Research on Multi-subject Governance of Personal Information Security in Internet Finance: Based on CNKI Database

Ziman Liu[1,a,*], Jiafeng Liu[2,b]

[1]Business School, China University of Political Science and Law, No. 25, Xitucheng Road, Beijing, China

[2]Human Resources Department, Baoding Xinao Gas Co., Ltd., No. 606, Xiangyang South Street, Baoding, China

[a]maner1107@163.com, [b]liujiafeng@enn.cn

*Corresponding author

Keywords: Internet Finance, Personal Information Security, Financial Security, Multi-subject Governance, Financial Information Governance

Abstract: With the rapid development of internet finance, while it brings huge economic benefits, it also faces huge security problems for the personal information that is processed in large quantities. At this stage, the research on personal information security on the internet is still characterized by decentralization and fragmentation. Using systematic review and literature analysis methods, this paper studies and analyzes the personal information security problems and countermeasures of 21 literature based on CNKI core database. It is concluded that personal information leakage has become a basic problem in internet finance personal information security, which needs to be solved through a governance system with the participation of multiple subjects. Based on the analysis of existing literature, this paper proposes a multi-subject governance system for Internet financial personal information security.

1. Introduction

With the application of big data, blockchain and other information technologies in the information age, the Internet economy is in the ascendant, especially the financial sector has ushered in a new round of expansion. However, while information technology brings development opportunities to finance, it also brings new challenges, especially the problem of information security. On October 8, 2021, the US trading platform Robinhood published a blog about data security incidents, revealing that the system of the platform was invaded and leaked the personal information of a total of 7 million users. In April 2021, the *Economic Information Daily* reported that billions of personal information were traded on platforms such as dark-net and Telegram[1].

In order to protect the rights and interests of personal information, on August 20, 2021, the Standing Committee of the National People's Congress passed *the Personal Information Protection Law of the People's Republic of China* (hereinafter referred to as *the Personal Information Protection Law*); On November 11, *the Resolution of the Central Committee of the Communist Party of China on Major Achievements and Historical Experience of the Party's Centennial Struggle* also pointed out that in the financial field, we should "comprehensively strengthen financial supervision, prevent and resolve risks in the economic and financial field, and strengthen market supervision and anti-monopoly regulation"[2]. However, at this stage, there is less research on personal information security under the internet finance. Through literature search, it is found that relevant or similar studies show the characteristics of dispersion and fragmentation, and lack of overall analysis and research on this problem. In view of this, this research will adopt the research methods of systematic review and literature analysis, based on the sorting and analysis of existing literature, summarize and find out the main problems faced by personal information security in the context of internet finance, and preliminarily discuss the governance based on multiple-subjects system.

  DOI: 10.25236/iche.2022.067

2. Analysis of information security problems and countermeasures

2.1. Data acquisition and research samples

Data acquisition first needs to determine the database to be used. Based on the relatively rapid and leading development trend of internet and industrial integration in China, China is selected as the large country background, and CNKI is used as the literature source database. Specifically, in order to avoid the omission of documents caused by keyword matching in the retrieval process as much as possible, and maintain the matching degree between the retrieved documents and the research topic as much as possible, the retrieval is carried out with "internet financial information security" as the topic word and the secondary retrieval is carried out with "internet financial information risk" as the topic word, and the literature results of the two searches are integrated, eliminate the duplicate literature, and obtain 21 effective literature as the research samples. Due to the small number of literature, no time conditions were set in the screening process, and the selected literature were distributed from 2014 to 2021.

From the literature, it is found that these studies are not all directly concerned with the security of internet financial personal information. Most studies delimit the research scope as "internet financial information security", and study the security of personal information as one of them. There are also some studies that involve security or risk issues in the process of focusing on financial information technology or supervision. Therefore, for the above 21 literature, according to the research purpose, only the part of the literature related to the security of internet finance personal information is studied, which is mainly the existing security problems and coping strategies for security problems, and the rest are not paid too much attention.

2.2. Safety problem analysis

At present, it is widely considered that the most serious problem in the field of personal information security of internet finance is the leakage of personal information. The other problems include the loss and tampering of personal information, virus intrusion, hacker attack, technical phishing, personal information problems caused by operation, etc. For details, please refer to Table 1.

Table 1 Sorting of safety problems.

Safety Problem	Authors and Literature
Personal information leakage	Ning et al[4]; Pan[5]; Wang[6]; Jin[7]; Zeng et al[8]; Peng[9]; Wang[10]; Liu et al[11]; Research Group of the Central Sub-branch of the Zhongguancun National Independent Innovation Demonstration Zone of the People's Bank of China[12]; Zhao et al[13]; Du[14]; Sherman et al[15]; Chen et al[16]; Zhao[17]
Operational problems	Ning et al[4]; Zhao et al[13]; Sherman et al[15]; Chen et al[16]
Loss of personal information	Chen et al[16]
Personal information tampering	Chen et al[16]
Virus invasion	Zhao et al[13]
Hacker attack	Ning et al[4]; Zhao et al[13]
Technical fishing	Chen et al[16]

Personal information leakage mainly refers to the information about the users' personal identity stored in the user database of internet financial institutions, including name, gender, date of birth, ID number, mailing address, contact number, etc,processing by a third party other than the user and the Internet financial institution authorized by the user to process its information. The more common hazards caused by personal information leakage include financial account theft, targeted fraud based on personal financial characteristics, false information induction, and profit-making by selling information. The reasons for the leakage of personal information come from both technical and institutional levels. The personal information leakage at the technical level is mainly due to the poor construction of the information security system of internet financial institutions, and the failure to

fight against network attacks, resulting in the attackers successfully steal users' personal information; the institutional level is mainly due to the poor construction of the information security system, which fails to prevent or timely stop the negligent operation of insiders or the subjective theft of insiders, resulting in the active outflow of users' personal information from the internet financial institutions.

The personal information security problems caused by operation mainly come from the internal personnel of financial institutions. Because internet finance relies on the development of electronic information technology, the internet finance model itself has the characteristics of technology and virtualization. When dealing with the users' personal information, internal personnel inevitably make mistakes in the process of operating the information terminal, which threatens the users' personal information security to a certain extent. In addition to the subjective factors of internal personnel, the defects and loopholes in the design of the operating system will also increase the probability of misoperation, or the security of users' personal information due to design problems in the process of system self-processing.

The loss and tampering of personal information are the security consequences caused by the network attack or misoperation of the users' personal information. The purpose of network attack against personal information is not only to steal the users' personal information, but also to delete or tamper with the users' personal information out of subjective malice. The misoperation of internal personnel or the system itself can also lead to the loss or tampering of users' personal information, resulting in problems caused by users' failure to use services normally or loss of funds.

Virus intrusion, hacker attack and technical phishing are all means to threaten users' personal information security and lead to personal information security problems. For illegal profit-making or other purposes, subjective malicious third parties launch attacks on internet financial institutions that store users' personal information through virus intrusion and hacker attacks, so as to steal, delete or tamper with users' personal information. The third party can also turn the attack target from internet financial institutions to users, and induce users to enter personal information on unofficial sites by designing malicious mobile phone apps and high imitation phishing websites, so as to complete the collection of users' personal information; or directly intercept the users' payment through technical means, so that the user can directly pay the proposed payment to the account established by the third party, so as to complete the theft of user account information and funds.

2.3. Coping strategy analysis

After clarifying the security problems of internet financial personal information, the discussion on security countermeasures has become an essential research content. According to the classification of the subjects implementing the response strategies, government departments such as legislative bodies, administrative bodies and financial regulators, internet financial institutions, financial industry and other market departments are involved. For details, please refer to Table 2.

Table 2 Coping strategies.

Behavior Subject	Author and Literature
Legislature	Ning et al[4]; Pan[5]; Zeng et al[8]; Peng[9]; Wang[10]; Sherman et al[15]; Chen et al[16]; Liu[18]
Administrative organization	Zeng et al[8]; Sherman et al[15]
Financial regulators	Zeng et al[8]; Peng[9]; Wang[10]; Zhao et al[13]; Sherman et al[15]; Chen et al[16]; Zhao[17]
Internet financial institutions	Ning et al[4]; Pan[5]; Wang[6]; Jin[7]; Zeng et al[8]; Peng[9]; Liu et al[11]; Zhao et al[13]; Du[14]; Sherman et al[15]; Chen et al[16]; Liu[18]
Financial industry	Sherman et al[15]

The biggest mission of the legislature to participate in the protection of personal information of internet finance is to clarify the processing of personal information and relevant supervision and punishment by means of legislation. At present, the formal implementation of *the Personal Information Protection Law* also responds to the call for the establishment of a special law for personal information protection. On this basis, the legislature should also gradually coordinate and

straighten out the relationship between laws and regulations, continuously guide internet enterprises to protect the security of their information systems through legal means, and sort out the legal awareness of employees in the internet financial industry.

Administrative agencies mainly participate in dealing with personal information security issues by refining functions and subdividing fields, setting up new specialized agencies and strengthening personal information security education for users. These measures mainly rely on the leading position of administrative institutions in market and social management.

In view of the small-scale and decentralized establishment of institutions in the internet financial industry, financial regulators need to make use of resources and regulatory advantages to promote the establishment of safety standards for the internet financial industry and guide industry self-discipline; lead the establishment of information security monitoring system, data storage and backup system. In the exercise of regulatory functions, we should strengthen supervision, severely investigate and crack down on violations of personal information security.

In the protection of users' personal information security, information security guarantee system and risk assessment and early warning system are necessary, which requires internet financial institutions to strengthen security technical means to prevent malicious attacks; we should also improve the internal control system, establish a data approval and key mechanism, strengthen the supervision of internal personnel, and improve the risk awareness and management level of internal personnel. Once a users' personal information security problem occurs, internet financial institutions should also provide emergency services combining online and offline, cooperate with users to quickly complete information modification, account freezing and other matters, and ensure the safety of users' personality and property.

The financial industry needs to play its role as a link to help coordinate the relationship between banks, internet financial institutions and financial regulators, strengthen industry self-discipline and guide the formation of an industry atmosphere that attaches importance to the protection of users' personal information.

3. Characteristics of information security issues: information leakage has become a basic problem

From the analysis of relevant security issues, it can be found that the most basic problem of personal information security in the field of internet finance at this stage is personal information disclosure, and other operational errors, hacker attacks and other problems all focus on personal information disclosure. Figure 1 shows the ways and purposes of personal information disclosure.

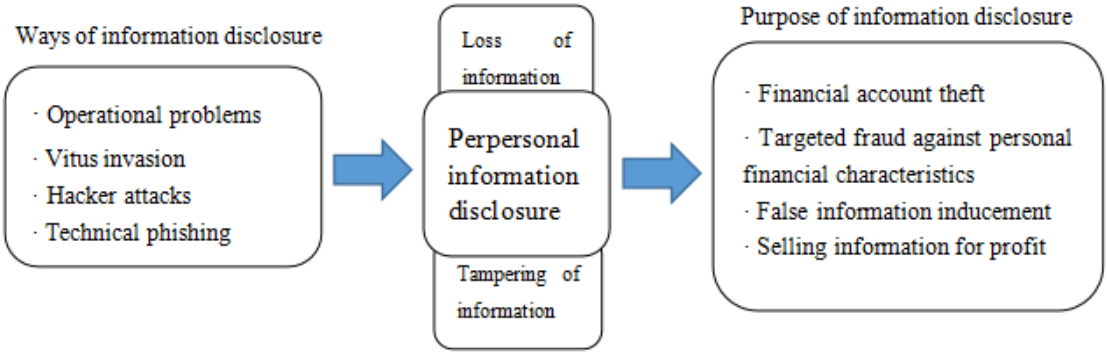

Figure 1 Security problems surrounding personal information leakage.

Operational problems, virus intrusion, hacker attacks and technical phishing are all ways to lead to personal information disclosure. Malicious third parties, including internal and external personnel of internet financial institutions, gangs and organizations, may steal users' personal information from the sites where users' personal information is stored through technical or non-technical means, resulting in the disclosure of users' personal information. The targets of these pathways are also different. Operational problems mainly affect the internal of internet financial institutions and disclose personal information through the subjective or unintentional operation of internal personnel;

virus intrusion and hacker attack mainly attack information nodes through technical means, or intercept information in the process of transmission and steal users' personal information, which is "technical war"; technical phishing induces the user to voluntarily provide personal information without knowing the truth by cheating and cheating the user, so as to defraud the users' personal information.

The loss and tampering of personal information are mostly based on personal information disclosure. The loss and disclosure of personal information is mainly due to the malicious third party deleting or modifying the users' personal information stored in the information node of internet financial institutions, and the operation of deleting or modifying information must be based on the exposure of the original information. Once a users' information is known or obtained by a third party other than the user and the internet financial institution authorized by the user to process his personal information, personal information disclosure occurs.

Stealing users' personal information leads to the disclosure of users' personal information. The ultimate purpose is to illegally infringe on users' property based on users' personal information. These behaviors include financial account theft, targeted fraud against personal financial characteristics, false information inducement, selling information for profit, etc. Account theft is one of the possible serious consequences of personal information disclosure, especially after the disclosure of user account information, which will make the funds in the users' internet financial account be looted, resulting in all losses of account property. Targeted fraud and information inducement may enable the user to transfer part of the funds to a third party, resulting in part of the loss of account property. The single act of selling users' personal information will not have a direct impact on users' property, but information buyers often use the purchased personal information to carry out illegal infringement against users' property, resulting in damage to users' property.

4. Multi subject governance path of personal information security

Multi subject governance originates from the polycentric governance theory jointly founded by Elinor Ostrom and Vincent Ostrom[18]. They believe that both the government and the market have failures in the governance process of public affairs. Therefore, the "single center" governance model of simply governing public affairs by the government or the market needs to be transformed into a three-dimensional joint governance model of government, market and society.

The multi subject governance system of internet financial personal information security also adheres to the concept of independent decision-making and collaborative cooperation. On the basis of including the original governance subjects such as legislative institutions, administrative institutions, financial regulators, internet financial institutions and financial industry, it also includes multi governance subjects such as judicial institutions, National Internet information departments, social and social groups and individual users. Figure 2 shows the multi-subject governance system.

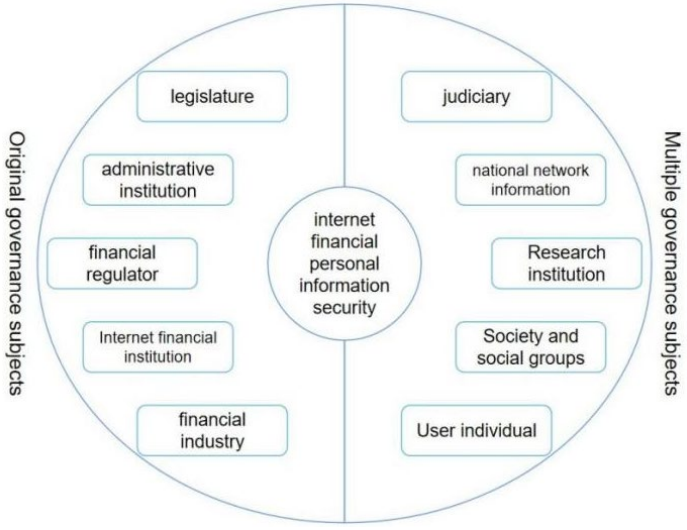

Figure 2 Multi-subject governance system.

4.1. Original governance subjects

The legislature plays a leading role in all governance subjects. The development of the internet financial industry, as well as the resulting governance problems and their solutions need to be clarified by law. Therefore, the most urgent task for the legislature is to improve the existing laws, formulate new laws, and coordinate the relationship between laws, so as to provide basis and guidance for solving the problem of personal information security on the Internet. At this stage, China has initially established a legal system to protect personal information. *The network Security Review Measures Officially* implemented on February 15, 2022 will also further strengthen the barriers to the protection of Internet personal information at the level of administrative regulations.In addition to formulating relevant legal provisions, the legislature also shoulders the responsibility of guiding internet finance to pay attention to personal information security and promoting practitioners to establish legal awareness through legislation.

Administrative institutions need to carry out personal information security publicity through their huge administrative network and do a good job in law popularization, so as to effectively improve the personal information security awareness of all citizens. In the process of popularizing the law on personal information protection, adopting different forms of popularizing the law for different objects will help to achieve good results.

Financial regulators are mainly responsible for regulatory functions, and jointly establish an information regulatory system led by themselves with internet financial institutions.The information supervision system should include technical system and management system.The technical system shall include a complete set of financial information supervision system connecting all internet financial institutions. By strengthening the supervision of information security protection of internet financial institutions, it can guide and stimulate them to continuously enhance their ability of information security protection.The establishment of the management system needs to strengthen guidance through institutional means, formulate standard actions for personal information processing, and prevent and deal with the leakage of users' personal information caused by operational problems.

Internet financial institutions are important subjects in the governance system, and their governance measures can be divided into three stages: before, during and after. Prevention is the main stage in advance.This requires internet financial institutions to establish a sound risk early warning and prevention mechanism, strengthen the information security protection ability of their own platform through technical means, prevent malicious attacks against information nodes, upgrade the encryption technology in the process of data collection and transmission, and prevent information from being intercepted; through system construction, establish a sound information security emergency plan, implement identity authentication, information approval and key system, strengthen and improve the supervision of internal personnel, and improve the operation level of information processing. In the process stage, rapid response is the main.In terms of technology, we should design a complete attack and countermeasures system and provide perfect anti fraud services;In terms of services, we should set up a green channel, which should not only actively discover, freeze and deal with users' personal information security problems, but also provide users suffering from information security problems with fast online and offline processing windows, so as to facilitate users to stop losses in time. The post event stage is mainly to make up for losses. We should innovate insurance products to insure users' personal information and related properties to make up for users' subsequent losses; internet financial institutions can also share IP addresses and users with potential security risks by establishing a blacklist system; through the case publicity of security problems that have occurred, strengthen the publicity to the users receiving services, and help improve the users' awareness of personal information security risk prevention.

The financial industry will play a more advocacy role, promote the self-discipline of the internet financial industry, coordinate the interests and relations of all parties, and undertake the task of connecting the preceding and the following and connecting the left and the right.

4.2. Multiple governance subjects

The judiciary should undertake the work of the legislature and punish individuals or organizations

who infringe personal information in accordance with the laws promulgated by the legislature. This is exactly complementary to the work of financial regulators. Financial regulators mainly focus their supervision and punishment on the object of information security problems - internet financial institutions. Judicial institutions mainly focus their supervision and punishment on the subject of information security problems - malicious third parties. It can be said that they cooperate with each other to deal with personal information security problems from both ends.In the process of sentencing cases of infringement of personal information, the judiciary can also provide reference for the judgment of subsequent personal information security cases by forming precedents.

The national network information department is a special department in the administrative organization responsible for overall coordination of personal information protection and relevant supervision and management. Network information departments at different levels perform their duties of personal information protection within the framework of relevant laws and administrative regulations. The national network information department protects the security of personal information by carrying out publicity and education on personal information protection, receiving reports, organizing evaluation, investigating and dealing with illegal activities, and can also coordinate relevant departments to promote personal information protection by formulating rules, establishing detailed rules, supporting research, promoting services, improving working mechanisms, etc. The Internet not only plays an important role in the specific governance of the national information sector, but also plays an important role in the security of the entire information sector.

Scientific research institutions also play an important role in the governance system. In order to improve their management and prevention ability, financial regulators, internet financial institutions and other subjects have great demand for information security technology, and most of these needs need to be met by scientific research institutions. Scientific research institutions should give full play to their knowledge advantages, deeply study information security technology, and provide technical weapons for other subjects to carry out personal information protection. In addition to technology, the management knowledge produced by scientific research institutions will also effectively provide reference and guidance for other subjects to design and improve the system more conducive to the protection of personal information.

As a flexible subject, society and social groups can undertake a variety of functions in governance. The most common is to help promote the publicity of personal information protection. At the same time, society and social organizations can also cooperate with the governance behavior of other subjects by means of disclosure, independent innovation, funding research and participating in evaluation, so as to enhance the breadth and depth of governance and improve governance efficiency.

As the "victim" of personal information security, the most important thing for users is to improve their awareness of information security, not provide their own personal information at will, beware of being deceived, do a good job in the publicity of people around them, and jointly reduce the harm of personal information security.

4.3. Cooperation among subjects

The cooperation among the main bodies is mainly carried out in three aspects: technological innovation, supervision and management and safety publicity. In terms of technological innovation, scientific research institutions, as the main force, produce information security knowledge and technology on the basis of receiving project funding or spontaneous research from other subjects; financial regulators, internet financial institutions and other entities apply emerging technologies to improve their own information security protection systems and systems, and build a more convenient, efficient and secure internet financial platform. In terms of supervision and management, legislative bodies, administrative bodies, National Internet information departments and other departments have the right to establish laws and administrative regulations to provide basis for the supervision, management and punishment of other subjects by formulating various rules; judicial institutions, financial regulators and other subjects supervise and manage the personal information processing behavior of internet financial institutions and users, and punish the illegal infringement of personal information by malicious third parties.In terms of security publicity, all subjects can and have the

responsibility to carry out personal information security publicity and education, promote internet finance practitioners to establish risk prevention and legal awareness, improve users' personal information security awareness, and establish the wind of personal information protection in the whole society.

References

[1] Economic Information Daily. (2021) Billions of personal information marked "hidden rules" are popular, and sales are rampant. Retried from http://dz.jjckb.cn/www/pages/webpage2009/html/2021-04/19/content_73288.htm.

[2] n.a. (2021) Resolution of the CPC Central Committee on the major achievements and historical experience of the party's hundred year struggle. People's daily, 2021(01).

[3] Ning, Y, Yao, M.F. (2020) Research on green financial information risk and prevention system under the background of "mass entrepreneurship and innovation", Information science, 38(10), 148-153.

[4] Pan, Q. (2020) Construction and optimization path of internet financial consumer protection system in China. Economic System Reform, 2020(01), 196-200.

[5] Wang, Z.C. (2019) Analysis on the blockchain model of personal credit investigation system alliance in the Internet era. Credit Investigation, 37(08), 26-32.

[6] Jin, Y.H. (2018) Research on internet financial information security prevention and guarantee system under big data environment. Information Science, 36(12), 134-138.

[7] Zeng, D.H., Liu, Z.Y. (2018) Internet financial personal information security and its governance. Shanghai Finance, 2018(01), 91-95.

[8] Peng, X.J. (2017) Legal approach to the supervision of Internet investment and financing platforms Journal of Central South University for Nationalities (Humanities and Social Sciences), 37(05), 152-155.

[9] Wang, S.Z. (2017) Legal prevention and control of internet financial information risk. Contemporary Economic Management, 39(06), 81-85.

[10] Liu, G.C., Wang, Y.T. (2017) Research on internet financial information security audit based on process mining. Journal of Xinjiang University (Philosophy, Humanities and Social Sciences), 45(03), 18-25.

[11] Research group of Zhongguancun national independent innovation demonstration zone central sub branch of the People's Bank of China, Li, Y.X. (2016) Impact of internet consumer finance on traditional consumer finance: Competition and cooperation. Southern Finance, 2016(12), 57-63.

[12] Zhao, D., Zhang, H.Y. (2015) Construction and implementation path of internet financial audit and supervision system. Monthly Journal of Finance and Accounting, 2015(25), 45-47.

[13] Du, Y.H. (2015) Research on the development countermeasures of internet finance in the era of big data. Price Theory and Practice, 2015(07), 109-111.

[14] Sherman, Huang, X., Zhou, Y. (2015) Analysis of network security and information security elements of internet finance. Journal of Shanghai University (Social Science Edition), 32(04), 27-36.

[15] Chen, Y.D., Qiao, G.M. (2015) Research on information security risk prevention under the mode of "Internet plus finance". Journal of Suzhou University (Philosophy and Social Sciences Edition), 36(06), 124-130+200.

[16] Zhao, Y.J. (2014) Research on the development and supervision of third-party Internet payment business. Southern Finance, 2014(04), 17-19.

[17] Liu, H.E. (2014) Mobile payment: Principle, mode, typical cases and financial supervision. Southwest Finance, 2014(05), 61-64.

[18] Li, P.Y. (2014) On the applicability and limitations of Ostrom's multicentric governance theory, *Tribune of Study*, 30(05), 50-53.