International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 16, No. 2, 2024

Study on the Protection and Rational Utilization of Personal Information in the Digital Era

Mingzhu Zhu*

School of Law,Anhui University of Finance and Economics, Longzi Lake District, Bengbu, Anhui, 233000, China
* **Corresponding author**: Mingzhu Zhu (Email: jolyye@qq.com)

Abstract: Since the advent of the digital age, personal information has been collected and aggregated, evolving into a new type of asset through innovative data technologies, which has generated significant economic benefits in circulation. At the same time, the traditional approach to personal information protection, which primarily focuses on privacy, is no longer sufficient for the demands of the digital era and does not facilitate the realization of the social value of personal information. How can these interests be appropriately balanced in law, and how can the legitimate rights and interests of the relevant parties be protected? To address these issues, the Personal Information Protection Act was introduced. However, the implementation of this law still faces challenges related to conceptual definitions, self-determination, and the protection and utilization system. Therefore, this article will consider the Personal Information Protection Law and international legislative practices to clarify the legal attributes of personal information, define the concept, and outline the rights of the information subjects, as well as the duties, responsibilities, and liabilities of information processors. It aims to answer these questions from the perspective of integrating sectoral laws and safeguard mechanisms. The article also explores the balance between individual and societal interests, promoting the protection and rational use of personal information in the digital age.

Keywords: Digital Age; Personal Information; Rational Use; Coordinated Protection.

1. Introduction

In today's digital economy, the interaction of personal information has become an unavoidable norm in people's lives. Personal information is frequently transmitted in the vast world of the Internet. Many conveniences of life also benefit from the high-speed flow of information. When you take an online car, tap the screen and the vehicle will be in place instantly. when you receive a courier, accurate address and contact information ensures that the parcel will be delivered smoothly. the personalized service of shopping software accurately pushes out the desired products based on personal preferences and needs. However, while enjoying the conveniences of the digital age, personal information is also being leaked constantly. To address this issue, the Law of the People's Republic of China on the Protection of Personal Information (hereinafter referred to as the Personal Information Protection Law), the Law of the People's Republic of China on Cybersecurity (hereinafter referred to as the Cybersecurity Law), and the Law of the People's Republic of China on Data Security (hereinafter referred to as the Data Security Law), along with other closely related laws and regulations, have demonstrated a trend towards balanced development in legislation concerning the protection and utilization of personal information.

However, It should be acknowledged that there are still many challenges in the implementation of current personal information laws and regulations in China. For instance, the definition of personal information leaves much room for interpretation. The notification-consent principle, which is fundamental to personal information protection, often becomes a mere formality. The current framework for personal information protection is still based on the respective rights and obligations of individuals, personal information processors, and personal information protection authorities. However, there is a higher degree of creativity in the actual situation when focusing on the linkage and construction of sectoral law protection mechanisms.

In the era of digital proliferation, personal information holds significant value in circulation. For individuals, it is an undeniably powerful tool to enhance the convenience and happiness of their lives. The accurate and appropriate use of personal information can save time, make life more convenient and efficient, and increase the sense of well-being. For society, personal information is a key driver for the growth of the digital economy. Accurate market analysis and efficient resource allocation both rely on the rational use of personal information. The management of personal information is an essential requirement for national and socio-economic development. Therefore, it is crucial to comprehensively examine the major propositions of personal information protection. It is necessary to seek a balance between public and private laws to protect individual dignity, ensure rational use by licensed enterprises, and maintain effective state supervision. This balance is essential to ensure that the digital economy's progress is smooth and secure, leading to a win-win situation for individuals, society, and the state.

2. Balancing Strategy of the Current Law

2.1. Evolution of the Legal Attributes of Personal Information

In the era of the burgeoning digital economy, the conventional approach to safeguarding individual privacy and human dignity has increasingly shown inadequacies in meeting contemporary developmental demands. Western nations have developed a variety of models for personal information protection through extensive judicial experience. Germany, for instance, has consistently anchored its legal protection in the right to personality. The 1983 Census Case

saw the court rule that the free development of personality requires the safeguarding of citizens' personal information from unauthorized collection, storage, use, and transfer. This ruling established that any use of personal information beyond its initial purpose, whether initial or subsequent, necessitates the informed consent of the individual, thereby ensuring their right to self-determination in information disclosure. Conversely, the United States has adopted a market-oriented approach to personal information protection, reflecting its antiregulatory culture. Here, personal information can be freely bought and sold, with the purchaser acquiring ownership rights, including the ability to resell without the original subject's consent. The EU's General Data Protection Regulation (GDPR) begins with the objective of safeguarding individuals during personal data processing and ensuring the unhindered flow of personal data. The regulation's goal is to foster a union that is economically free, secure, and just, promoting economic and social advancement while upholding the dignity of individuals. Similarly, other nations have adapted their legal frameworks to the data age's demands for personal information. India's Digital Personal Data Protection Act, the Philippines' Data Privacy Act, South Africa's Personal Information Protection Act of 2013, and Japan's Personal Information Protection Act have all introduced provisions to balance individual interests with economic growth, reflecting a global trend towards reconciling personal rights with the evolving digital landscape.

Since the Cybersecurity Law and the Personal Information Protection Law were enacted in China, there's been a steady trend towards balancing interests in personal information protection. The legislature's efforts to balance the protection and utilization of personal information are evident. For instance, Article 4 of the Personal Information Protection Law defines personal information as “all kinds of information recorded electronically or by other means relating to an identified or identifiable natural person, excluding anonymized information.” This definition not only affirms the personal interest in information in terms of the right to personality but also clarifies that once personal information's identifiability is permanently destroyed during the flow of information, its interests are no longer affected. When identifiability is lost, the information ceases to be a private right, and processors gain corresponding freedom to process it with public attributes. This balance is also evident in Article 42(1) of the Cybersecurity Law, which states that “Network operators shall not disclose, tamper with, or destroy personal information collected by them, nor provide personal information to others without the consent of the person from whom it was collected, except for those that cannot identify a specific individual after processing and cannot be restored.” This provision not only safeguards personal information from misuse but also provides a legal framework for its reasonable use. Article 13(5) of the Personal Information Protection Law further delineates the rights of personal information processors when they engage in activities such as news reporting and public opinion monitoring in the public interest, highlighting the public aspect of personal information. As technology advances, the public attribute of personal information has become increasingly significant. Data, once reorganized and analyzed, serves as a foundation for building personal profiles, facilitating modern social life and contributing to a safe and equitable social order. For example, at high-speed railway stations or airports, personal bio-information is collected using face recognition technology for accurate identification and traveler safety. In road traffic, violations are captured by electronic monitoring equipment, which uses portrait collection technology to identify vehicle owners for legal penalties. Another example is the requirement for electric bicycle riders to wear safety helmets, with non-compliance resulting in administrative penalties like warnings or fines. In such cases, those investigated by traffic police for not wearing helmets may resist providing identity information, but facial recognition devices can swiftly identify offenders and enforce penalties accordingly. These phenomena illustrate that personal information encompasses a broad range of public interests, meeting the diverse needs of various stakeholders. The group attributes of personal information have been reinforced, building upon individual dependence and propelling the ongoing evolution of the information age.

In summary, under the background of the digital era, the role and value of personal information in social operation and management are undergoing profound adjustment and reshaping. Nevertheless, the private nature of personal information remains unshakeable. The economic and social value behind the public attributes can only be explored within reasonable limits, which is the right way to protect and rationally utilize personal information.

2.2. Definition of Personal Information under Legislative Interpretation

Article 4 of the Personal Information Protection Act clearly stipulates that “personal information is all kinds of information recorded electronically or by other means relating to an identified or identifiable natural person, excluding anonymized information.” Here, “identifiability” serves as the key premise for defining personal information and aligns with the definition model widely accepted internationally. The evolution of traditional personal information theory has seen a shift between the "association theory" and the "privacy theory." The "privacy theory" confines the scope of personal information to that which pertains to personal privacy, a definition that can be contentious in practice due to the subjective nature of what is considered private. For instance, opinions on what constitutes "privacy" vary widely. Some individuals may view names and telephone numbers as private, while others may not and willingly share such information to access online services. Even with property information, such as bank account numbers and passwords, attitudes and handling methods differ among individuals. Some are hesitant to link high-balance bank cards to online shopping apps, opting instead to use cards with smaller balances or cash for purchases to safeguard their funds. Conversely, others may willingly share their frequently-used bank card details with merchants for small discounts or incentives. This variability in privacy definitions leads to an arbitrary and non-standard approach for information processors to adopt a binary service model. In the era of big data, where "privacy" is often elusive, it is more scientifically sound to adopt the "association" definition, which considers all information linked to an individual as personal information.

As the data and information era progressed, the "association theory" was deemed too broad in defining the scope of personal information, posing challenges for modern society's needs. Consequently, the "identification theory" gained traction, marking a pivotal shift where personal

information protection was extracted from traditional privacy protection to form its own distinct system. This marked the first time personal information protection was separated from traditional privacy protection to establish its own framework. The Civil Code defines personal information as information recorded electronically or by other means that can be used to identify a specific natural person, either alone or in combination with other information. This definition aligns with the concept of "identified" and "recognizable" information, focusing on the "identification" aspect. By including information that has the potential to identify a specific individual within the personal information framework, the aim is to safeguard personality interests over property interests in information.

This paper posits that employing "identifiability" as the central feature of personal information does not adequately address the challenge of balancing its protection with its utilization. "Identifiable" generally denotes the ability to recognize personal identity information through technical means, either directly or indirectly. On the other hand, anonymized personal information that is not identifiable is free to circulate without restrictions. The concept of "identifiability" can be seen as a method to provide a layer of anonymity to personal information that is "not directly or indirectly identifiable" and yet can be de-anonymized amidst the rapid evolution of Big Data. Similarly, the concept of "anonymization" could be interpreted as a protective veil for personal information that is "not directly or indirectly identifiable" and susceptible to de-anonymization in the context of Big Data's accelerating transformation.

Firstly, we will discuss "anonymization," which legislatively is defined as the process that renders personal information incapable of identifying a specific natural person and irrecoverable. The initial consideration is whether information that cannot be identified after "anonymization" still qualifies as personal information in a legal context—a debatable question. Secondly, many scholars have abandoned the "anonymity assumption" theory, concluding from numerous "de-anonymization algorithm" and data modeling studies that truly "de-anonymized" personal information does not exist in reality. Big data's strength lies in its capacity to re-associate and reorganize information fragments through algorithms, creating precise and detailed individual profiles through repeated cross-use, thereby revealing the value of personal data. Lastly, stepping back, if we assume that information can be both "de-identified" and "anonymized," it's possible to anonymize the information using an algorithm not predicated on personal information. Assuming further that such information can be circulated in the data resource market without the consent of the information owner, one might question whether it retains any value and whether this formalistic pursuit aligns with the goal of harnessing the value of personal information. Additionally, academics have proposed a personal information classification management model, distinguishing between sensitive and non-sensitive information. Sensitive information warrants stringent protection strategies, while non-sensitive information is more readily circulated and utilized. However, for this emerging conceptual category, it's insufficient to focus solely on its definition and theoretical framework; the deeper issues in practical application scenarios must also be considered. Similar to the discussion on "privacy," the boundary between "sensitive information" and "non-sensitive information" may be blurred, varying by individual and lacking a definitive, universally accepted conclusion.

The discussion on the definition of personal information, drawing from current legal provisions and scholarly research, reveals that significant attempts have been made to balance the protection and utilization of personal information. Yet, operational and implementation challenges persist. Given that personal information pertains to an individual, the subject should possess a degree of autonomous control over their information during processing. Moreover, it is essential for the state to manage and safeguard this information within a framework of public supervision and regulation.

2.3. Individual Self-determination - application of the Inform-consent Principle

The notification-consent principle is a significant strategy that aligns with the digital age's evolution, offering a breakthrough in balancing the traditional information protection model. This principle empowers individuals with control over their personal information before it is collected, aggregated, mined, or utilized. It mandates a prior notification by information controllers and processors, ensuring that once individuals are informed and consent to the collection and processing of their data, processors may proceed with related activities. Widely adopted in global personal information protection legislation, this principle was first established as a fundamental guideline for personal information collection in the European law on personal information protection in 1970. China's Personal Information Protection Law also adopts the notification-consent principle as a means to achieve the protection and reasonable use of personal information. However, in practice, the notification-consent principle is sometimes used by information processors as a blanket "exemption" for all information collection and processing. There's a misconception that simply notifying users before collecting and processing their information provides immunity for arbitrary processing, regardless of the sensitivity of the data or the necessity and justification for its collection. While highly private information indeed requires robust protection under both privacy rights and personal information protection laws, some applications, such as games and ordering services, request access to more private personal information than necessary for their functions. For example, before entering a game, users may be prompted to "allow this APP to obtain your camera, cell phone number, geographic location," and other sensitive personal information. Similarly, many restaurants now use a QR code ordering system, requiring customers to scan a code and authorize their WeChat account to place an order. These permissions often seem unrelated to the actual service provided, raising questions about their necessity. Furthermore, privacy policies, which are meant to inform users, are often lengthy and complex. Studies suggest that users spend about 40 minutes a day skimming through privacy policies of various websites, with more time required for a thorough understanding. These policies, crafted by legal professionals, contain terminology and phrases that may be difficult for the average user to comprehend without legal expertise. As a result, most users opt for the quickest route, which is to agree to the privacy policy without fully understanding it, in order to access the application or service.

The fundamental purpose of establishing the "notification-consent" mechanism is to empower information subjects with the autonomy to decide how their information is handled and to uphold human dignity's supremacy when personal and

economic interests collide. However, some information processors, while seemingly fulfilling the "notification" obligation, actually use it as an "exemption clause" to conceal their pursuit of information economic interests and to avoid legal oversight. Faced with the formalized dilemma of the "notification-consent" principle, relying solely on an individual's right to control information as the standard and mainstay of personal information protection and utilization may not yield the desired outcomes. The market-oriented mechanism, which depends on the supervision and enforcement by private entities like society and individuals, struggles to address the risks and violations posed by highly organized, large-scale, and technologically advanced information processors. It might be considered an unrealistic ideal for personal information protection. Should we then consider establishing reasonable limits at the information collection and processing stages? The General Data Protection Regulation asserts that "data shall be sufficient, relevant, and limited to the minimum necessary for the purposes for which they are processed." China's Cybersecurity Law mirrors this sentiment, stating that network operators should not collect personal information unrelated to the services they provide. Articles 5, 6, and 51(4) of the Personal Information Protection Law call for "reasonably determining the operating authority for personal information processing and regularly providing safety education and training to practitioners," both of which necessitate the principle of proportionality in data processing. This principle should be adhered to before initiating information processing activities. Drawing from the "victim consent" model in criminal law, we can discuss the complexity of notifications and their impact on individual comprehension. This framework allows for the introduction of both express and implied consent, offering fresh perspectives on defining informed consent mechanisms. Explicit consent requires the information subject to have a clear understanding and acceptance of the key terms, whereas implied consent infers tacit approval based on the subject's behavior or silence. Addressing the challenges in the informed consent mechanism can be more effectively achieved by subsequently determining the intensity of term readings.

The informing mechanism's design should adhere to the principle of proportionality, ensuring the reasonableness and necessity of information collection. This implies that the notification content should correspond with the purpose of information collection to prevent information overload. Concurrently, information subjects should be thoroughly informed about the nature, scope, and potential outcomes of the information collection activities they are part of, achieving a balance between the collection's purpose and the subjects' rights and interests at the outset of collection. By carefully designing the notification mechanism, it's possible to preserve the efficiency of information collection while upholding the information subject's right to know and to choose, thus harmonizing information utilization with personal privacy protection.

2.4. Obligations, Powers and Responsibilities of Information Processors and National Authorities

The Personal Information Protection Law's handling rules aim to ensure personal information is managed and protected reasonably through autonomous decision-making and the State's legal interest protection regulations. Autonomous decision-making, specifically the "notification-consent" mechanism, provides individuals with the authority and state-backed protection to control their information, while also setting a legal rights barrier for information processors. However, relying solely on autonomous control to safeguard personality rights' legal interests is inadequate to counter the risks associated with large-scale collection, leakage, and misuse of personal information in electronic systems. Thus, the state must implement additional mechanisms to protect legal interests, ensuring the effective safeguarding of the freedoms and rights associated with personal information.

Information processors are tasked with upholding the principles of legitimacy, necessity, and purpose as dictated by current legal standards. Should the personal freedom, interests, and rights inherent in personal information face potential violation due to the processor's misconduct, it falls on the processor to preempt such risks of infringement. The processor is duty-bound to both avert the risk and to swiftly implement corrective or mitigating actions following any damage. These institutional norms form the initial defense for the protection and prudent utilization of personal information, situating the processor as the frontline guardian.

Informatized offices position administrative agencies as the primary collectors and processors of citizens' personal information, also assuming the sole responsibility for safeguarding this data. As information collection and processing are integral to the daily execution of government departments' legal duties, the integrity of administrative bodies and the robustness of their internal regulations and supervisory systems are crucial, especially amidst the intricate interplay of interests. Chapter 6 of the Personal Information Protection Law explicitly defines the responsibilities of the State Internet Information Department and associated government agencies, empowering administrative entities with the requisite authority to bolster the efficacy of administrative enforcement. Administrative bodies are permitted, through legal channels, to gather citizens' highly sensitive information, including financial, real estate, employment, and medical data. This information harbors significant economic value, as evidenced by its use in social security management by administrative law enforcement, such as monitoring behavior via traffic cameras, and by judicial entities in accessing personal information for trials. However, the substantial volume of highly private personal information in the possession of public authorities also introduces potential conflicts in personal information protection. Article 34 of the Law on the Protection of Personal Information places a necessity restriction on the authority to collect and manage information, aiming to balance the legitimate use of information with its protection. Nonetheless, the lawful and legitimate collection, use, and even sharing of personal information among government, law enforcement, and judicial sectors can still engender conflicts in personal information protection, which indeed sets the stage for such conflicts.

The current framework of personal information protection is grounded in the rights and interests of personalities under civil law, relying on the "notification-consent" mechanism. This mechanism is designed to enable citizens to independently control and make decisions regarding their personal information flow and to assume responsibility for it. However, individuals often face limitations in anticipating and being accountable for the potential damage caused by

their information-handling actions. Thus, it becomes the State's duty to proactively implement measures that provide essential protection and safeguard rights and interests. The state must establish a specialized legal framework by setting rules for information processing, which governs key stages including data collection initiation, the processing itself, and risk assessment. This entails a comprehensive oversight of information processing to ensure that personal information is used lawfully and reasonably, while also preventing potential misuse and leakage risks. Establishing this legal order goes beyond the scope of private law alone, necessitating the involvement and harmonization of public law to balance personal information protection with societal development.

3. Linkage of Sectoral Law Safeguard Mechanisms to Promote the Protection and Rational Use of Personal Information

3.1. Combining Public and Private Law

Firstly, under civil law, both the Civil Code of the People's Republic of China (hereinafter referred to as the Civil Code) and the Personal Information Protection Law focus on the protection of legal interests over rights. Prof. Wang Liming noted in his monograph on the General Principles of the Civil Law that personal information isn't treated as an independent personality right. There's a significant difference in the strength of protection between rights and legal interests, with considerable controversy surrounding the elements of tort liability. The Civil Code's Tort Liability Section outlines four elements necessary for tort liability: an illegal act, damage, causation, and fault. Damage must reach a certain threshold to constitute an infringement, but defining this "threshold" is often vague. If a citizen's phone number is stolen and sold, their ability to predict future loss risks is likely limited. Moreover, throughout the information circulation process, processors and users at various stages, such as resale and marketing, may reattribute economic value to information, increasing the risk of harm to the information subject. Estimating a person's information economic value is equally challenging. In contrast, public law plays a more pronounced role in personal information protection. For instance, the Criminal Law has become a powerful social governance tool, with the "crime of infringement of personal information" serving as a severe remedy for such infringements. The Cybersecurity Law enhances the responsibilities of cybersecurity supervision staff, and the Data Security Law ensures the security of personal information-containing data. The combination of consumer public interest litigation mechanisms in the Consumer Rights and Interests Protection Law and the public interest mechanism in the Personal Information Protection Law strengthens personal information protection capabilities. Secondly, the purpose of personal information protection is to uphold human dignity, a core objective in authoritative international legislative documents and most countries' legislation. China's Constitution includes personal information protection under "human dignity" in the "fundamental rights and freedoms of the individual" chapter. This constitutional guarantee reflects the promotion of "human dignity" as a universal value, leading to the enjoyment of "freedom," "correct identification," and "equality." Legal protection of personal information includes the individual's right to information self-determination, meaning citizens can decide whether to consent to their personal information's disclosure. Unconsented collection by entities violates individual dignity. "Correct identification" means individuals can ensure the accuracy and completeness of their information, including rights to access, copy, correct, and delete. "Equality" implies that personal information protection should adhere to principles of equality and non-discrimination. However, modern Internet economies see platforms using big data for price discrimination, such as "familiar customer price killing," marking up consumer groups and treating user rights as bargaining chips, thus not respecting or safeguarding constitutional "human dignity." This calls for effective measures to regulate platform behavior and protect consumer rights, issues beyond civil law's scope and closely related to economic law's anti-monopoly provisions and administrative law. From the perspective of personal information utilization, the value of data lies in its circulation and reasonable use, reflecting individual interests' concession to public interests. However, unreasonable information use may harm human dignity and social public interests. Public law offers a more authoritative and mature system for setting, restricting, enforcing, and safeguarding information. The integrated application of public and private law sectors provides crucial support for administrative protection, civil safeguards, and criminal penalties for personal information, constructing a comprehensive legal remedy system for its protection.

The legal attributes of personal information rights have evolved from individual attributes to incorporating public attributes. This evolution signifies that during information processing, individual and public interests are increasingly intertwined. As a result, risks have transformed from individual to public, implicating the deprivation of human dignity and the value interests of social groups when they reach a public scale. In the journey of personal information protection, the fusion of public and private law protection can compensate for the inadequate protection offered by a single sectoral law, especially in the swiftly evolving digital economy. This fusion represents a departure from the traditional single-sector law system and marks a significant innovation in forging a diversified approach to personal information protection. The integration of public and private law aims to establish a dynamic equilibrium between individual and public interests in most cases. This equilibrium not only safeguards the legitimate rights and interests associated with personal information but also fosters the rational use of information, showcasing the law's adaptability and progressiveness in response to societal development.

3.2. Coordinated Pairing of Risk Management and Relief Mechanisms

The existing methods for protecting personal information rights and interests are primarily reactive, only engaging when a specific civil entity's rights and interests have been actually infringed upon, causing the information subject to suffer damage to privacy and other personality rights or property rights. At this point, civil law exerts its punitive function, initiating civil litigation mechanisms, issuing injunctions to characterize the damage to personality rights, barring nuisance, or ceasing infringement, and providing compensation for losses and other relief. The trigger for an individual to initiate civil litigation is not the mere infringement of private information but the actual harm that results from it. Both the United States and the European

Union demonstrate this principle in cases involving information infringement and personal data enforcement proceedings. Given the retrospective nature of civil enforcement remedies, it's worth considering whether a risk-adjustment mechanism should be introduced for both ex ante and ex post violations of information processing regulations. Such a mechanism could ensure more comprehensive protection of individual rights and interests and bolster individuals' confidence and motivation in information protection. Enterprises, as the origin of potential information processing violations, should enhance information protection measures from the outset. China's current Personal Information Protection Law, particularly Chapter V detailing the obligations of personal information processors, illustrates this approach. It includes provisions such as "the development of internal management systems and operating procedures," "the designation of a person in charge of personal information protection in accordance with regulations by the national net information department," and "requirements for foreign personal information collectors to establish specialized agencies or appoint representatives in China." These measures reflect China's deliberate effort to consolidate scattered personal information collection enterprises into a systematic Information Processing Pool. Firstly, the government takes the lead in vetting domestic enterprises eligible for data collection. Only those enterprises that meet the government's unified verification standards—such as corporate credit, supervisory and management systems, risk prevention and control measures, and rights and remedies—obtain licenses to collect citizens' personal information within the country. Secondly, after obtaining a license and the informed consent of the information subject, enterprises are authorized to collect data. The information subject retains the freedom to grant or withhold consent, embodying the "right to self-determination," a key right for safeguarding human dignity and fostering human development. Furthermore, once an individual consents to an enterprise collecting their personal information, they still possess the right to request changes, the right to erasure, and the right to seek compensation for privacy infringements. Individuals can request updates to their personal information data when it changes or request erasure when they no longer wish their data to be circulated. Lastly, once an enterprise acquires personal information, it must ensure that data is circulated only within the designated enterprise. The enterprise should regularly self-inspect its information processing and data circulation standards, while the administrative authority's supervisory and management department should oversee compliance. Non-compliant enterprises may face license revocation or administrative or criminal penalties. The implementation of these measures requires stringent control and administrative supervision at multiple levels.

In accordance with the aforementioned principles, formal "risk minimization" and "risk limitation" can be achieved, aligning with the current era's focus on data and personal information protection and use, as well as industrial development policies. The enforcement mechanism of civil law is better suited for providing post-infraction tort relief, given its consideration of individual preferences and diverse interests. Conversely, personal information protection necessitates the complement of administrative oversight and criminal sanctions during the pre- and ongoing stages. Firstly, administrative authorities must coordinate the establishment of a permit pool for personal information collection and develop corresponding regulations to set standards that balance leniency and strictness for protection and reasonable use. Secondly, to safeguard citizens' right to information self-determination, administrative authorities should enforce the law in line with the public supervision provisions of the Personal Information Protection Law. Thirdly, given their role in managing information security risks and minimizing damages, administrative authorities may enhance these efforts. Fifthly, the link between administrative responsibility and criminal punishment must be fortified to ensure that government agencies adhere strictly to regulations when handling personal information, thereby effectively safeguarding its security through increased criminal penalties. However, such strengthened legal constraints should not impede the normal functioning of government agencies. Criminal law, with its apologetic nature, targets legal interests unprotectable by other means. Even with ample evidence of legitimacy indicating an at-risk legal interest, the presence of severe consequences and public impact must be assessed. The Supreme People's Court and the Supreme People's Procuratorate's interpretation on several issues regarding the application of law in criminal cases of personal information infringement clearly defines "seriousness of circumstances," considering factors like the sensitivity of the information, the volume of the infringement, its value, and the infringement's purpose. This reflects judicial officials' deliberate consideration of the risks of information infringement and potential misuse, aiming to maximize the deterrent and corrective effects of punishment and ensure proportionality in meting out justice. Where harm occurs, in addition to civil liability remedies, public law sanctions, including administrative and public security penalties, as well as criminal penalties, may also be invoked.

4. Conclusion

In the digital age, personal information's attributes have evolved from traditional personal to public attributes, necessitating a shift in protection methods. Protection now revolves around individual autonomy, focusing on regulating information processing risks and implementing preventive measures and remedies, rather than merely defending human dignity and freedom. However, relying solely on "anonymized" information for compliant handling may not suffice. The "informed consent" mechanism has its limits in empowering individuals to safeguard their personal information rights and interests, with civil law remedies typically activated only after a violation has occurred. As highlighted earlier, personal information holds significant economic value in modern society, where reasonable utilization often surpasses absolute protection in meeting contemporary demands and fostering progress. Yet, the current normative system and logical framework have gaps that impede the creation of a balanced system for personal information that respects individual rights and public values. An in-depth examination of personal information's legal attributes, concept definitions, information subject rights, and the obligations, duties, and responsibilities of information processors can guide legislative directions during societal transformations. Undoubtedly, future legislation or legal revisions will need to delicately address the balance between personal information protection and utilization. Integrating personal information protection within a public and private law framework, consolidating information collectors into a unified processing pool, and complementing this with

administrative, criminal, and civil law remedies presents a valuable developmental direction. This approach may foster equilibrium between safeguarding and utilizing personal information. Each societal transition brings new values and concepts, meriting our appreciation and thorough exploration.

Acknowledgments

First of all, I would like to thank my school, Anhui University of Finance and Economics, which initiated the Graduate Student Research and Innovation Fund program, giving me writing opportunities and financial support.

Second, I would like to thank my supervisor, under whose guidance and supervision it has been a great honor to study.

Thirdly, I would like to thank my friends who gave me a lot of advice and accompanied me during the process of writing this thesis.

Lastly, I would like to thank my family for providing me with a comfortable and quiet environment in which I was able to write in peace.

I would also like to thank the people who took the time to read and give me advice that will help me immensely in writing future papers.

References

[1] Zhang Xinbao. "From Privacy to Personal Information: Theory and Institutional Arrangements for Rebalancing Interests." Zhongguo Jurisprudence, No. 3, 2015, pp. 38-59.

[2] European Data Protection Supervisor. EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. p. 20.

[3] Zhang, J. and Yao, Y. (Eds.). (2020). Legal Guide to Data Protection and Network Security of Countries Along the "Belt and Road" [M]. Beijing: Intellectual Property Publishing House.

[4] Li, L. (2024). The Path to Balancing Personal Information Protection and Utilization in the Digital Age [J]. Administrative Law Research, (01), 111-122.

[5] Shu, S. (2024). The Practical Dilemma and Solution Path of Personal Information Protection and Utilization in the Digital Age: Reflections on the "Notice-Consent" Mechanism [J]. Southern Journal, (02), 65-68.

[6] Deng, L. and Chen, Z. (2024). Reflections on the Concept of the Right to Privacy: Centered on the Analysis of Private Information [J]. Information Communication Technology and Policy, 50(01), 53-58.

[7] Zhu, X. and Zhou, X. (2018). Balancing Personal Data Utilization and Protection in the Big Data Era: Proposing the "Resource Access Model" [J]. Journal of Zhejiang University (Humanities and Social Sciences), 48(01), 18-34.

[8] Zhou, H. (2018). Practice and Future of Online Privacy and Personal Information Protection: A Comparative Study Based on Judicial Practices in the EU, the USA, and China [J]. Governance Research, 34(04), 122-128. DOI: 10.15944/j.cnki.33-1010/d.2018.04.015.

[9] Wang, X. (2021). The Three-Layered Structure and Protection Mechanism of Personal Information Rights and Interests [J]. Modern Legal Science, 43(05), 105-123.

[10] Ding, X. (2019). On the Ideological Origin and Basic Principles of Legal Protection of Personal Information: Based on the Analysis of "Fair Information Practices" [J]. Modern Legal Science, (03).

[11] Zhang, X. (2019). The Limitations of the Application of the Informed Consent Principle in Personal Information Collection [J]. Comparative Law Research, (06), 1-20.

[12] Lv, B. (2021). The Dilemma of "Consent" in Personal Information Protection and Its Solution [J]. Legal and Commercial Research, 2021(2), 89-90.

[13] Gao, F. (2016). International Rules on Personal Data Protection and Utilization: Origins and Trends [M]. Beijing: Law Press China, p. 36.

[14] Zhang, X. (2021). On the Construction of Personal Information Rights and Interests [J]. Chinese and Foreign Law, 33(05), 1144-1166.

[15] Wang, J. (2024). Legal Interests and Rights: Legislative Choices and Value Expression of Personal Information Protection in the Big Data Era [J]. Journal of Hubei University of Technology, 44(01), 49-56. DOI: 10.16751/j.cnki.hbkj.2024.01.003.

[16] Tang, H. (2023). Correcting the Perspective of Weakening the Protection of Publicly Disclosed Personal Information [J]. Journal of Jiangxi Electric Power Vocational and Technical College, 36(11), 127-131.

[17] Wang, L. (2018). Research on the General Rules of Civil Law [M]. Beijing: China Renmin University Press, p. 401.

[18] Huang, W. (Ed.). (2020). Interpretation of the Tort Liability Code of the People's Republic of China [M]. Beijing: Law Press China, p. 7.

[19] Yang, L. (2021). Problems and Countermeasures in the Private Law Protection of Personal Information [J]. Frontline of Social Sciences, (01), 193-202.

[20] Gao, F. (2019). On the Purpose of Personal Information Protection: Centered on the Distinction of Legal Interests in Personal Information Protection [J]. Digest of Social Sciences, (03), 11-13.

[21] Veil, W. (2018). The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law [J]. Neue Zeitschrift für Verwaltungsrecht, 10, 686, 703-705.

[22] Haley, T. D. (2020). Data Protection in Disarray [J]. Washington Law Review, 95(3), 1193-1252.

[23] Roxin, C. (2007). The Development and Modern Trends of German Criminal Law Principles [J]. Jurist, (01), 151.