was ultimately permitted to sell user data, the sale was subject to several conditions, including: (1) user information could not be sold separately, but only as part of the enterprise's assets; (2) the purchaser had to be from the same industry and be approved by the court; and (3) the purchaser had to agree to abide by Toysmart's original privacy statement, and any material change thereto required prior notice to users[39]. In this case, the court effectively acknowledged the transfer and sale of personal data in bankruptcy proceed-

ings, and the settlement did not explicitly require users' consent for the sale of their data. The solution primarily aimed at maximizing the value of the bankruptcy estate and protecting creditors' interests, emphasizing the proprietary attributes of personal information while allowing the sale of personal data in bankruptcy subject to certain conditions.

The treatment of personal information in the XY case, by contrast, was entirely different. XY Magazine was a gay men's magazine whose website, XY.com, offered magazine content and online dating services. As in Toysmart, XY's privacy statement promised not to share users' personal information. However, in 2010, XY Magazine and XY.com filed for bankruptcy and sought to revive operations by selling or transferring user data. The FTC argued that continued use of the data would pose privacy risks to users[40], and the court ultimately ordered the destruction of all user data[41].

Both Toysmart and XY involved attempts by bankrupt enterprises to sell or transfer user personal data, yet the outcomes diverged sharply: Toysmart was permitted to sell personal data under certain conditions, while in XY the court ordered the destruction of the data. The fundamental reason for this divergence lies in the different types and sensitivity levels of personal information in the two cases. In XY, the data involved highly sensitive information, such as sexual orientation, making the user data significantly more sensitive than that in Toysmart. For relatively ordinary personal information, U.S. practice typically allows sale and transfer subject to additional conditions, whereas for sensitive information, a much stricter stance is adopted, prohibiting its sale and transfer. The differentiated treatment of different categories of information adopted in U.S. practice aligns with the approach advocated in this article and offers valuable guidance for developing rules on the treatment of personal information in Chinese bankruptcy proceedings.

4. Constructing Rules for the Disposal of Personal Information from the Perspective of the Bankruptcy Administrator

4.1 Legal Status and Duties of the Bankruptcy Administrator

4.1.1 Functions and Obligations of the Bankruptcy Administrator

Article 13 of the Enterprise Bankruptcy Law provides that, when a people's court issues a ruling accepting a bankruptcy petition, it shall appoint a bankruptcy administrator at the same time. The bankruptcy administrator plays a crucial role throughout the entire bankruptcy process. His or her duties run through all stages of the proceedings: the administrator must take over the debtor's property in its entirety and also bears the important responsibility of disposing of that property. Once the court declares the debtor bankrupt, the administrator is required to assume comprehensive control over the debtor's assets. On the premise that enterprise data assets qualify as part of the bankruptcy estate, the various data resources held by the debtor will naturally be incorporated into the bankruptcy estate.

As discussed above, personal information possesses both personality and proprietary attributes, with the former ranking higher in the hierarchy of legal interests than the latter. When examining the functions of the bankruptcy administrator, it is therefore appropriate to follow this analytical path: in disposing of the debtor's



personal information, the administrator should adhere to a certain order of priority. The administrator must first assume obligations of security and confidentiality with respect to personal information; this constitutes a baseline obligation once the administrator, by taking over the debtor's property, becomes the handler and manager of the relevant data. Only after giving priority to the protection of the personality attributes of personal information should the administrator shift perspective to its proprietary dimension. As an extension of the duty of loyalty and due diligence, another core obligation of the administrator is to maximize the value of the bankruptcy estate. Bankruptcy is not an ordinary scenario; where the exercise of rights by individual users may impose substantial burdens on the value of the bankruptcy estate, the administrator may appropriately tilt the balance slightly toward the proprietary attributes of personal information, and, without breaching the baseline obligation of security and confidentiality, seek to maximize the economic value of personal information as a data asset[42].

This requirement also resonates with Article 22 of the Personal Information Protection Law, which provides that, where a personal information handler needs to transfer personal information for reasons such as being declared bankrupt, and the recipient does not change the original purpose and method of processing, the handler need only fulfill the duty of notification to users. The requirement that "the recipient does not change the original purpose and method of processing" serves to protect the personality attributes of personal information. Such a mode of handling, while respecting the personality dimension, is at the same time the optimal means of realizing the proprietary value of personal information as a data asset.

4.1.2 Normative Basis for the Administrator's Performance of Duties

Because the Enterprise Bankruptcy Law does not set out in detail the rights, obligations, and responsibilities of the administrator when dealing with personal information and other data assets, it is appropriate to begin the analysis from the duty of loyalty and due diligence stipulated in Article 27. The administrator's obligations of security and confidentiality should be grounded in this duty of loyalty and due diligence. One commonly held view is to draw on the provisions of the Company Law of the People's Republic of China concerning directors, supervisors, and senior management, and to interpret this duty as a "duty of care of a prudent manager." At the same time, other scholars further refine it, arguing that the administrator should possess the capability necessary to discharge the role, conscientiously perform his or her duties, and be able to foresee adverse consequences in a timely manner and take corresponding measures[43].

On this basis, the administrator's obligation of security and confidentiality may be understood as requiring the administrator to exercise due care in supervising the debtor's maintenance of necessary data-processing operations and in properly managing the enterprise's data, so as to prevent security incidents—such as data breaches or damage—that could impair its economic value. Furthermore, the administrator's obligation of security and confidentiality is grounded in the nature of his or her functions. As noted above, the administrator bears responsibilities for taking over and disposing of the debtor's property. These responsibilities implicitly include a further requirement: the administrator must ensure that the debtor's assets do not suffer manifest diminution. For data such as personal information, the best way to avoid a diminution in value is to strictly fulfill obligations of security and confidentiality, thereby preventing data breaches and similar incidents[44].

In sum, while bankruptcy administrators enjoy broad managerial powers under the Enterprise Bankruptcy Law, particular attention must be paid, in disposing of personal information assets, to striking an appropriate balance between protecting creditors' interests and safeguarding the rights of data subjects. The Personal Information Protection Law imposes relatively stringent requirements on the handling of personal information. The administrator should, without contravening these requirements, evaluate personal information, classify and dispose of it accordingly, conduct compliance reviews, and constantly adhere to the baseline obligations of security and confidentiality, so as to ensure the lawful circulation of personal information. On the premise of not infringing the rights and interests of data subjects, the administrator should protect creditors' legitimate interests and seek to maximize the value of the bankruptcy estate, thereby providing a workable legal pathway for the governance of personal information assets in bankruptcy proceedings.

4.2 Processing of Personal Information

4.2.1 Classified Disposal of Personal Information

When disposing of personal information as a form of data asset, the administrator should adopt differentiated treatment based on the varying importance and sensitivity of the information concerned. Personal information embodies both personality and proprietary attributes. In other words, it is not only associated with economic value, but also closely tied to the privacy and security of the data subject. Accordingly, finding an appropriate balance between maximizing the value of the bankruptcy estate and protecting personal information becomes a key issue in the administrator's performance of duties.

Pursuant to the Personal Information Protection Law, the Cybersecurity Law, and related statutes and regulations, the processing of personal information must comply with the principles of lawfulness, propriety, and necessity, and differentiated protective measures must be taken for different categories of information. As discussed above, this article divides personal information into "general personal information" and "sensitive personal information." In bankruptcy proceedings, the administrator should therefore treat these two categories differently in accordance with their degree of sensitivity and formulate distinct evaluation, management, and disposal measures for each.

With respect to general personal information, Article 22 of the Personal Information Protection Law, in the author's view, provides clear operational guidance. When enterprises obtain the personal information of users, they typically have already secured an initial authorization, and both the scope of this authorization and the methods of information collection have become routine in commercial practice. Because general personal information entails relatively low legal risk, the administrator may, in disposing of it, act by analogy to Article 22: provided that the transferee does not change the original purpose and method of processing, the administrator need only fulfill a duty of notification to the data subject.

By contrast, the legal protection of sensitive personal information is far more stringent. In dealing with sensitive personal information, the administrator should strictly comply with Article 29 of the Personal Information Protection Law by obtaining the separate, explicit consent of the data subject, and, pursuant to Article 55, conduct a prior personal information protection impact assessment and record the relevant processing activities. In practice, a more meticulous evaluation of the sensitive information held by the debtor is



required, distinguishing between sensitive information that has economic value and that which, due to high privacy risks, should be subject to strict restrictions on circulation. Sensitive information that lacks economic value or has been collected without proper authorization should be deleted as a priority or anonymized and converted into general personal information or ordinary enterprise data, so as to avoid unnecessary legal risks.

For the disposal of sensitive personal information, the author suggests drawing on the “three-tier authorization principle” [45], namely the principle of “user consent+platform consent+user consent.” The final layer of “user consent” naturally aligns with Article 29 of the Personal Information Protection Law. Some scholars argue that discussing privacy interests in abstraction from specific scenarios and applications, and imposing the “consent rule” in a mechanical manner, does not necessarily reflect reality [46]. Nevertheless, for sensitive information, greater attention should be paid to personality interests and to the protection of the user’s right to informed consent, and more stringent security safeguards should be adopted.

4.2.2 Secure Disposal and Compliant Transfer of Personal Information

The dual attributes of personal information determine that, in bankruptcy proceedings, its disposal must address not only the protection of the data subject’s right to privacy, but also the realization of creditors’ interests through the maximization of the value of the bankruptcy estate. When dealing with personal information as an asset, the administrator should seek a balance between asset realization and legal compliance, strictly fulfilling his or her duties in the contexts of transfer, licensing, and review of personal information, and adhering to statutory requirements so as to prevent risks such as misuse of information or data breaches.

Secure and compliant processing must be the precondition for the administrator’s handling of personal information in bankruptcy. Data desensitization, as an important technique for reducing the sensitivity of personal information, can serve as a core method for protecting the privacy of data subjects. Data desensitization refers to a set of techniques that, while preserving the original structure and attribute characteristics of data, transform sensitive information involving personal privacy according to defined sensitivity rules, thereby reliably protecting such data [47]. When dealing with sensitive personal information or personal information that is identifiable to a certain degree, the administrator may choose different desensitization methods according to the type and sensitivity of the data, ensuring adequate protection of personal information and, on this basis, further leveraging its proprietary value [48].

As discussed above, different categories of personal information require different methods of processing. Accordingly, the administrator should, when dealing with different types of personal information, comply with the corresponding legal requirements, scientifically evaluate the economic value and legal risk of the information assets, and formulate compliant strategies for asset disposal. Of course, the administrator must consistently adhere to the principles of lawfulness and propriety, ensuring the security and legality of information disposal.

For general personal information, the bankruptcy administrator should first conduct a rigorous assessment of its market value and, in light of the overall data assets of the bankrupt enterprise, determine the optimal

method of realization. Even though the privacy risk associated with general personal information is relatively low, the administrator must still pay particular attention to issues of privacy and security, ensure that data storage is compliant, and strictly examine the qualifications of potential transferees to prevent misuse. During the circulation of information assets, the administrator should dynamically assess market conditions and legal compliance requirements and adjust the disposal plan for general personal information in a timely manner to ensure that asset disposal remains reasonable and lawful.

For sensitive personal information, particular care must be taken to ensure that the lawful rights and interests of data subjects are not infringed. The “three-tier authorization principle” discussed above may be applied, with more stringent measures for informed consent.

4.3 Pathways for Improving Rules on the Administrator’s Disposal of Information in China

Because personal information possesses both personality and proprietary attributes, its proper treatment in bankruptcy proceedings concerns not only the data subject’s right to privacy but also the interests of creditors. As a central actor in bankruptcy proceedings, the bankruptcy administrator plays a pivotal role in the disposal of personal information.

First, the administrator’s obligations concerning data compliance should be clearly specified, so as to ensure that the disposal of personal information complies with the Enterprise Bankruptcy Law, the Personal Information Protection Law, the Data Security Law, and other relevant statutes and regulations. At the same time, the administrator’s duty of loyalty and due diligence should be strengthened, and mechanisms for holding administrators accountable should be established. Where information leakage results from negligent or unlawful disposal of personal information by the administrator, the relevant parties should bear administrative, civil, and, where appropriate, criminal liability. This will enhance administrators’ awareness of compliance and further safeguard the information rights and interests of users.

Second, the administrator’s role in the valuation of information assets should be optimized by establishing a dedicated data asset valuation system and clarifying the administrator’s responsibilities and powers in the disposal of information assets. In view of the substantial uncertainty inherent in the valuation of data assets and the lack of clear transactional rules, the administrator should play a leading role in the bankruptcy process by promoting the formulation of sound valuation standards, ensuring that the market value of data assets is accurately reflected, and facilitating their lawful and compliant circulation. In addition, exploration may be made of a unified national data asset trading platform, which would, through market-based mechanisms, promote the lawful circulation of personal information. In the course of such transactions, the administrator should ensure that the transferee possesses lawful data-processing qualifications and require the transferee to continue fulfilling data protection obligations after receiving the data, thereby reducing the risks of misuse and leakage.

Finally, the classification-based protection of personal information in bankruptcy proceedings should be strengthened. The prerequisite for classification-based protection is a sufficiently clear categorization of personal information. In determining whether personal information is sensitive, not only should the standards



in the Personal Information Security Specification be taken into account, but a comprehensive assessment should also be made, in specific processing contexts, of all elements surrounding the processing conduct—such as the identity of the data subject, the purpose of processing, the location of processing, and the consequences of such processing[49]. In concrete situations, sensitive personal information should be evaluated comprehensively in light of the data subject's identity, the purposes and methods of use, and the potential privacy risks[50].

In terms of the treatment of general personal information and sensitive personal information, reference may be made to the approaches adopted in the Toysmart and XY cases. For general personal information, the administrator and the debtor may be allowed to dispose of it subject to certain conditions, in a manner that naturally aligns with Article 22 of the Personal Information Protection Law. For sensitive personal information, the practice in XY may provide a useful model, whereby courts directly determine how such information is to be handled. Alternatively, in accordance with Article 29 of the Personal Information Protection Law, separate consent from data subjects may be obtained, thereby reinforcing the protection of users' personality interests.

References

- [1] Viktor Mayer-Schönberger, Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*[M]. Trans. Sheng Yangyan, Zhou Tao. Hangzhou: Zhejiang People's Publishing House, 2013:20.
- [2] See Civil Ruling of Guangzhou Intermediate People's Court, (2018) Yue 01 Po No.12-1.
- [3] The Paper. "The First Bike-Sharing Bankruptcy Case: Liabilities of 55.4 Million Yuan, How to Refund 23.63 Million Yuan of Deposits"[EB/OL]. (2018-07-13). [2024-03-07]. [https://www.thepaper.cn/newsDetail_forward_2261704] (https://www.thepaper.cn/newsDetail_forward_2261704)
- [4] See China Appraisal Society. Expert Guidance on Asset Appraisal No.9—Data Asset Appraisal[EB/OL]. (2020-01-09)[2024-03-12]. [<https://www.cas.org.cn/docs/2020-01/20200109165641186518.pdf>] (<https://www.cas.org.cn/docs/2020-01/20200109165641186518.pdf>)
- [5] See Xu Ke. "Data Ownership: A Dual Perspective of Economics and Law"[J]. *Electronic Intellectual Property*, 2018(11):23–30; see also Zheng Jianing. "Constructing a Private Law Regulation System for Data Property in the Digital Economy Era"[J]. *Academic Research*, 2021(6):70–79.
- [6] See Mei Xiaying. "The Legal Nature of Data and Its Position in Civil Law"[J]. *Social Sciences in China*, 2016(9):164–183.
- [7] See Yang Lixin, Chen Xiaojian. "Derivative Data as the Object of Data Exclusive Rights"[N]. *Chinese Social Sciences Today*, 2016-7-13(005); see also Li Xiaoshan. "Definition and Legal Protection of Data Products"[J]. *Law Forum*, 2022(3):122–131.
- [8] Cheng Xiao. "On Personal Data Rights in the Era of Big Data"[J]. *Social Sciences in China*, 2018(3):102–122+207–208.
- [9] See He Dan. "Internet Economic Development and the Trend of Reform in Bankruptcy Law"[J]. *Law Magazine*, 2016, 37(02):79–85.
- [10] See Liu Bing. "On the Initial Acquisition, Circulation and Protection of Property Rights in Enter-

prise Data Assets”[J].Journal of Shanghai University of Political Science and Law(Rule of Law Review),2024,39(04):70–86.

[11]See Wang Liming.Civil Law(6th ed.)[M].Beijing:Law Press,2020:167.

[12]See Peng Chengxin,Wang Ranjan.“A Study on the Reasonable Scope of the Rules Governing the Use of Voluntarily Disclosed Personal Information”[J].Journal of Xiamen University(Arts&Social Sciences),2023(03):113–125.

[13]Peng Chengxin.“On the Dual Legal Attributes of Personal Information”[J].Tsinghua Law Journal,2021,15(06):78–97.

[14]See Wang Liming.“On the Hierarchy of Civil Rights and Interests:Centered on the Civil Code”[J].Chinese Journal of Law,2022(01):32–54.

[15]See Peng Chengxin.“Cognitive Transformation and Rule-of-Law Foundations in the Digital Society:Centered on Personal Information Protection”[J].Exploration and Free Views,2022(05):116–125+179.

[16]See Xu Defeng.“Rethinking the Basic Principles of Bankruptcy Law”[J].Law Science,2009(08):49–59.

[17]See Liu Deliang.“Protection of Property Rights in Personal Information”[J].Chinese Journal of Law,2007(3):91.

[18]See Zhang Xinbao.“From Privacy to Personal Information:Rebalancing Interests in Theory and Institutional Design”[J].Chinese Journal of Law,2015(03):38–59;see also Wang Liming.“On the Status of the Right to Personal Information in the Law of Personality Rights”[J].Journal of Soochow University(Philosophy&Social Science Edition),2012,33(06):68–75+199–200.

[19]Liu Jinrui.Personal Information and the Allocation of Rights:Reflections on and Prospects for the Right to Informational Self-Determination[M].Beijing:Law Press,2017:166.

[20]See Hu Wentao.“A Proposal for Defining Sensitive Personal Information in China”[J].Chinese Journal of Law,2018(05):235–254.

[21]Article 28(1)of the Personal Information Protection Law provides that sensitive personal information is personal information which,once leaked or illegally used,is likely to result in the infringement of a natural person’s dignity or harm to his or her personal or property safety.It includes information such as biometric data,religious beliefs,specific identities,medical and health information,financial accounts,and location tracking,as well as personal information of minors under the age of fourteen.

[22]Hu Chaoyang.“Legal Regulation of Personal Information Processing Conduct in the Context of Big Data—From the Perspective of the Dual Externalities of Personal Information Processing”[J].Journal of Chongqing University(Social Science Edition),2020,26(1):131–145.

[23]See Guo Dongyang.“A Study on the Consent Rule for the Transfer of Personal Information from the Perspective of Bankruptcy Law”[J].Journal of Northeastern University(Social Science Edition),2020,22(05):90–97.

[24]Chen Qiqian.“A Study on the Rules Governing the Transfer of Personal Data from the Perspective of Bankruptcy Law”[C].Shanghai Law Studies,Proceedings of the Data Compliance and Circulation Forum,2022(20):211–218.

[25]See Chen Kelin.“The Legal Status of Bankruptcy Administrators from the Perspective of Fiduciary Relationships”[J].Politics and Law,2023(11):160–176.

[26]Article 127 of the Civil Code provides that,where the law contains provisions on the protection of data



and network virtual property, such provisions shall be followed.

[27]Article 22 of the Personal Information Protection Law provides that, where a personal information handler needs to transfer personal information due to merger, division, dissolution, being declared bankrupt, or other reasons, it shall inform the individual of the name or personal name and contact details of the recipient. The recipient shall continue to perform the obligations of the personal information handler. Where the recipient changes the original purpose or method of processing, it shall obtain the individual's consent again in accordance with this Law.

[28]See Xiang Qin, Gao Fuping. "On the Property Attributes of Rights in Personal Information" [J]. Nanjing Social Sciences, 2022(02): 92–101.

[29]Xu Wei. "Rethinking and Typological Construction of the 'Three-Tier Authorization Principle' for Enterprise Data Acquisition" [J]. Shanghai Jiao Tong University Law Review, 2019(04): 20–39.

[30]Zhao Xiaomeng. "Disposal of Personal Data Assets in Enterprise Bankruptcy Proceedings" [J]. South Finance, 2024(09): 89–99.

[31]Liu Yaqi, Zhang Mengdan. "A Review of Domestic and Foreign Research on the Valuation of Personal Information" [J]. Information Science, 2020, 38(09): 157–165+173.

[32]See Christopher G. Bradley. "Privacy for Sale: The Law of Transactions in Consumers' Private Data" [J]. Yale Journal on Regulation, 40: 127 (2023).

[33]See Orin S. Kerr. "Norms of Computer Trespass" [J]. Columbia Law Review, 116: 1143, 1163 (2016).

[34]See Michael St. Patrick Baxter. "The Sale of Personally Identifiable Information in Bankruptcy" [J]. American Bankruptcy Institute Law Review, 27: 1, 2 (2019).

[35]The Google Spain case (C-131/12) was decided by the Court of Justice of the European Union in 2014 and established the "right to be forgotten." The case arose when Spanish citizen Mario Costeja González requested that Google delete outdated search results concerning his financial problems. The Court held that the operator of the Google search engine was a data controller and, in certain circumstances, must delete search results relating to an individual in order to protect privacy rights while balancing the public's right to know. The judgment promoted the codification of the "right to be forgotten" in the EU General Data Protection Regulation (GDPR) and has had a far-reaching impact on global data protection rules.

[36]In December 2016, the European Parliament and the Council reached agreement on the EU General Data Protection Regulation (GDPR), which had first been proposed in 2012.

[37]UWG. Anti Unfair Competition Act [EB/OL]. (2018-02-27) [2025-3-20]. [<https://www.lexetius.com/leges/UWG/Inhalt?1>] (<https://www.lexetius.com/leges/UWG/Inhalt?1>)

[38]Section 363(b) of the U.S. Bankruptcy Code provides: (1) After notice and a hearing, the trustee may use, sell, or lease property of the estate, other than in the ordinary course of business. However, if the debtor, in providing a product or service, has disclosed to an individual a policy prohibiting the transfer of personally identifiable information to persons unaffiliated with the debtor, and if that policy remains in effect on the petition date, then the trustee may not sell or lease such personally identifiable information to any person unless: (A) the sale or lease is consistent with that privacy policy; or (B) after the appointment of a consumer privacy ombudsman under section 332 and after notice and a hearing, the court approves the sale or lease, having (i) given due consideration to the facts, circumstances, and conditions of such sale or lease, and (ii) found that there is no showing that the sale or lease would violate applicable non-bankruptcy law.

- [39]See“FTC Announces Settlement With Bankrupt Website,Toysmart.com,Regarding Alleged Privacy Policy Violations”[EB/OL].<https://www.ftc.gov/news-events/news/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding-alleged-privacy-policy-violations>
- [40]Letter to XY Magazine and XY.com Regarding the Use,Sale,or Transfer of Personal Information Obtained During Bankruptcy Proceeding[EB/OL].[https://www.ftc.gov/system/files/documents/closing_letters/letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf](https://www.ftc.gov/system/files/documents/closing_letters/letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf)
- [41]See Daniel Brian Tan.“Maximizing the Value of Privacy through Judicial Discretion”[J].Emory Bankruptcy Developments Journal,34:681(2018).
- [42]Zhao Xiaomeng.“Disposal of Personal Data Assets in Enterprise Bankruptcy Proceedings”[J].South Finance,2024(09):89–99.
- [43]See Sun Chuangqian.Practical Operation of Bankruptcy Administrators[M].Beijing:Law Press,2018:17–22.
- [44]See Zhao Jingwu.“On the Treatment of Enterprise Data Assets in Bankruptcy Proceedings”[J].Chinese Journal of Law,2024(03):103–123.
- [45]Unfair Competition Dispute between Beijing Taoyou Tianxia Technology Co.,Ltd.et al.and Beijing Weimeng Chuangke Network Technology Co.,Ltd.,Civil Judgment of Beijing Intellectual Property Court,(2016)Jing 73 Min Zhong No.588.
- [46]See Gao Fuping.Research on Personal Information Protection Legislation[M].Beijing:Guangming Daily Press,2021:51.
- [47]See Xu Shuang,Liu Wenbin,Li Jialong,et al.“Research Progress on Data Security Governance in the Context of Big Data”[J].Journal of Taiyuan University of Technology,2024,55(01):127–141.
- [48]See Li W.,Li C.“Research and Design of a Data Desensitization System”[J].Journal of Physics:Conference Series,2020,1.
- [49]See Wang Liming.“Basic Issues in the Protection of Sensitive Personal Information—Against the Background of the Interpretation of the Civil Code and the Personal Information Protection Law”[J].Contemporary Law Review,2022,36(01):3–14.
- [50]See Zhang Yong.“Integrated Public–Private Law Protection of Sensitive Personal Information”[J].Oriental Law,2022(01):66–78.

