Research on Personal Information Protection from the Perspective of Economic Law in the Digital Economy Era

Shuang Liu*

College of Accounting, JiLin University of Finance and Economics, Changchun, Jilin, China

*Corresponding author: Shuang Liu (Email: 2367702898@qq.com)

Abstract

This article explores the economic law attributes and protection strategies of personal information in the era of digital economy. With the development of the digital economy, personal information has become a key resource, and its protection is confronted with challenges such as market asymmetry, high social costs, and imbalance of rights and obligations. This article analyzes the economic value, transaction characteristics and legal dilemmas of personal information. Drawing on the experiences of Europe and America, it proposes countermeasures such as strengthening legal construction, optimizing the data market, improving the regulatory system and providing legal remedies, aiming to balance the protection and utilization of personal information and promote the healthy and orderly development of the digital economy.

Keywords

Digital Economy, Personal Information Protection, Economic Law, Regulatory Optimization.

1. Introduction

In the contemporary era of accelerated digital economic development, personal information has emerged as a pivotal catalyst for this growth. This pervasive phenomenon encompasses various domains, including e-commerce platforms, online social media, and specialised fields such as digital finance. In these contexts, personal information is systematically collected and extensively utilised. However, in the event of technical or legal loopholes being present in these links, there is a risk of abuse or leakage of personal information, which has the potential to result in significant financial losses for individuals, in addition to causing disruption to the normal order of the digital economy. It is evident that economic law, as a regulatory framework that seeks to balance the interests of individuals and society in economic activities, should play a significant role in protecting and promoting the rational use of personal information. In addition, it should address the issue of illegal use of personal information, thereby further regulating the economic order in the digital environment.

2. Analysis of the Economic Law Attributes of Personal Information

2.1. The Importance of Personal Information

In the contemporary digital economy, there is an imperative to rely on the sharing of personal information to optimise the allocation of resources, to demonstrate the advantages of new technologies such as big data and artificial intelligence, to promote industrial upgrading, and to achieve common benefits for society and individuals. The overarching institutional objective of personal information protection is not to safeguard personal information itself, but rather to protect the relevant rights and interests in the processing of personal information. In light of these concerns, The Times has proposed an escalation in the requirements for the protection of personal information security[1]. This proposal entails a further elucidation of the objectives, responsibilities and pertinent technical standards governing the protection of personal information. It emphasises the integration of personal information protection with particular application scenarios, and identifies the optimal equilibrium between the safeguarding of privacy and the promotion of economic development in the context of e-commerce[2]. The overarching aim of these measures is to establish a more robust and sustainable information ecosystem. In the contemporary context of digitalisation, informatisation and intelligence, personal information is set to become a pivotal asset. The collection, organisation and application of personal information will permeate all aspects of social and economic development. The establishment of a robust economic order, as well as the efficient circulation and full utilisation of data resources, is predicated on the protection of this fundamental resource of personal information. On the one hand, the enhancement of personal information protection is conducive to market entities further carrying out personalised, innovative and diversified economic activities. By leveraging personal information to accurately determine user location, the platform can optimise resource allocation, enhance the efficacy of economic activities, and offer users products that are more aligned with their needs. Furthermore, the scientific collection and systematic utilisation of personal information are conducive to the government's ability to predict market trends, gain insight into the actual needs of users, and thereby provide substantial support for the guidance of industrial development and the optimisation of industrial policies.

2.2. The Economic Law Attributes of Personal Information

The protection of personal information has been demonstrated to be closely related to the construction of economic rule of law. The establishment of a robust economic legal guarantee system is imperative for ensuring the security of personal information in economic activities. Such a system is also crucial in addressing the harm caused by unstable factors in market application to personal information security. In general, economic law places greater emphasis on the intricacies of personal information protection. Firstly, the protection of personal information is an integral component of maintaining economic order, emphasising the prevention of illegal theft and use of personal information from the perspective of regulating market order. Secondly, economic law has established a comprehensive personal information protection mechanism, striving to form an all-round and multi-level protection system. For instance, it emphasises the importance of safeguarding the information security of market entities. It also stresses the establishment of a reliable data and information circulation management environment, the acceleration of research and development and promotion of related protection technologies, and the promotion of a positive interaction between personal information protection and the development of the digital economy[3]. Furthermore, from the standpoint of economic law, the protection of personal information security is characterised by a more global perspective. This perspective aims to enhance cross-border exchanges and cooperation, thereby effectively promoting the joint efforts of multiple countries and regions to safeguard the security of personal information. In the digital age, the most significant challenge confronting traditional legal acts pertains to the protection of personal information rights and interests in data transactions. The distribution and utilisation of the benefits derived from personal data have become subjects that necessitate regulatory oversight. [4] Within the domain of economic law, the safeguarding of personal information is inherently intertwined with the preservation of personal privacy. The emphasis is placed on the orderly flow of personal information in economic activities. The utilisation of personal information is regulated, and its property value attribute is ensured. Personal information is regarded as an important asset, and its value is guaranteed through relevant laws.

2.3. The Transaction Characteristics of Personal Information

In the context of the rapid development of the digital economy, there has been a notable increase in the trading of personal information. The subjects involved in the trading of personal information principally comprise individuals, enterprises and intermediary agencies, amongst others. Furthermore, transaction data manifests in a variety of forms, each of which possesses distinct characteristics. It has been demonstrated that such systems have the capacity to facilitate direct exchange of personal information. This exchange may be of a direct nature, for example in the way enterprises use personal information with the authorisation of users. The acquisition of personal information can also be achieved indirectly through the utilisation of data intermediary agencies, which employ data monitoring methodologies to obtain insights regarding the online and offline behaviours of consumers. It is generally accepted that information itself is non-competitive and can be repeatedly used and traded in the transaction process. Nevertheless, the value of the information is challenging to quantify, and there is an imbalance between the two parties involved in a transaction, which to a significant extent amplifies the transaction risk. To illustrate this point, consider the case of China, where the exchange of personal data is categorised into two distinct markets: the primary market and the secondary market. The primary market is defined as the exchange of data between individuals and institutions, which can be considered as the process of collecting personal information. It is imperative that transactions between major index data processors in the secondary market adhere to the principle of legal compatibility. In the context of the increasing volume and complexity of data and information, there is an imperative to explore democratic consultation and individual self-governance mechanisms for personal data transactions. Such mechanisms are designed to prevent unfair phenomena and to ensure the effective protection of personal privacy in the public domain.

3. The Economic Legal Predicament of Personal Information Protection

3.1. Information Asymmetry in the Market

In the digital economy, information asymmetry is pervasive, and the collection of personal information has become a significant means for enterprises to gain competitive advantages. Enterprises rely on their technological advantages to control, centrally process and utilise personal information, while individuals are at a disadvantage and find it difficult to accurately judge information processing behaviours. This may result in huge losses, such as the loss of rights and interests due to a lack of understanding of complex transaction policy documents. In the context of information reuse or sharing within enterprises, individuals frequently remain unaware of such activities[5]. For instance, the dissemination of information to third parties has the potential to result in users being subjected to targeted advertisements. Information asymmetry has been demonstrated to have several consequences. Firstly, it can result in individuals being unable to fully exercise their rights. Secondly, it can lead to the failure of data market allocation. Thirdly, it can result in the concentration of information resources in a small number of enterprises. This, in turn, can influence market operation and cause the data market to lose vitality.

3.2. The Persistently High Social Costs

In the current era, characterised by the proliferation of data assets, it is imperative to not only prevent data abuse and leakage, with a view to reducing losses suffered by subjects, but also to regulate the infringement of individual privacy by data, which is now considered a public asset. Should the overseas listing of a specific taxi-hailing application result in the disclosure of user information, or give rise to class-action lawsuits, questions concerning regulatory capabilities would be raised. Furthermore, such an occurrence would also engender risks such as telecommunications fraud, thereby increasing the cost of maintaining social information security. In the pursuit of optimising the benefits of information assets, enterprises frequently neglect the privacy attributes of personal information, resulting in its utilisation deviating from the social optimum[5]. The associated costs are then shouldered by society and individuals. From the perspective of economic law, the protection of personal information should originate from the perspective of the public domain of privacy. It is imperative that the property-like nature of personal data in the public domain is recognised, whilst simultaneously acknowledging its personal characteristics. It is imperative that we utilise all available resources while also circumventing the "tragedy of the Commons".

3.3. The Imbalance between Rights and Obligations

There is a discrepancy in the amount of information available to enterprises and individuals. Enterprises possess greater autonomy in the domains of information collection, organisation and utilisation, while individuals possess limited ability to safeguard their rights and interests. In the event of an infringement of an individual's personal data, it can prove challenging for that individual to exercise their rights. The provision of evidence in such cases is often challenging, due to the high costs involved and the fact that compensation frequently fails to cover the losses incurred. The prevailing legislation does not impose adequate penalties on enterprises for violations and has weak deterrent effects. The encouragement of individuals to receive a share of the revenue from information transfer has the potential to result in a significant increase in data transaction costs, impede information circulation, and render the data market meaningless. Consequently, the ethical processing of data must encompass both the safeguarding of individual rights and the mitigation of transactional expenses. In light of the aforementioned circumstances, it is imperative to address the prevailing disparity between rights and obligations. This necessitates the identification of reasonable and economically sound methods that align with the principles of economic law. Such methods are designed to balance the rights and interests of all parties involved, thereby fostering the growth and prosperity of the data market. Furthermore, these approaches are intended to maximise the interests of all stakeholders and to accurately reflect the inherent value of data assets.

4. Economic Law Principles for Personal Information Protection

4.1. Principle of Acting in Accordance with the Law

The establishment of more reasonable systems is imperative, whether for the protection of personal information or the realisation of the rights and interests of personal information. Presently, the principle of legality is predominantly applicable to the secondary market, emphasising that enterprises should protect personal privacy from infringement. Specifically, it is manifested as not constituting a crime, not constituting infringement, not constituting a breach of contract, and not being subject to administrative penalties. For instance, it is prohibited to obtain information by exploiting loopholes in data technology and to intercept non-public information through technical means, etc. Concurrently, economic law imposes restrictions on the transfer behaviour of the previous owner of personal information and ensures the traceability of data transactions. It is evident that China's data trading market is undergoing continuous improvement, which is set to result in the professionalisation of data security and protection utilisation. Consequently, data trading is poised to occur within a more comprehensive and legally sound environment. The principle of adherence to the law necessitates not only the standardisation of data trading behaviour within the secondary market, but also the cultivation of a conducive data trading culture. This is fundamentally aimed at promoting a comprehensive understanding of the essence of data trading among all relevant parties, while ensuring the safeguarding of personal privacy and security.

4.2. Compatibility Principle

It is imperative to note that data transactions necessitate not only the explicit consent of the data subject, but also the alignment with their stipulated privacy expectations. Secondary transaction behaviours should be given greater consideration to ensure a balanced consideration of the rights and interests of all parties. The methods of processing personal information are diverse, and frequently involve the repeated collection of personal information. It can be posited that the data transmission chain is not a single entity, but rather a complex non-chain structure. It is evident that the principle of compatibility necessitates adherence to the reasonable expectations of the data subject as the criterion, superseding the necessity to obtain the consent of each data subject. It is acknowledged that an enterprise may, without seeking the consent or permission of any subject, engage in a transaction if the relevant behaviour is regarded as reasonable under reasonable circumstances and in line with expectations, and such transaction behaviour is objectively considered reasonable. The concept of compatibility is of particular significance in the context of data collection and processing. It is imperative to ensure that the purpose of data collection and subsequent processing is aligned with the expectations of social recognition. This necessitates the implementation of robust safeguard measures to ensure the integrity and security of the data. It is imperative to consider several significant variables in the implementation of compatibility practices. One is the participant, who is understood to refer to the providers, recipients and processors of data. A further category of data is that which is of a medical, financial or educational nature, et cetera. The third is the principle of information transmission. The compatibility principle must take into account compatibility in specific scenarios. The reutilisation of personal information is only permissible when all aspects fall within a reasonable range, and this can only be achieved with the explicit consent of the subject.

5. Personal Information Protection Can Draw on Experience

5.1. EU Experience

The European Union has established a strict personal information protection mechanism. Following the formulation of the Computer Data Protection Act in 1995, the General Data Protection Regulation was introduced, with the purpose of restricting the collection, transmission, storage and processing of data. From the perspective of economic law, this regulation attaches great importance to protecting the right to know, access and delete personal information, and strengthens individuals' control over their own information. For instance, it requires enterprises to clearly inform users of the purpose of the information before they can obtain it, and prohibits tacit consent to obtain it. It is imperative that the conditions under which enterprises are permitted to utilise information are standardised, and that a data protection impact assessment mechanism is adopted in order to ensure the security of personal information. It is imperative that a high-fine mechanism be established, with a view to imposing a fine amounting to 4% of the global turnover on enterprises that violate the law. Furthermore, the cost of violations must be increased, while the market order must be maintained and a personal information protection barrier built.

5.2. American Experience

The United States has a long-standing tradition of safeguarding personal information. The constitution and common law of the United Kingdom place significant emphasis on the protection of information privacy rights. However, the most relevant regulations are those that restrict government agencies and regulate their use of personal information. The advent of data collection and utilisation has led to the adoption of decentralised legislation in the United States, with the aim of regulating the protection of personal information in various sectors, including financial institutions and medical institutions, through the implementation of specialised legislation. The efficacy of these regulations in enhancing compliance mechanisms for utilisation is well-documented, and their professional approach, extensive range of applications, and cost-effectiveness in safeguarding individual rights have been widely acknowledged. Furthermore, the United States has implemented enhanced regulatory oversight through institutions such as the Federal Trade Commission, imposed sanctions for violations, and advocated for remedial measures to prevent the recurrence of such incidents.

5.3. Implications for Our Country

The European Union and the United States have both demonstrated a strong commitment to the protection of personal information security, amassing considerable expertise in this domain. The insights garnered from this experience can serve as a valuable foundation for China to refine its regulatory framework and bolster the efficacy of its protection mechanisms. Firstly, the spirit of the rule of law must be upheld, with legislation being strengthened and it being clearly stipulated that the processing of personal information must be agreed upon by the individual. The second of these approaches is to strengthen the rights of data subjects, such as their right to know. The third approach is to impose strict penalties on illegal acts and to increase the cost of violations. Concurrently, there is a necessity to draw upon the regulatory frameworks of foreign data markets, to provide guidance to market regulation through legislation, to encourage self-regulation among enterprises, and to assign regulatory responsibilities. Furthermore, it is imperative to strike a balance between the principles of protection and utilisation. In order to achieve this, it is essential to optimise the regulatory mechanism, innovate regulatory methods, strengthen international cooperation, and establish a comprehensive information protection mechanism. This may be achieved by enhancing impact assessment, conducting pre-review of high-risk behaviours, and promoting the establishment of ethical assessment institutions[6].

6. Countermeasures for Protecting Personal Information under Economic Law

6.1. Strengthen the Construction of Laws and Regulations

To leverage the role of economic law in safeguarding personal information security, it is necessary to improve the legal protection system, refine regulations, and formulate rules that meet the demands of China's data market. First, improve the rules for the collection and sharing of personal information[7]. On the basis of the Personal Information Protection Law, improve the Data Security Law and clarify the standards for protection and application. Second, clarify the boundaries of personal information collection, determine the rights and responsibilities of data transaction subjects, formulate relevant regulations, specify penalties for violations, and balance the relationship between enterprises and individuals. Third, economic law needs to coordinate its relationship with other regulations, avoid legal conflicts, and pay attention to the applicability of the law[8].

6.2. Strengthen the Construction of the Data Market

To protect personal information security, it is necessary to strengthen the construction of the data market and explore market circulation mechanisms. For instance, improve the data pricing mechanism and establish a reasonable pricing system; Under the guidance of economic law, develop data intermediary services, grant them the authority to anonymize and de-identify, carry out personal information security assessment services, and reduce the risk of leakage. Advocate the establishment of an industry self-discipline mechanism, optimize protection standards, encourage enterprises to issue privacy protection commitments, and industry associations should strengthen supervision and guidance, punish illegal acts, and create a favorable trading environment.

6.3. Optimize the Information Supervision System

In the era of digital economy, to protect personal information security, it is necessary to improve laws and regulations, give full play to the leading role of the government, and establish a socialized supervision system. Clarify the division of regulatory responsibilities to avoid regulatory gaps. Establish a multi-departmental collaboration and communication mechanism to achieve information sharing; Innovate regulatory methods, leverage the role of information technology, and obtain real-time leakage clues. Cooperate with international organizations, draft cooperation agreements, establish cross-border supervision mechanisms, and ensure the security of cross-border personal information flows.

6.4. Optimize Legal Remedies

To demonstrate the value of economic law in protecting personal information, it is necessary to explore legal remedies. Improve the litigation mechanism, optimize the procedures, and lower the threshold for rights protection. For instance, introduce the class action litigation system, improve the cost-sharing mechanism, and rationally allocate the burden of proof. Advocate non-litigation resolution methods, promote arbitration, and give full play to the role of industry associations; Explore legal aid methods, increase assistance to victims, provide legal knowledge aid, consultation and agency services, and protect their legitimate rights and interests.

7. Conclusion

Personal information is an important resource in the digital economy. Protecting and rationally utilizing personal information in accordance with the law is of great significance for promoting the healthy development of the digital economy. In today's social environment, it is necessary to effectively balance the relationship between personal information and market applications based on economic law, further interpret the economic attributes and transaction characteristics of personal information from the perspective of economic law, and solve many problems brought about by the asymmetry of information acquisition and the imbalance of rights and obligations. To this end, it is necessary to widely draw on domestic and international experiences, improve the market-based regulatory mechanism in accordance with the law, broaden the channels for legal relief, and adopt multi-level protection methods, so as to promote the orderly development of China's digital economy. In future construction, it is necessary to constantly innovate the supervision methods of personal information, actively respond to the new challenges brought about by technological changes, and ensure that personal information can be circulated in compliance and effectively utilized in the emerging technological environment

References

[1] Ding Xiaodong. Interpretative Reconstruction of the Sensitive Personal Information Protection System [J]. China Law,2025(2):173-176.

[2] Zhang Yu. Research on the Impact of Digital Economy in Agriculture and Rural Areas on Common Prosperity in Urban and Rural Areas: Based on Evidence from Quasi-Natural Experiments in Comprehensive Demonstration Counties of E-commerce Entering Rural Areas [J] Research in Technology Economics and Management,2024(2):123-128.

[3] Zhuang Jinsong. Research on the Promotion of Common Prosperity by Digital Technology Development: Theoretical Mechanism, Practical Challenges, and Practical Paths [J] Modern Trade Industry,2025(1):34-36.

[4] Xu Juan. "Two-sided Expansion, Three-Layer Referral" : A Legal Analysis of Digital Legal Acts [J]. Legal Review,2025(2):127-132.

[5] Li Ming. Application of the Principle of Minimizing Personal Information Collection in the Digital Economy [J]. Jiangsu Social Sciences,2025(2):182-184.

[6] Zhang Xuanxuan. Analysis of the Risks Posed by Generative Artificial Intelligence to Personal Information [J] Cooperative Economy and Technology,2024(22):182-184.

[7] Gao Beibei. The Impact of Digital Economy on High-Quality Economic Development: An Intermediary Perspective Based on the Upgrading of Human Capital Structure [J]. Science & Technology and Industry,2024,24(18):126-133.

[8] Chen Lu. Analysis on the Employment of College Graduates under the Background of Digital Economy [J]. Modern Trade and Industry, 2024,45(21):142-144.