International Journal of Trend in Research and Development, Volume 11(4), ISSN: 2394-9333
www.ijtrd.com

Legal and Economic Analysis of Personal Data Sharing Risk Regulation in the Context of Open Banking

Shang Mengzhen
Law and Economics, Beijing Wuzi University, Beijing City, China

Abstract: Digital finance represents the innovation of Internet technology in the financial field, promotes the further exploration and recognition of data value, and makes data sharing a hotly discussed topic. Open banking came into being against the backdrop of the rapid development of financial technology and the growing value of data. Its core lies in the data sharing between banks and third parties, which in turn promotes the integration and innovation of business. However, as an institution with a large amount of personal data of financial consumers, banks must take more effective regulatory measures to legally and compliantly protect consumers' personal data under the open banking model centered on information sharing. Therefore, from the perspective of law and economics, this paper analyzes the risks that may be encountered in the process of personal data sharing under the open banking model and emphasizes the importance of supervision. At the same time, a model is established to analyze the optimal legal supervision of personal data sharing and protection under the background of open banking, and a specific regulatory path for personal data sharing risks is proposed.

Keywords:*open banking, personal data protection, risk regulation, law and economics*

I.INTRODUCTION

Today, with the rapid development of digitalization and information technology, open banking has become an important trend in global financial innovation. Through open application programming interfaces, open banking allows third-party developers to seamlessly connect with banking systems to provide users with more personalized and convenient financial services. However, what follows is a significant increase in the sharing of personal data, which not only increases the efficiency of data processing, but also creates unprecedented risks. Due to the high value and sensitivity of personal data, the risk of data leakage and abuse has become increasingly prominent. How to balance the economic benefits of data sharing with the protection of personal privacy has become an urgent problem to be solved.

From the perspective of law and economics, legal supervision must not only focus on protecting consumer rights and preventing data abuse, but also take into account the potential impact of supervision on market innovation. Excessive regulation may inhibit technological innovation and market development, while insufficient regulation may lead to a lack of consumer trust and market chaos. Therefore, it is particularly important to build a legal and regulatory framework that can not only ensure the security of personal data, but also promote the healthy development of open banking. This article will focus on the risks of personal data sharing in the context of open banking, and explore how to promote financial innovation and service efficiency while ensuring data security and privacy. By analyzing existing laws, regulatory measures and their economic impacts, we propose improvements and suggestions, aiming to provide decision-making references for legislators and regulatory agencies to achieve the best balance between law, economy, and technology.

II.BASIC THEORETICAL

A.Risks of sharing personal data in the open banking model

1)Data authorization risks

The development of open banking relies on the mining of data benefits, and its platform tends to expand the scope of use of personal data. In the processing of personal financial data by open banks, there is always the risk of unauthorized use or exceeding the scope of authorization. In the data collection stage, personal data mainly faces the risks of over-collection and blanket authorization. Over-collection is reflected in the fact that the collected data exceeds the necessary scope; while blanket authorization means that the open banking platform usually adopts the "informed consent" model for one-time authorization. If financial consumers do not agree, they will not be able to enjoy certain services. In addition, individuals lack the right to choose and control the content and scope of authorization. In order to obtain services, they have to authorize according to the requirements of open banks. In the data processing and data sharing stage of open banks, the main risks faced by personal financial data are over-scope processing and over-scope sharing.These risks stem from the fact that after obtaining authorization, open banks expand the processing of personal financial data or share it beyond authorization, which is essentially an unauthorized or unauthorized behavior. The "Personal Information Security Specification" stipulates that when using personal information, it shall not exceed the reasonable scope of the purpose of use stated when collecting the information. However, since the definition of "reasonable scope of association" is not clear enough, in order to maximize data utilization, open banks may expand the scope of "reasonable use" as much as possible.

2)Data breach risk

The risk of data leakage mainly comes from two levels: internal and external. The internal risk is mainly related to system technology. In the open banking system, the processing of personal financial data depends on hardware such as machines and optical fibers, as well as software such as algorithms and codes. These data are circulated and shared through technical means such as APIs and SDKs. With the rapid development of digital finance, the complexity of the open banking system is also increasing. However, the current development trend shows that there is a mismatch between the focus on enhancing data processing capabilities and data protection capabilities. The improvement of data processing

capabilities and the enrichment of data resources have exposed personal financial data to greater risks. Vulnerabilities in any component or stage of the system may cause large-scale personal financial data leakage, bringing unpredictable serious consequences. The risk of external data leakage mainly comes from hacker attacks and abuse of public power. The financial sector has inevitably become the main target of hacker attacks due to its high asset nature and the high value, high accuracy and easy-to-identify characteristics of financial data. In addition, there are also cases of receiving illegal information such as illegal links, and the more serious problem is the theft of personal account passwords. The serious consequences of personal data leakage not only infringe on the citizens' right to a peaceful life, but are also more likely to cause malicious crimes such as financial fraud and online fraud.

3)Data discrimination risk

Data discrimination risk involves the open bank formulating its future development strategy based on the data after integrating and analyzing it. Due to the inherent bias and limitations of personal financial data, the open bank uses big data technology to conduct classification analysis, aiming to provide customized and differentiated services for different groups. However, in this process, some data subjects may be discriminated against or treated differently due to the results of data analysis.

B.The necessity of risk management

1)Data sharing rights protection requires regulatory support

The strategic choice of data sharing between consumers and banks seems to be the product of a spontaneous market mechanism, but in fact it is a problem involving legal and regulatory design. The uncertainty and imbalance of legal and regulatory policies have led to banks being unwilling, unable or afraid to share data. Therefore, regulatory intervention and improvement are needed to correct the failure of private law and the market, balance the interests of all participants in open banking, and promote data sharingto fully release its potential value. To this end, a solid legal foundation should be established for data sharing. On the one hand, the protection of the rights of data sharing requires regulatory support. Although Article 45, paragraph 3 of my country's "Personal Information Protection Law" stipulates the right to data portability, allowing the data subject to require the holder to transfer his data to a third party, this requires "complying with the conditions stipulated by the national cybersecurity and informatization department", which itself has a strong regulatory implication. On the other hand, the boundary between data sharing and the bank's confidentiality obligations needs to be clarified through supervision. As the guardian of customer data, banking institutions do weaken their confidentiality obligations through data sharing, but it is difficult to use this as a reason for exemption from liability in law, which reduces the motivation of banks to share data.

2)Abuse of data holders ' rights requires regulation

In the open banking model, shared data usually has the characteristics of subject-object separation. Even if consumers authorize third parties based on trust, banks as holders of customer data are still required to cooperate. However, in reality, banks may reject reasonable sharing requests out of the mindset of "owning customer data" or based on competition considerations. In this case, regulators need to restrain the abuse of data holders' rights. For example, the UK Competition and Markets Authority pointed out that it is unlikely to solve the problem of bank customer data sharing through market voluntary mechanisms, so it is necessary to take mandatory regulatory measures to promote data sharing.

3)Building a trust environment for data sharing requires improved supervision

Improving the regulatory system for risk prevention and control of personal data in open banking is crucial to ensuring the security of financial consumers' transactions on open banking platforms. As a bridge for sharing personal data between financial consumers and banks and third-party financial institutions, open banking platforms play a key role as information intermediaries. Given that information asymmetry is a common phenomenon, open banking platforms have become a key intermediary to reduce information asymmetry in the process of sharing personal data. Building a trust environment for data sharing is inseparable from effective supervision. By strengthening supervision of open banking personal data sharing, it is possible to promote the establishment of a more trustworthy data sharing environment and ensure that the platform assumes the responsibilities and obligations of a guardian. In addition, long-term supervision of the platform will help enhance financial consumers' trust in the platform, which will have a positive role in building an open, collaborative and win-win financial service ecosystem.

III.REASON ANALYSIS

In the open banking model, data sharing can significantly improve the operational efficiency of commercial banks, thereby enabling financial consumers to obtain better financial services. At the same time, strict protection of personal data may increase banks' credit reporting costs, but it also reduces the personal data risks faced by consumers. Therefore, when evaluating the effectiveness and fairness of legal regulatory principles, the sharing and protection of financial consumers' personal data should also be considered. To this end, a model can be built to analyze how to balance personal data sharing and protection under the open banking model to achieve the best legal regulatory effect.

A. Analysis of the optimal legal supervision of personal data sharing and protection

Assume that the personal data provided by financial consumers to commercial banks is i, and commercial banks provideThe amount of services provided is s, then $s = f(i)$.Assume that the amount of financial services provided by commercial banking institutions is proportional to the amount of personal data provided by consumers, and the growth rate of financial services is inversely proportional to the amount of personal data provided, that is, $f'(i) > 0, f''(i) < 0$, and $f(0) = 0$. Assume that the legal protection of financial consumers' personal data is $x(0 < x < 1)$, the larger the x, the stronger the legal protection of financial consumers' personal data. $m(x)$ is the damage coefficient caused by the leakage of consumers' personal financial data. The stronger the legal protection of personal data, the lower the cost coefficient and the lower the rate of reduction, that is, $m'(x) < 0, m''(x) < 0$, $m(0) = 1, m(1) = 0$. The personal data infringement caused by consumers' consumption of s units of financial services is $m(x)i^2$. From the perspective of

commercial banking institutions, the stronger the legal protection of personal data of financial consumers, the higher their operating costs and the lower the efficiency of financial services. Let $n(x)$ be the cost coefficient of commercial banks providing financial services, and its growth rate increases with the growth of x, that is,$n^{'}(x) > 0, n^{''}(x) > 0$. The cost paid by commercial banks to obtain the amount of information i is $n(x)s^2$; let α be the proportion parameter of consumers transforming from consumer financial services s into their own utility, and β be the proportion parameter of commercial banks transforming from shared information i into their own utility. Then the consumer utility function is:

$$E(s,x) = \alpha s - m(x)i^2 \qquad (1)$$

The utility function of commercial banking institutions is:

$$D(s,x) = \beta i - n(x)s^2 (2)$$

Assume that the total social utility is the sum of the consumer utility and the utility of commercial banking institutions, and its function is:

$$U(s,x) = \theta[\alpha s - m(x)i^2] + (1-\theta)[\beta i - n(x)s^2] \qquad (3)$$

Among them, θ is the weight assigned by the law to the rights and interests of financial consumers$(0 < \theta < 1)$, which is an increasing function of the legal emphasis on the rights and interests of financial consumers. By analyzing the optimal regulatory intensity x^* of consumer rights under the maximization of legal regulatory utility.

Taking the partial derivative of equation (3) with respect to x, We get:

$$\bigcup_x(s,x) = -\theta m^{'}(x)i^2 - (1-\theta)n^{'}(x)s^2 = 0 \qquad (4)$$

Available: $\frac{n^{'}(x^*)}{m^{'}(x^*)} = \frac{-\theta i^2}{(1-\theta)s^2} (5)$

From formula (5), we can see that the optimal regulatory intensity of the law on commercial banking institutions is x^*, which is determined by two factors: one is the degree of legal emphasis on consumer rights θ; the other is the relationship between the supply of commercial banking institutions s and the amount of consumer personal data provided i, that is, the conversion rate of commercial banking institutions from personal financial data to financial services $s = f(i)$. The impact of these two factors on the optimal regulatory intensity x^* is determined by the functional properties of $m(x)$ and $n(x)$. Here we mainly discuss the impact of changes in θ on x^*, and let $f(s) = s$. Since the utility of financial consumers consists of two parts, one is the increase in utility brought byreceiving financial services, and the other is the loss of utility brought by sharing personal financial data.

Therefore, the impact of θ on the optimal regulatory intensity x^* of the law can be divided into two cases: (1) When $[(n^{\wedge\prime}(x^{\wedge}*))/(m^{\wedge\prime}(x^{\wedge}*))]^{\wedge\prime} < 0$, the privacy protection effect caused by financial regulation exceeds its financial service effect. As θ increases, the optimal legalregulatory intensity x^* also increases accordingly. (2) When $[(n^{\wedge\prime}(x^{\wedge}*))/(m^{\wedge\prime}(x^{\wedge}*))]^{\wedge\prime} > 0$, the financial service effect caused by financial regulation is greater than the personal financial data protection effect. As θ increases, excessive regulation will reduce the utility brought by financial services, and then the legal optimal regulatory intensity x^* will decrease.

B. Constructing a legal and economic model to analyze the optimal regulatory intensity

For the supervision of personal financial data under the open banking model, the legal supervision intensity is optimal when the supervision utility is maximized, and there is an inverted U-shaped relationship between the two, as shown in Figure 1. In the early stage, the level of personal data protection is low. For each additional unit of legal supervision, the positive effect of personal data protection is greater than the negative effect of reduced financial efficiency, that is, $|\Delta E(s,x)| > |\Delta D(s,x)|$, thereby increasing the total legal supervision utility $U_x(s,x)$. However, as the law continues to increase the importance of consumers' personal financial data, after reaching the optimal point θ^*, the excessive pursuit of fairness means that the costs and risks of commercial banks will increase, making it impossible for them to provide more financial services. The negative effect of reduced financial efficiency will exceed the positive effect of personal data protection, that is, $|\Delta E(s,x)| < |\Delta D(s,x)|$, which will eventually lead to a decline in overall utility, which undoubtedly violates the goal of law and economics to maximize social utility. Therefore, the law should establish regulatory principles based on seeking a balance between the efficiency and protection of financial consumers' personal data sharing under the open banking model.

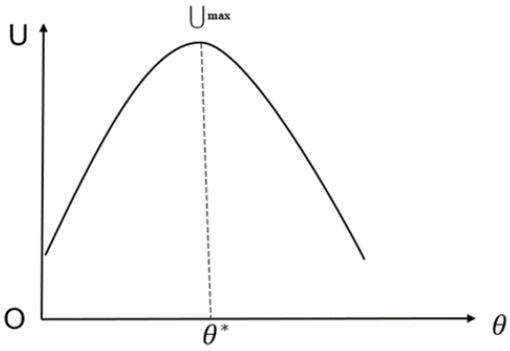

Figure 1: The relationship between legal regulatory effectiveness and legal regulatory intensity

IV. REGULATION

A. Establish and improve the system for protecting financial consumer information

As the main financial regulatory agency in my country, the People's Bank of China has established a mature management system to manage traditional financial institutions and has a dedicated financial information management center. This center is responsible for supervising the collection, use and sharing of personal financial data and is fully capable of comprehensively supervising the open banking platform. In establishing and improving the institutional system for protecting financial consumer information, the People's Bank of China has provided institutional guarantees for the protection of financial consumer information. Within its responsibilities, the People's Bank of China strives to establish and improve the institutional system for protecting the rights and interests of financial consumer information. This is its basic responsibility as the main body of financial consumer rights protection supervision, and it also provides an

institutional basis for its further implementation of regulatory functions.

B. Strengthen guidance and supervision of banking institutions

Strengthening guidance and supervision of banking institutions is the key to ensuring the standardization of banking behavior. Banking financial institutions must protect the personal data of financial consumers in accordance with the relevant provisions of the implementation measures for the protection of financial consumer rights and interests. However, it is obviously unrealistic to rely solely on the initiative and consciousness of banks. Therefore, it is necessary to rely on external regulatory forces to ensure the security of personal data of financial consumers. Regulatory agencies should supervise and manage the implementation of commercial banks in protecting the security of personal data of financial consumers. Regulatory bodies need to supervise not only the business activities of commercial banks, but also the financial consumer personal data security protection system involved in their business processes and its implementation. In actual work, regulatory agencies supervise the information security of financial consumers through supervision and inspection. Whether it is on-site supervision or off-site supervision, "external physical examinations" should be conducted on the main responsibilities of banking financial institutions in protecting the personal data of financial consumers in order to effectively discover and solve problems.

C. Strengthen cooperation with other data security and information protection authorities

To provide a good regulatory environment for the protection of personal data of financial consumers under the development of open banking, it is necessary to strengthen cooperation with other competent authorities for data security and information protection. The development of open banking involves the circulation and processing of personal data of financial consumers between different industries and information processing entities. This is the biggest challenge to protecting the security of personal data of financial consumers and an important challenge to the performance of the duties of regulatory entities. Therefore, when improving the duties of regulatory entities, it is necessary to cooperate with regulatory departments of other industries and regions to establish a regulatory and law enforcement cooperation mechanism for the protection of personal data of consumers, strengthen the supervision of personal data of financial consumers across markets, industries and regions, and realize communication and cooperation between regulatory entities in personal data sharing and protection of personal data of financial consumers.

D. Raising the cost of illegal activities for financial institutions

Increase the crackdown on behaviors that infringe on the personal data security of financial consumers, and at the same time strengthen the personal data security education of financial consumers to improve the self-protection awareness of financial consumers. In the process of supervision, once the regulatory authorities find any behavior that infringes on the personal data rights of financial consumers, they should impose penalties in accordance with the law to increase the cost of illegal behavior of financial institutions. When conflicts arise between financial consumers and banking financial institutions over the protection of personal financial data, the regulatory authorities should establish a non-litigation third-party resolution mechanism to reduce the cost of dispute resolution. In addition, the regulatory authorities should also strengthen risk warnings and risk education for personal financial data protection. With the development of open banking, the spread of personal data sharing will accelerate, and related risks will gradually increase. Therefore, regulatory authorities need to carry out risk warnings and safety education while commercial banks develop open banking business to enhance consumers' risk prevention awareness and ability.

References

[1] Zhang Jian. China's open bank data sharing supervision mode choice [J]. Political Science and Law Series, 2023,(01):65-76.
[2] Liu Hui, Jiang Lili. Data risk of open banks and its legal prevention [J]. Journal of Hebei University of Science and Technology (Social Science Edition), 1-10.
[3] Wen Shuying. British experience and enlightenment of open banking supervision [J]. Journal of Shanxi University (Philosophy and Social Sciences Edition), 2023, 46(02): 152-160.
[4] Xuan Xuan, Fang Yan. Risk challenges and legal regulation of data sharing in China's open banks [J]. Credit Information, 2022, 40(07): 39-44.
[5] Yang Xue, An Xuemei. Open banking practice: data portability and its regulatory logic [J]. Financial Economics Research, 2021, 36(02): 132-142.
[6] Guo Li. The "exquisite" approach to personal financial data governance in the digital age [J]. Journal of Shanghai Jiaotong University (Philosophy and Social Sciences Edition), 2022, 30(05): 15-27.
[7] john young. Research on data sharing mechanism in financial supervision [J]. Financial Supervision Research, 2019, (10): 53-68.
[8] Wu Di, He Linhua. Legal Research on the Utilization of Personal Financial Information of Commercial Banks in the Digital Age [J]. Liaoning Economy, 2023,No. 460(01): 62-68.
[9] Zhou Kunlin, Wu Zhongqi. Dilemma and legal response of personal data protection obligations of financial institutions [J]. Journal of Yangtze University (Social Science Edition), 2023, 46(01): 90-97.
[10] Xing Huiqiang. Positioning and orientation of personal financial information protection law [J]. Contemporary Law, 2022, 36(03): 100-112.
[11] Li Yumeng. Exploring the path of open banking supervision-from the legal boundary between the government and the market [J]. Liaoning Economy, 2022, (04): 86-92.
[12] Wang Zhipeng, Long Haiming, Li Jiake. Legal and economic thinking on Internet financial supervision [J]. Financial Theory and Practice, 2017, 38(04): 9-14.
[13] Wang Yuyu. The legal and economic analysis of the oversupply of China's financial supervision system [J]. Modern Law, 2014, 36(05): 61-69.
[14] Yang Wang, Wang Sister-in-law. Open Bank International Paradigm and China Practice [J]. China Finance, 2019(11): 24-26.