Evolutionary Game Research on Personal Data Protection and Utilization by Internet Companies - Wang Ning

Authors: Wang Ning, Wang Ning

Date: 2022-09-03T00:00:00+00:00

Abstract

Purpose/Significance: The advancement of internet technology has made personal data increasingly important as a production factor, with its value potential and energy function becoming more evident. Exploring how to achieve a balance between personal data protection and utilization has become a critical challenge in digital economy development and data governance. Method/Process: This paper takes personal data protection and utilization as its research subject, constructs an evolutionary game model between internet platforms and the government, explores the behavioral characteristics and stable strategies of the participating entities, and uses MATLAB numerical simulation technology to conduct simulation analysis of the evolutionarily stable strategies of the participating entities under different circumstances, and proposes solutions to personal data protection issues. Results/Conclusions: Research shows that government regulatory costs, strength of reward-punishment mechanisms, level of industry association participation, data sensitivity, and enterprise data protection technology costs are important factors affecting the strategy choices of both parties. Therefore, to achieve the dual Pareto optimality of the ideal evolutionary equilibrium between data protection and utilization, the government should actively explore the modernization of regulatory systems and institutions, improve regulatory effectiveness, reduce regulatory costs, perfect data classification and grading ex-ante, ensure policy implementation during the process, and provide incentives and accountability for non-compliant enterprises ex-post; internet enterprises should strengthen industry self-discipline and technological innovation to reduce enterprise data protection costs.

Full Text

Preamble

Research on the Evolutionary Game of Personal Data Protection and Utilization by Internet Enterprises

Wang Ning; Zhang Min
School of Management, Hebei University
Baoding, Hebei 071002

Abstract

[Objective/Significance] Advances in internet technology have made personal data increasingly important as a production factor, with its value potential and energy function becoming more apparent. Exploring how to achieve a balance between personal data protection and utilization has become a critical challenge for digital economy development and data governance. [Method/Process] This paper takes personal data protection and utilization as its research object, constructs a two-party evolutionary game model between internet platforms and government, explores the behavioral characteristics and stable strategies of participating actors, and uses MATLAB numerical simulation technology to simulate the evolutionary stable strategies of participants under different conditions, proposing solutions to personal data protection issues. [Results/Conclusions] The study shows that government regulatory costs, reward and penalty intensity, industry association participation level, data sensitivity, and enterprise data protection technology costs are important factors affecting the strategy choices of both parties. Therefore, to achieve the dual Pareto optimality of the ideal evolutionary equilibrium for data protection and utilization, the government should actively explore the modernization of regulatory systems and institutions, improve regulatory efficiency, reduce regulatory costs, improve data classification and grading beforehand, ensure policy implementation during the process, and provide incentives and accountability for non-compliant enterprises afterward. Internet enterprises should strengthen industry self-discipline and technological innovation to reduce enterprise data protection costs.

Keywords: digital economy, internet enterprises, personal data protection, evolutionary game
Classification Number: G252

In the era of big data, data is regarded as a new type of production factor and an important economic resource. Currently, internet platforms in various fields such as social networks, short videos, and e-commerce all possess vast amounts of commercial data including consumer transaction records and online behaviors, making the protection of user personal data imperative. The internet industry has also actively introduced self-discipline treaties to urge internet enterprises to attach importance to personal data protection. China’ s “Internet Industry Self-Discipline Convention” stipulates: “Consciously protect the legitimate rights and interests of consumers, keep user information confidential; do not use information provided by users to engage in any activities unrelated to commitments made to users, and do not use technical or other advantages to infringe upon the legitimate rights and interests of consumers or users" [1]. However, news reports show that various incidents of internet user personal data leakage emerge endlessly. Some internet platforms, institutions, and even individuals, driven by profit, excessively utilize and illegally trade personal data, causing distress and infringement to netizens' data rights and interests. In January 2021, the Ministry of Industry and Information Technology reported on 157 APPs involved in personal data infringement incidents, announcing issues such as inadequate implementation of platform main responsibilities by Tencent App Store, Xiaomi App Store, and Huawei App Market, and illegal processing of personal information. Personal data protection has become the most urgent basic issue in public social life. Whether individuals, internet platforms, or the government as the main regulator of the digital market, all have recognized that the cornerstone of digital economy development lies in the benign interaction between data utilization and data protection. Exploring how to construct a personal data protection order has become a fundamental task for digital economy development.

Meanwhile, conflicts of interest among various stakeholders in the personal data protection process have become increasingly prominent, largely restricting the development of the data economy. Users, as data producers, claim personality rights and interests over their personal data; internet platforms, as the largest data controllers, have their core interests reflected in property rights over data; local governments, as data supervisors, mainly represent social public interests. In the process of personal data protection and utilization, internet platforms and government are the participating actors, and one party' s strategic choice will inevitably be influenced by the other' s strategic choice. This is a long-term dynamic process where participating actors continuously adjust their strategy choices based on the other party' s choices and various factors, ultimately achieving an interest equilibrium among all parties in the personal data protection and utilization process. As a game theory analysis method for dynamic evolutionary processes, evolutionary game theory can analyze key factors such as benefits and costs of various decision behaviors from an economic perspective, and has good applicability to personal data protection strategy choice issues.

1.1 Research on Personal Data Protection

Personal data protection is a typical interdisciplinary research issue, with disciplinary penetration ranging from social sciences to natural sciences, including economics, management, law, computer science, library and information science, and other fields. From the research results of various disciplines, personal data protection research is mostly concentrated in the legal field. In the legal field, discussions on personal data protection paths mainly include the following two aspects: one is granting rights to data subjects, and the other is protecting data controllers and regulating their behavior.

Scholars holding the rights-granting protection viewpoint attempt to incorporate data into the "rights-based" legal protection objects, thereby granting data right holders control and dominion over data, advocating treating data as objects in civil law, constructing a complete data rights system for them, and granting data subjects corresponding data rights [2]. Data rights-granting can draw clear boundaries between data-related rights and others' behavioral freedom, reduce public information costs, provide reasonable behavioral expectations for data users, and ensure legal stability [3]. In view of this, many scholars have constructed complex data rights systems. From the perspective of data rights subjects, data rights include national data rights, enterprise data rights, and personal data rights. However, some scholars believe that mandatory use of rights-granting protection would excessively hinder the operation of data markets, improvement of data technology, scientific research, and data sharing, advocating for the construction of another data subject rights protection mechanism, shifting from a "rights norm model" to a "behavior control model" [4].

1.2 Related Research on Evolutionary Game in Data Protection

Achieving a balance between data protection and utilization most importantly requires resolving conflicts of interest among multiple actors to reach a stable cooperative behavior. Currently, some scholars have introduced evolutionary game methods into data protection and utilization research to explore the long-term dynamic decision-making process of participants. Internet platforms and government are important actors in data collection, utilization, and supervision. Ho T Y et al. used evolutionary game theory to construct a game model between patients and medical service institutions to help medical institutions make optimal decisions regarding data protection [5]. In China, Feng M N constructed a privacy game model between users and social platforms. The results showed that user trust, social platform influence, rewards, and supervision are key factors affecting the evolution of privacy strategies for users and social platforms, and proposed corresponding countermeasures and suggestions for social network privacy protection [6]; Wei Y H et al. constructed a non-cooperative evolutionary game model between information subjects and the data industry, proposing that government supervision mechanisms, judicial responsibility systems, and internal governance of the data industry are key factors affecting the behavioral decisions of both game parties [7]. In addition, there are studies on cooperation strategy games between network content providers and service providers [8], privacy protection investment strategy games between social network platforms and users [9], and strategy games between social network service providers and users based on privacy issues [10]. Zhou M constructed an evolutionary game model regarding personal data protection and use between over-collecting APPs and [government], proposing that enterprise data protection costs, government regulatory costs, and user data leakage sensitivity are key factors affecting government and enterprise decisions [11].

In summary, combining evolutionary game methods to study the interest balance in data protection and utilization, the main factors affecting game actors'decisions are: from the government actor perspective, regulatory mechanisms, judicial mechanisms, reward and penalty intensity, regulatory costs, and benefits; from the enterprise actor perspective, mainly considering enterprise data mining costs and benefits, enterprise self-discipline costs, and data protection costs; from the user actor perspective, mainly considering user trust in enterprises, user sensitivity to information leakage, and risk perception. Currently, there are few studies using game evolution methods from an economic perspective to explore decision-making games between government and enterprises. What impact will loose or overly strict government data protection policies have on data collection and utilization? What strategy choices will lead to costs and benefits in the long run? Therefore, we need to explore the influencing factors of internet enterprises' and governments' personal data protection behavioral decisions to promote data protection and utilization.

2.1.1 Basic Assumptions

Assumption 1: Game Actors. The game actors in data protection and utilization are internet enterprises and local governments. The behavioral strategy set of internet enterprises is self-discipline or non-self-discipline. Self-discipline refers to internet enterprises complying with legal regulations, fulfilling responsibilities and obligations, not excessively collecting or abusing user data, and ensuring user data security; the non-self-discipline strategy refers to internet enterprises excessively collecting user sensitive data and even causing user data leakage to maximize their own interests, infringing upon user data rights and other behaviors. The behavioral strategy set of local governments is strict protection or loose protection. Strict protection means prioritizing social security benefits, i.e., investing higher protection costs, strictly protecting internet platforms' personal data use, and imposing corresponding penalties for violations; loose protection means prioritizing social economy, i.e., investing lower protection costs and not regulating internet enterprises' non-self-discipline behavior. The probability of internet enterprises choosing self-discipline is x, and the probability of choosing non-self-discipline is 1-x; the probability of local governments adopting strict protection of data rights is y, and the probability of adopting loose protection of data rights is 1-y.

Assumption 2: When internet enterprises choose the "self-discipline" strategy, if the government chooses "strict protection," enterprises obtain fixed income from developing user data within legal limits (0W) and financial subsidies or rewards given by the government (H), and bear data protection obligations, paying data security protection costs (D). The government gains improved credibility due to strict protection of user data security (3W), obtains socio-economic benefits and security benefits created by enterprise self-discipline (4W), and pays rewards given to internet enterprises and regulatory costs and policy formulation costs for strict data protection (1C). If local governments choose "loose protection," internet enterprises only have fixed income and need to pay data security costs. Due to its inaction in "loose protection," the local government only obtains socio-economic benefits and security benefits created by enterprise self-discipline, and pays a small amount of data protection costs (2C).

Assumption 3: When enterprises choose the "non-self-discipline" behavioral strategy, they obtain not only fixed income from developing user data (0W) but also additional income from developing user sensitive data (1W), where additional income is related to the sensitivity of developed user data ( ), with more sensitive data yielding higher additional income. Simultaneously, if the government chooses the "strict protection" strategy, enterprises' non-self-discipline also bears the risk of reputation decline (S) and penalties (F) due to discovery and disclosure by the government, where is the probability of government and third-party industry associations jointly discovering enterprises' non-self-discipline behavior. The government side obtains credibility improvement (3W), economic benefits created by enterprises (5W), and penalty fees from internet enterprises' non-self-discipline behavior (F). If the government "loosely protects," enterprises only bear the risk of regulation and disclosure by industry associations (S ,), and the government side obtains socio-economic benefits created by enterprises (5W) and penalty fees from enterprises under industry association supervision (F).

The research variables and their meanings in this paper are shown in Table 1 . Table 1 Evolutionary Game Model Research Variables: When enterprises choose the "self-discipline" strategy, the fixed income from developing data, W0>0; When enterprises choose the "non-self-discipline" strategy, the additional income from excessively developing sensitive data; When enterprises choose the "self-discipline" strategy, the data security protection cost paid D; When enterprises choose the "non-self-discipline" strategy, the reputation and economic loss when discovered by the government; The sensitivity of enterprise-developed data, 0≤ $ $1; The financial subsidy or reward given by the government when enterprises choose the "self-discipline"strategy; The penalty fee when enterprises choose the "non-self-discipline" strategy and are discovered by the government; The credibility benefit obtained under the government' s "strict protection"strategy; The economic and security benefits created by enterprise self-discipline under strict government protection; The economic benefits created by enterprise self-discipline under loose government protection; The cost of the government' s "strict protection" strategy, C1>0 (policy formulation cost and regulatory cost); The cost of the government' s "loose protection" strategy, C2>0 (policy formulation cost and regulatory cost); The probability of discovering enterprise non-self-discipline behavior under the government' s "strict protection" strategy; The probability of discovering enterprise non-self-discipline behavior by third-party industry associations; , , .

2.1.2 Model Construction

Based on the above basic assumptions, construct the payoff matrix of the two-party game model of "internet enterprises and local governments," as shown in Table 2 . Enterprise Self-discipline (x) Table 2 Constructed Two-Party Game Model Payoff Matrix: Local Government Strict Protection (y), Local Government Loose Protection (1-y), W D H; Enterprise Non-self-discipline (1-x) W W C .

2.2.1 Enterprise Game Strategy Replication Dynamic Equation

Based on the above payoff matrix, the expected payoff when enterprises are self-disciplined xU, the expected payoff when enterprises are non-self-disciplined 1 xU , and the average expected payoff x can be obtained as: y W D x U . Enterprise game strategy replication dynamic equation: x U U x U U S F D.

2.2.1 Government Game Strategy Replication Dynamic Equation

Based on the above payoff matrix, the expected payoff when government adopts strict protection yU, the expected payoff when enterprises are non-self-disciplined 1 yU , and the average expected payoff gU are: x W C x W C y U . Government game strategy replication dynamic equation: y x H y U U y U U F W C.

3.2.3 Evolutionary Stability Analysis of Enterprise and Government Strategies

Based on the above replication dynamic equations, a two-dimensional dynamic system for the evolutionary game between internet enterprises and government can be obtained: x U U x U U S F D y U U y U U y x H F W C (,) (,) (,). Setting ( ) = 0 0 ( ) = dx dy dt dt, five equilibrium points of the system can be obtained: (0,0), (0,1), (1,0), (1,1), (M,N). Where (A,B) is H F F . Based on the above replication dynamic equations, a two-dimensional dynamic system for the evolutionary game between internet enterprises and government can be obtained. Therefore, the five equilibrium points of the system are (0,0), (0,1), (1,0), (1,1), (A,B). We respectively calculate the partial derivatives of x and y to obtain the Jacobian matrix J, and the five local equilibrium points are substituted into the Jacobian matrix. If the matrix satisfies two conditions, it is an evolutionary stable point of the game system, and the corresponding strategy is an evolutionary stable strategy. The conditions are: (1 2){ [y W C y x H (1 2)[(F W C. Based on the assumption conditions, the point where the game actors evolve from any initial intention after game evolution is only meaningful in two-dimensional space, so . Based on the above conditions, the stability analysis of the five local equilibrium points (0,0), (0,1), (1,0), (1,1), (A,B) is shown in Table 3 , where S F D , C D W C. Table 3 Stability Conditions for Equilibrium Points of Both Game Parties: (0,0) Det(J) (A+B)·(-D) (-B)·(C+D) = Tr(J) A+B-D -B+C+D; (1,1) [-(A+B)]·[-(C+D)] -A-B-C-D; (0,0) [-D(C+D)/C·B]·[-B(A+B)/A·D]; (1,0) (0,0); (1,1). Table 4 Stable Points of Both Game Parties: Det(J) (sign) Tr(J) (sign). Based on the evolutionary stable point results in Table 4, points (0,0) and (1,1) are two ESS equilibrium points, indicating that the replication dynamic curves of internet enterprises and government both converge to these two points. When the two replication dynamic curves converge to (0,0), enterprises and government respectively choose non-self-discipline and loose protection strategies. When the two replication dynamic equation curves converge to point (1,1), enterprises choose the self-discipline strategy and government chooses the strict protection strategy. The intermediate point E S F D) is the key point for determining the convergence probability of the two replication dynamic equation curves (0,0) and (1,1). As shown in Figure 1 [Figure 1: see original paper], if the initial probabilities of both game parties are near point E, changes in different parameters will alter the game evolution results. The final evolution result depends on the area S1 of region EFGHH and area S2 of region EFIH. When S1 > S2, enterprises evolve toward the non-self-discipline strategy direction, and government tends toward the loose protection strategy; when S1 < S2, enterprises evolve toward the self-discipline strategy direction, and government evolves toward the strict protection direction. The game evolution process between enterprises and government is shown in Figure 1.

F(0,1) I(1,1) G(0,0) H(1,0) Figure 1 Evolutionary Stable Phase Diagram of Strategy Choices for Internet Enterprises and Government.

Case 1: Stability Conditions: (α+C- W, 0<βF+S+D- 0<C+β)F-, when enterprises perceive that the payoff from self-discipline strategy is lower than that from non-self-discipline strategy, driving enterprises to choose excessive mining and development of user data, and when government’ s payoff from choosing strict protection strategy is less than that from loose protection strategy, the system’ s evolutionary stable strategy is (0,0), where enterprises choose the “non-self-discipline” behavioral strategy and government chooses the “loose supervision” behavioral strategy.

Case 2: Stability Conditions: λW-αS+αF+H 0,-H>D- 0>C+C-, when enterprises perceive that the difference between reward benefits obtained from government, data development benefits, and paid data development costs and data protection costs is greater than the difference between illegal data development benefits obtained when non-self-disciplined and paid data development costs, reputation loss when discovered by government or industry associations, and penalty fees, and when government chooses strict data protection, wins high public recognition of the department’ s work capability, and the difference between credibility benefits obtained, security benefits and socio-economic benefits created by enterprise self-discipline, and paid strict protection costs and rewards given to self-disciplined enterprises is greater than the difference between benefits and costs when choosing "loose protection," the system' s stable evolutionary strategy is (1,1), where enterprises choose the "self-discipline" behavioral strategy and government chooses the "strict protection" behavioral strategy.

To satisfy the stability condition λW-αS+αF+H, requirements are: data protection cost (D) is relatively small, government reward (H) is relatively large, probability of government or industry associations discovering enterprise non-self-discipline behavior is relatively large, government punishment of enterprises (F) is relatively large, thus enterprises tend to choose the "self-discipline" behavioral strategy. To satisfy the stability condition 0>C+C-, requirements are: government credibility benefits from strict protection (3W) are relatively large, cost of strict protection (1C) is relatively small, reward to self-disciplined enterprises (H) is relatively small, thus government tends toward the "strict protection" behavioral strategy.

3 Numerical Simulation

This paper uses Matlab programming for numerical simulation to further demonstrate the evolution trajectory of the above game actors toward (1,1), while analyzing the impact paths of changes in penalty intensity F, reward intensity H, government regulatory capacity , and third-party industry association participation level on the stability of both game parties.

3.1 Equilibrium Point (1,1) Simulation Analysis

Based on the stability conditions of equilibrium point (1,1) λW-αS+αF+H (0,-H>D- and China' s legislative practice, parameters are assigned values as shown in Table 5 .

Table 5 Initial Values for Simulation:)0>C+C-. Figure 2 [Figure 2: see original paper] (1,1) Simulation Results. As shown in Figure 2, when the probabilities of both game parties (x,y) take different initial values, after long-term repeated games between enterprises and government, the final game evolution result converges to point (1,1), i.e., enterprises choose the "self-discipline" strategy and government chooses the "strict protection" strategy. The simulation analysis results are consistent with the above theoretical derivation results.

3.2 Different Penalty Intensity F

To further analyze the impact of different penalty intensity changes on the game results between enterprises and government, numerical simulations are conducted with F=30, F=50, and F=100 respectively. As shown in Figure 3 [Figure 3: see original paper], when other conditions are constant, as government penalty intensity increases, the probability of enterprises choosing the "self-discipline" strategy tends to 1 faster over time, and over time, the probability of enterprises choosing the self-discipline strategy has long-term stability. Therefore, the government can constrain enterprise behavior by increasing penalty strategies for enterprise non-self-discipline behavior.

Figure 3 Simulation Results of Different Penalty Intensity F on Internet Enterprise Strategy Choice.

3.3 Different Reward Intensity H

Taking H=10,20,30 respectively to analyze the impact of different government reward intensity on the game evolution path. As shown in Figure 4 [Figure 4: see original paper], when the government' s reward intensity to enterprises increases, the probability of enterprises choosing the self-discipline strategy gradually increases, and the speed of gradually tending to 1 over time also increases. For the government, in the early stage of the game, the probability of government strategy shows no obvious change. In the middle and later stages, as reward intensity increases beyond the government' s financial load, the government no longer provides rewards and tends toward the "loose protection" strategy. Therefore, in the initial stage of government policy implementation, the government can provide higher reward intensity to enterprises, rewarding enterprises for choosing self-discipline strategies and actively conducting data security protection. After enterprises themselves form certain norms, in the middle and later stages of policy rewards, the government can reduce reward intensity to enterprises to achieve long-term stability of both parties' game.

Figure 4 Simulation Results of Different Reward Intensity H on Internet Enterprise Strategy Choice.

3.4 Different Government Regulatory Capacity

The probability of government discovering enterprise non-self-discipline behavior represents the government' s regulatory capacity and governance capability. Taking =0.1, 0.5, and 0.9 respectively to analyze the impact of different government regulatory capacity on the game evolution path. As shown in Figure 5, if the government' s regulatory capacity is too low, even if the country implements strict data protection policies, enterprises still adopt non-self-discipline strategies. As government regulatory capacity improves, the probability of enterprises choosing the "self-discipline" strategy shows a small initial decrease then increases, finally tending to 1.

Figure 5 [Figure 5: see original paper] Simulation Results of Government-Enterprise Strategy Choice Under Different Government Regulatory Capacity.

3.5 Different Industry Association Participation Probability β

To verify the impact of different participation levels of third-party industry associations on the game evolution path, β=0, 0.5, 0.9 are taken respectively. β=0 represents that industry associations do not participate in government supervision of enterprise non-self-discipline behavior, β=0.9 represents that industry associations highly participate in government supervision of enterprise non-self-discipline behavior. As shown in Figure 6 [Figure 6: see original paper], for enterprises, as industry association participation in supervision increases, enterprises tend toward self-discipline behavior. For the government, due to the intervention of third-party industry associations, the government' s work burden is reduced, and the speed of government choosing the "strict protection" strategy becomes slower, but eventually tends to 1.

Figure 6 Simulation Results of Different Industry Association Participation Levels on Government-Enterprise Strategy Choice.

4.1 Conclusions

Through the above stability analysis, solving the game process between internet enterprises and government clarifies the influencing factors of both parties' behavioral strategy choices: (1) Reducing the cost of government strict protection 1C, improving the probability of government discovering enterprise non-self-discipline behavior , and enhancing government credibility 3W from strict protection strategy are the main factors for government to choose the "strict protection" strategy. Therefore, it is necessary to improve the government' s management capabilities and regulatory levels in law enforcement and judiciary, introduce comprehensive data protection laws, improve the data classification and grading framework, establish specialized data information security protection institutions, reduce the strategic costs of strict protection, strengthen data protection science popularization and publicity, and enhance personal data protection awareness and capabilities of all social parties. (2) Government increasing financial subsidies H for enterprise data development and administrative penalty fees F for enterprise non-self-discipline have positive impacts on enterprises adopting self-discipline data development strategies. Therefore, the government can adopt incentive measures and penalty constraints to promote enterprises evolving toward self-discipline strategies. (3) As a third-party supervision actor, increasing the probability of industry association participation in data protection can assist government in supervising enterprise behavior, reduce government data protection costs, and regulate internet enterprise self-discipline behavior. (4) Reducing data protection cost D when enterprises are self-disciplined has positive impacts on enterprises adopting self-discipline data development strategies. Therefore, it is necessary to strengthen technological innovation and reduce enterprise data protection costs. Meanwhile, the higher the sensitivity λ of data developed by enterprises, the higher the benefits obtained by enterprises, while also bearing the risk of being discovered by government and industry associations for non-self-discipline behavior. Therefore, enterprises need to comply with industry self-discipline norms, implement graded management for different data according to sensitivity differences, explain to users and society why data is collected, what data is collected, and where this data will be used, ensure data security, to gain trust benefits from users and government rewards.

4.2.1 Government: Management and Guidance

In the big data era, the entire lifecycle process of data processing involves multiple actors. In the process of data protection and utilization, it is difficult to form collective action, often resulting in excessively high data protection costs. Simply considering autonomy or self-discipline of various data actors is difficult to achieve ideal results. Under China' s national conditions, through government management and guidance, the interests of all parties can be protected while fully leveraging the social value of data and enhancing social welfare. (1) **Ex-ante Prevention: Improve Data Classification and Grading Framework** In the development process of data mining, establishing personalized emerging protection and graded protection mechanisms for various process stages and scenarios including data collection, cleaning, processing, and application, with different protection modes for different protection levels, clarifying data management rights and obligations, and formulating different data management strategies are important means of data security management. Data assets in different industries and regions have great value differences. To properly classify and grade different data, attention must be paid to grasping corresponding attributes and processing standards. Before conducting data classification and grading, it is necessary to understand the basic situation of relevant industries, first conduct data inventory, and unify data formats. Second, set data security levels, clarify data classification systems, design catalog lists, and assign different categories and protection levels to data according to data security level determination rules. Finally, review data levels, match corresponding usage subjects and regulatory institutions according to data security levels, and implement different data protection methods. Pay attention to classification dimensions, with related settings needing to consider the operability of data classification and contextualization of data classification. There are many dimensions for data classification, nowadays mostly classified by data form and data content. (2) **In-process Supervision: Ensure Policy Implementation** For enterprises, their ultimate pursuit is profit maximization. When the benefits of adopting non-self-discipline strategies to illegally mine user data are higher than those of self-discipline strategies, they are highly likely to ignore data protection policies and adopt non-self-discipline strategies. In this situation, government policy is the key factor affecting enterprise behavioral decisions. Specialized data information security protection institutions should be established to regularly inspect enterprises' implementation of data protection policies and rules. Simultaneously, combine strict data protection and loose protection methods to alleviate the opposition and conflict between data protection, data flow, and data rights, and promote balanced data circulation and sharing. (3) **Ex-post Balance: Government Incentives and Accountability** To promote the stable strategy of internet companies evolving toward "self-discipline," increase enterprise income while reducing protection costs. However, under current economic and technological conditions, it is difficult to achieve breakthroughs in income and costs in the short term. Therefore, external forces are needed, i.e., government departments should provide certain financial assistance and subsidies to the internet. Tax authorities grant certain tax reductions and exemptions. Meanwhile, establish traceability and accountability mechanisms, strengthen government supervision, and push enterprises onto the path of self-regulation.

4.2.2 Enterprise: Industry Self-Discipline and Technological Innovation

(1) **Formulate Industry Self-Discipline Norms** With the innovative development of emerging technologies such as big data and artificial intelligence, relying solely on government regulation for data protection is insufficient for effective data protection. Under the condition that China's personal information protection laws and regulations are not yet perfect, data protection standards and norms of industry associations can effectively compensate for legal deficiencies and loopholes, playing a role in regulating market activities. Industry association self-discipline is the self-restraint of countries to maintain industry competition order, formulating industry rules to standardize industry behavioral standards, relying on self-restraint and conscious action of industry members to promote high-quality development. Industry self-discipline must first comply with national laws, regulations, and policy orientations, and second mainly rely on industry norms to constrain the behavior of industry members, thereby forming functions of internal self-supervision and self-protection. (2) **Technology Empowerment to Reduce Enterprise Data Protection Costs** Information security technology is an important means of protecting data. Enterprises need to continuously innovate technical means to reduce data protection costs while improving data protection intensity. Currently, China has developed many technologies for data protection, such as blockchain technology, reversible data hiding technology, and data citation analysis technology.

[1] Internet Industry Self-Discipline Convention [EB/OL]. [2022-05-28]. http://nmc.xhu.edu.cn/3b/da/c2954a80858/page.htm
[2] Chen Chuqiao, Analysis on the Protection Path of Enterprise Data. Journal of Hunan Radio & Television University, 2021(01): pp. 90-96.
[3] Chen Chuqiao, Analysis on the Protection Path of Enterprise Data. Journal of Hunan Radio & Television University, 2021(01): pp. 90-96.
[4] Feng Guo, Xue Yisa. From "Rights Norm Model" to "Behavior Control Model" Data Trust—Another Approach to Constructing Data Subject Rights

Protection Mechanism [J]. Law Review, 2020, 38(03): 70-82.
[5] Ho T Y, Fishman P A, Zabinsky Z B. Using a game-theoretic approach to design optimal health insurance for chronic disease [J]. IEEE Transactions on Healthcare Systems Engineering, 2019: 1-30.
[6] Feng M N, Zhu G, Yang J Y. Research on Social Network Privacy Protection Based on Evolutionary Game [J]. Journal of Intelligence, 2017, 36(09): 127-132+85.
[7] Wei Y H, Chen X L, Zou X F. Research on the Evolutionary Game of Personal Information Protection in the Digital Economy Era [J]. Economic Issues Exploration, 2019(12): 79-88.
[8] Zhang X X, Xu K, Zhong Y F, Su H. Evolutionary Game Analysis of Cooperation Behavior Among Network Service Providers [J]. Journal of Zhejiang University (Engineering Science), 2017, 51(06): 1214-1224+1232.
[9] Zhu G, Cao X L, Sun Y. Game Strategy Analysis of Privacy Protection Investment in Social Network Environment—Based on Evolutionary Game Perspective [J]. Information Science, 2017, 35(07): 25-30.
[10] Gu Q Y, Ju C H, Bao F G. Research on Evolutionary Game Model of Relationship Between Social Network Services and Users Integrating Privacy Concerns [J]. Information Science, 2019, 37(09): 29-36.
[11] Zhou M, Qian P. Research on Evolutionary Game of Over-collecting APP Personal Data Protection and Use Under Government Supervision [J]. Information Exploration, 2020(11): 8-18.

Note: Figure translations are in progress. See original paper for figures.