ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Optimization Pathways for Legal Mechanisms Protecting Personal Information in the Digital Economy

Daiwei Zhang[1,*]

[1] Public Security Department, Jilin Police College, Changchun, Jilin, 130123, China

SUMMARY: *This paper conducts an in-depth discussion on legal issues concerning personal information protection in data transactions. First, a three-party evolutionary game model is constructed, setting parameters such as regulatory costs and violation benefits. By replicating dynamic equations, the study analyzes the factors influencing each party's strategy selection and the stability of equilibrium. It defines the dual attributes of personal information rights and examines the legal conflict between circulation efficiency and strict protection in data transactions. Based on game simulations and conflict analysis, the paper proposes an optimization path for legal mechanisms protecting personal information. When sR4 + vR4 + (1-β)θR4 - β(F + I) - C2 < 0, (r1 - 11 + r2 - 12)R2 + L - β(1 - C3) - C1 > 0, and R4 + vR4 + 0R4 - C2 > 0, the value of x exhibits an initial increasing trend from the starting point, followed by a decreasing trend. While the y-value continuously decreases, both converging to the stable game point (0, 0). When sR4 + vR4 + (1 - β)θR4 - β(F + I) - C2 < 0, (r1 - l1 + r2 - l2)R2 + L - β(I - C3) - C1 > 0, and sR4 + vR4 + θR4 - C2 < 0, starting from the initial point, the x-value first exhibits a rapid increasing trend followed by a rapid decreasing trend, while the y-value continuously decreases, both converging toward the stable game point (0, 0). The level of government regulatory costs and the level of public awareness and ability to reasonably utilize tools like agreements to protect information security not only influence the evolution of one's own strategy but also affect the strategy evolution trends of other stakeholders.*

KEYWORDS: *Data Trading; Personal Information Protection; Evolutionary Game Theory; Replication Dynamics Equation; Legal Mechanisms*

1 Introduction

In the era of the digital economy, data has become a key factor of production driving economic development. Relevant documents emphasize accelerating the pace of digital economic development and deepening the integration of the digital economy with the real economy [1]. Simultaneously, efforts should be made to foster the development of strategic emerging industry clusters, creating new growth poles in next-generation information technology, artificial intelligence, biotechnology, new energy, new materials, and green environmental protection [2, 3]. Vigorous promotion of big data development and application is essential to enhance resource allocation efficiency and strengthen the endogenous momentum of economic growth [4]. Engagement in international collaboration in the digital economy is vital, where cooperation will continue to create innovative opportunities in the development of the economy through a win-win strategy [5]. In this regard, the contribution of the digital economy to China's economy continues to grow significantly. For instance, the digital economy contributes 41.5%

*zdw202509@126.com
https://doi.org/10.65102/is2026159
Published: 30 April, 2026

of China's GDP, making China the world's second largest digital economy [6]. The digital economy plays an important role as a driver for high-quality development.

With regard to the fast growth of the digital economy, the development of the platform economy is quite rapid [7]. In the market competition, the ability to gather and analyze personal information plays an important role in determining whether the platform enterprises will succeed. Advertisers may provide consumers with free goods and services in return for more personal data to obtain targeted audience and generate greater profits [8, 9]. Therefore, personal information becomes a valuable resource that many enterprises strive to possess. However, consumers do not fully understand the process of their data gathering and use. Furthermore, although they detect data breaches or leaks, people encounter considerable difficulties when exercising their rights against powerful platforms [10]. There are many judicial cases showing that monopolistic behavior violating personal information is common. Some of the cases in China involve Douyin suing Xiaohulu for live-streaming data scraping and Tencent suing Sishin Media for article data scraping on WeChat public accounts. Additionally, the Senate Judiciary Committee holds hearings in the US on the degree to which GAFA engages in anticompetitive activities concerning personal information [11]. On an international level, laws protecting personal information attract more attention [12]. Although China formulates civil law, the Data Security Law, the Personal Information Protection Law, and the Consumer Rights Protection Law that regulate personal information protection, there remain great challenges in regulating information monopolies and mass illegal collection and processing of personal information due to new developments in the digital economy [13]. Under this circumstance, discussing the optimization of the legal system protecting personal information becomes essential.

Looking at the issue from an international perspective, one can observe that there is some convergence between European and American nations concerning how they handle personal information privacy [14]. However, the routes taken by both are somewhat different. According to Iaia, V., the United States leans towards self-regulation, where the rights of the individual and self-regulation by the industry play a crucial role in protecting personal information [15]. On the other hand, Europe considers personal information a basic right that is protected through regulation by the state [16].

The General Data Protection Regulation (GDPR) of the European Union provides vast rights to data subjects based on various principles, including lawful personal data processing and user consent. Therefore, GDPR receives immense attention across the globe [17]. Regarding GDPR studies, Dhar, T. posits that GDPR represents certain spirit, features, and similarities and dissimilarities with other privacy frameworks such as California Consumer Privacy Act (CCPA). It also addresses the issues and compliance approaches adopted by multinational corporations in dealing with various privacy laws [18]. Marelli, L. and Testa, G. suggest that GDPR outstripped Directive 95/46/EC due to a decentralized regulatory structure that shifted the obligation from national agencies to data controllers to balance citizens' personal data with the free movement of data flows [19]. Dayalu, P. and Punnagai, M. highlight GDPR as a key regulation in modern data privacy protection with strengths and weaknesses alongside societal impacts on data privacy mechanisms [20]. Sullivan, C. draws parallels between the EU's GDPR and APEC's Cross-Border Privacy Rules (CBPR). He highlights both similarities and dissimilarities between these two regulatory instruments in data regulation processes and applicability [21]. However, the United States and the European Union utilize distinct approaches to ensure information privacy protection. Poladov, A. carries out an exhaustive review of the American legal regime on personal data protection, indicating that there is no dedicated federal law, and it lacks industry-specific court rulings [22]. Despite being a state-level law, the CCPA affects all major areas of the United States [23]. Cramer, J. highlights the

complexities involved in America's legal regime for personal data privacy protection that involves the intertwining of various federal and state laws undergoing consistent modification [24].

Examining personal information protection law in China, two most general provisions within the digital economy can be distinguished: namely, the Data Security Law and the Personal Information Protection Law. According to Shao Y., although some convergence in comprehensive legal mechanisms for personal information protection has occurred globally, China implements a specific "legal interest protection model" as compared to the American and European "rights-based protection model" [25]. Gong N. suggests that the Personal Data Protection Law, adopted on November 1, 2021, enlarges the scope of protection, determines individual rights, intensifies obligations towards data controllers, imposes strict rules on the processing of sensitive data and processing by public organizations. Thus, the legislation means China's movement from indirect to direct protection of personal information and its gradual progress in terms of comprehensive protection [26]. Cheng W. considers that Chinese personal data protection laws should be compatible with the global ones as far as their adoption is concerned. Specifically, it is proposed that such laws should follow the "rights-based protection model". The adoption of the model allows integrating personal information rights into personality rights, which ensures harmony between the legal framework and development of individuals' personal data control [27]. According to Ren H., cross-border data plays an essential role in the functioning of the digital economy, but the current legal regulation has been developed predominantly by Europe and the USA. China needs to develop international protection mechanisms of cross-border personal information transfer, identify the responsibilities of data controllers, intensify regulatory oversight and enhance international collaboration in protection of individuals' privacy right [28]. Chungang M. analyzes personal information protection in the EU, the US and China, identifying the specificity of the latter in the form of targeted legislation based on local context but marked with oversimplification and regulatory inconsistency [29]. Finally, Creemers R. suggests that the Personal Information Protection Law regulates the relation between businesses (information owners) and customers (information providers) while placing no restrictions on government information collection and processing, whereas the Data Security Law seeks to prevent damage to national security and public interests due to the use of information [30].

Regarding the path towards optimizing legal measures that ensure the security of personal data, the international academic community is not unanimous about the basic issues, such as defining personal information rights and developing efficient protective measures. Studies concerning personal information protection in China have been conducted mainly in the sphere of civil law. For instance, Li, Q., et al. have identified three major barriers that face China’s Personal Information Protection Law: sensitivity, digital technologies, and conflicting interests. The authors offer three optimization solutions: situation-oriented risk management, algorithmic optimization, and a double-tier balancing of interests and rights [31]. On the other hand, Hu, C. has pointed out some shortcomings in China’s current personal information protection legislation. Specifically, there is a lack of legal public protection, deficient consent requirement, regulatory imperfection, and public unawareness of personal information protection. Thus, the author proposes combining public and private laws, optimizing informed consent, and regulatory mechanisms to establish relative balance in protection and utilization [32].

Scholars and practitioners in the Western world have recently suggested that antitrust tools may be used to protect individuals' personal information, while research on this topic has been widely considered important. According to Kimmelman, E. et al., using antitrust laws as one of the strong tools for solving personal information issues could possibly reduce incentives for the competition and innovation of new goods, yet this will force platforms to be more careful about

the handling of personal data [33]. Moreover, Shapiro, C. suggests that in a centralized internet environment, personal data belongs to individuals and he, therefore, suggests the use of blockchain as an effective means for the protection of personal information. In a decentralized blockchain system, individuals can utilize encryption methods to regain control over their personal data [34]. Nevertheless, there are legal conflicts in protecting personal information by the use of blockchain technology. According to Schrepel, T., regulation of the newly developed blockchain technology is lagging behind the development of this technology [35]. Similarly to natural monopolies, price regulation is still an applicable means in the digital economy environment to benefit from economies of scale without putting consumers at risk [36, 37].

In this paper, the author constructs a tripartite game model involving the government, the personal information holders, and the personal information seekers/users based on the theory of evolutionary games. Through parameter setting and analysis of replicator dynamic equations, the evolution processes and factors influencing the decision-making of each player are analyzed. In the research, the author first makes clear some basic principles of personal information security protection in data transactions. Then, he analyzes the forms of legal disputes in data transactions vs. personal information security protection. Using the MATLAB software simulation method, the author evaluates the evolutionary stable strategies of the players under different situations.

2 Analysis of the Tripartite Dynamics in Personal Information Protection Under the Digital Economy

Within the backdrop of rapid development of digital economy, the emergence of data as a new factor of production and the major driving force of economic development is noteworthy. Personal information as one of the vital components of data resources circulates and utilizes widely, creating economic benefits while at the same time bearing the risk of causing privacy infringements and data misuses. It becomes urgent to deal with the problem of balancing the interests between the protection of personal information on one hand and its development and utilization on the other. This thesis focuses on improving legal approaches to the protection of personal information in digital economies. It applies a combination of theoretical reasoning, game theory, and normative analysis in addressing relevant questions.

2.1 Tripartite Game Model

2.1.1 Model Assumptions

This paper employs evolutionary game theory to analyze the interactions among three key actors—the government, personal information owners, and personal information acquirers/users—in the process of personal information utilization. From the perspectives of personal information usage, acquisition, and sharing, the primary participants are: (1) the government (G), primarily serving a regulatory role; (2) personal information owners (P), who are the source of personal data or information and the most significant victims of improper personal information usage; (3) Personal information acquirers/users (C), entities with needs to mine or utilize personal data or information, primarily enterprises.

Assumption 1: All stakeholders are perfectly rational, with their choices or behaviors adhering to the principle of maximizing benefits.

Assumption 2: Information among stakeholders is fully transparent.

2.1.2 Parameter Variable Settings

Government (G) implements unregulated and strictly regulated states for data usage. Strict regulation refers to the government incurring costs to oversee information activities. This includes management expenses of C_1. Rewarding lawful data acquisition yields S_{13}, while penalizing violations yields K_{13}. Regulatory efforts enhance the government's image, yielding R_1. Simultaneously, standardized data usage fosters a healthy data market, yielding R_{13}. No regulation means the government does not oversee the personal information market; unregulated usage disrupts the information market, resulting in losses of C_{12}.

Personal information owners (P) may adopt either a proactive or passive attitude when providing personal information. Active provision refers to a willingness to share information. If information is actively provided, individuals can access more convenient services, yielding a corresponding benefit of R_2. If the personal information acquirer/user adopts a compliant strategy, individuals also receive a reward of S_{32}. However, active provision carries certain risks, namely the potential for non-compliant use of information, incurring a cost of C_2. Passive provision denotes an unwillingness to share personal information. In this state, individuals face inconvenience costs of $C_2^{'}$ due to information scarcity.

Personal Information Acquisition/User (C) may adopt compliant or non-compliant strategies regarding personal information. A compliant strategy involves adhering to regulations for using and acquiring personal information while increasing protective investments, incurring a cost of C_3. If a compliant strategy is adopted while competitors employ non-compliant strategies, competitiveness is lost, resulting in a negative return of w. Compliant data acquisition requires payment to data sources S_{32} and is incentivized by governments implementing regulatory strategies S_{13}. Compliant usage promotes active data sharing, yielding convenience benefits of R_3. This gain materializes when both compliant and active-sharing strategies are adopted. Non-compliant strategies involve illegal acquisition and use of personal information. If governments implement regulatory strategies, personal information acquirers/users face governmental penalties K_{13}. Additionally, litigation risks exist, incurring costs of C_3, as the benefits derived from using data at lower costs than peers are $w^{'}$.

2.1.3 Setting Decision Variables

Assuming the probability of strict government regulation is p_1, then no regulation is $1-p_1$. The probability of personal information owners actively providing information is p_2, while passively providing it is $1-p_2$. The probability of personal information acquirers/users adopting a normative strategy is p_3, while adopting a non-normative strategy is $1-p_3$. The game relationship among relevant parties is illustrated in Figure 1.

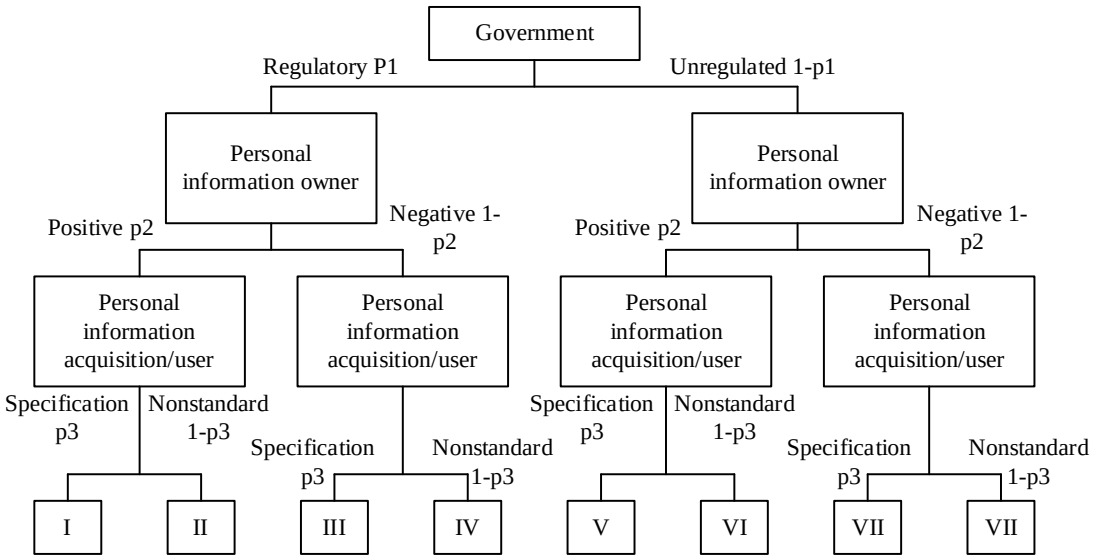


Figure 1: Diagram of the three-party game relationship

2.2 Tripartite Game Analysis Among Government, Data Providers, and the Public

2.2.1 Copying Dynamic Equations

(1) Dynamic replication equations for government game strategies. Let the expected payoff for the government choosing "strict regulation" be G_x, and the expected payoff for choosing "non-strict regulation" be G_{1-x}. Simultaneously, let the average expected payoff be $\bar{G}$. Then we have:

$$\begin{aligned} G_x &= y*z*(G_i - G_c) + y*(1-z)*(-G_c) \\ &+(1-y)*z*(G_i - G_c) + (1-y)*(1-z)*(-G_c - G_j) \end{aligned} \tag{1}$$

$$\begin{aligned} G_{1-x} &= y*z*(G_i) + y*(1-z)*(-G_j) \\ &+(1-y)*z*(G_i) + (1-y)*(1-z)*(-G_j) \end{aligned} \tag{2}$$

$$\bar{G} = x*G_x + (1-x)*G_{1-x} \tag{3}$$

According to the Malthusian equation, the replicating dynamic equation for the government's game strategy is as follows:

$$F_x = \frac{dx}{dt} = x(1-x)(G_x - G_{1-x}) = x(1-x)(yG_j - yzG_j - G_c) \tag{4}$$

For the government's choice of game strategy, its optimal state should satisfy the following conditions:

$$\begin{cases} F_x = 0 \\ \dfrac{\partial F_x}{\partial x} < 0 \end{cases} \tag{5}$$

That is

$$\begin{cases} x(1-x)(yG_j - yzG_j - G_c) = 0 \\ (1-2x)(yG_j - yzG_j - G_c) < 0 \end{cases} \tag{6}$$

When $x=0$, $0 \le y < \dfrac{G_c}{(1-z)G_j}$

When $x=1$, $\dfrac{G_c}{(1-z)G_i} < y \le 1$

It can be seen that the government's choice of game strategy is influenced by the game strategy choices of data providers and the general public. At the same time, it can also be observed that the positive benefit G_i generated by the government's "strict regulation" has no direct impact on the government's game strategy selection. However, the loss G_j resulting from citizens reducing their authorization due to "non-strict regulation," as well as the increased cost G_c required for "strict regulation," directly influence the government's game strategy selection.

(2) Replication dynamic equation for data providers' game strategies. Let the expected benefit of data providers choosing to "strictly comply" with regulatory requirements be denoted as E_y, and the expected benefit of choosing "non-strict compliance" as E_{1-y}. Simultaneously, let the average expected benefit be $\bar{E}$. Then:

$$\begin{aligned} E_v &= x*z*(E_i - E_c) + x*(1-z)*(-E_c) \\ &+(1-x)*z*(E_i - E_c) + (1-x)*(1-z)*(-E_c - E_k) \end{aligned} \tag{7}$$

$$\begin{aligned} E_{1-y} &= x*z*(E_i + E_f) + x*(1-z)*(E_f - E_j - E_k) \\ &+(1-x)*z*(E_i) + (1-x)*(1-z)*(-E_k) \end{aligned} \tag{8}$$

$$\bar{E} = y*E_y + (1-y)*E_{1-y} \tag{9}$$

According to the Malthusian equation, the replicating dynamic equation for the data provider's game strategy is derived as follows:

$$\begin{aligned} F_y = \frac{dy}{dt} &= y(1-y)(E_y - E_{1-y}) \\ &= y(1-y)(x(-E_j + E_j + E_k) \\ &-xz(E_j + E_k) - E_c \end{aligned} \tag{10}$$

For the choice of game strategy by data providers, the optimal state should satisfy the following conditions:

$$\begin{cases} F_y = 0 \\ \dfrac{\partial F_y}{\partial y} < 0 \end{cases} \tag{11}$$

That is

$$\begin{cases} y(1-y)(x(-E_f+E_j+E_k)-xz(E_j+E_k)-E_c)=0 \\ (1-2y)(x(-E_j+E_j+E_k)-xz(E_j+E_k)-E_c)<0 \end{cases} \tag{12}$$

When $y=0$, $0 \le x < \frac{E}{c}(-E_j+E_j+E_k)-z(E_j+E_k)$;

When $y=1$, $\frac{E_c}{(-E_c+E_c+E_c)-z(E_i+E_i)} < x \le 1$;

It is evident that the data provider's game strategy is influenced by the game strategies of both the government and the public. If the additional profit E_f generated by the data provider's "non-strict compliance" with regulatory requirements enables $(-E_f+E_j+E_k)-z(E_j+E_k)<0$, then $0 \le x < \frac{E_c}{(-E_f+E_j+E_k)-z(E_j+E_k)}$ cannot hold true. In this scenario, regardless of the government's chosen game strategy, the data provider will pursue its own optimal game state—that is, it will shift toward the game strategy of "non-strict compliance" with regulatory requirements.

(3) Dynamic replication equation for the public's game strategy. Let the expected benefit of the public choosing "authorization" be P_z, and the expected benefit of choosing "non-authorization" be P_{1-z}. Simultaneously, let the average expected benefit be $\overline{P}$.

$$\begin{aligned} P_z = {} & x*y*P_i + x*(1-y)*(P_i-P_i) \\ & +(1-x)*\gamma*P_i \\ & +(1-x)*(1-y)*(P_i-P_j) \end{aligned} \tag{13}$$

$$P_{1-z}=0 \tag{14}$$

$$\overline{P}=z*P_z+(1-z)*P_{1-z} \tag{15}$$

According to the Malthusian equation, the replicating dynamic equation for the public's game strategy can be derived as follows:

$$\begin{aligned} F_z = \frac{dz}{dt} &= z(1-z)(P_z-P_{1-z}) \\ &= z(1-z)(P_i-P_j+yP_j) \end{aligned} \tag{16}$$

For the strategic choices of the general public, the optimal state should satisfy the following conditions:

$$\begin{cases} F_z=0 \\ \frac{\partial F_z}{\partial z}<0 \end{cases} \tag{17}$$

That is

$$\begin{cases} z(1-z)(P_i - P_j + yP_j) = 0 \\ (1-2z)(P_i - P_j + yP_j) < 0 \end{cases} \tag{18}$$

When $z = 0$, $0 \le y < \dfrac{P_j - P_i}{P_j}$

When $z = 1$, $\dfrac{P_j - P_i}{P_j} < y \le 1$

It can thus be seen that the public's choice of game strategy is directly related to the data provider's strategy selection, but not directly related to the government's strategy choice. Furthermore, when $P_j - P_i < 0$, then $0 \le y < \dfrac{P_j - P_i}{P_j}$ cannot hold true. This indicates that under such circumstances, regardless of the strategy chosen by the data provider, the public's game strategy will shift toward selecting "authorization."

2.2.2 Stability Analysis of Game Scenarios

Stability Analysis Based on the Jacobian Matrix:

The Jacobian matrix serves as a crucial tool for assessing the stability of equilibrium points in evolutionary systems. When all eigenvalues in the Jacobian matrix are less than zero, it indicates that the corresponding scenario meets stability policy requirements.

Let the Jacobian matrix for the tripartite game involving the government, data providers, and the public be denoted as Y. Then:

$$Y = \begin{bmatrix} \dfrac{\partial F_x}{\partial x} & \dfrac{\partial F_x}{\partial y} & \dfrac{\partial F_x}{\partial z} \\ \dfrac{\partial F_y}{\partial x} & \dfrac{\partial F_y}{\partial y} & \dfrac{\partial F_y}{\partial z} \\ \dfrac{\partial F_z}{\partial x} & \dfrac{\partial F_z}{\partial y} & \dfrac{\partial F_z}{\partial z} \end{bmatrix} = \begin{bmatrix} F_{11} & F_{12} & F_{13} \\ F_{21} & F_{22} & F_{23} \\ F_{31} & F_{32} & F_{33} \end{bmatrix} \tag{19}$$

It can be calculated that:

$$F_{11} = \frac{\partial F_x}{\partial x} = (1-2x)(yG_j - yzG_j - G_c) \tag{20}$$

$$F_{22} = \frac{\partial F_y}{\partial y} = (1-2y)(x(-E_f + E_j + E_k) - xz(E_j + E_k) - E_c) \tag{21}$$

$$F_{33} = \frac{\partial F_z}{\partial z} = (1-2z)(P_i - P_j + yP_j) \tag{22}$$

Therefore, for the corresponding calculation matrix Y, when the three eigenvalues $\lambda_1, \lambda_2, \lambda_3$ under different conditions satisfy $\lambda_1 < 0, \lambda_2 < 0, \lambda_3 < 0$, the corresponding scenario represents a conditionally stable state.

2.3 Fundamental Theories of Personal Information Protection in Data Transactions

2.3.1 Legal Nature and Scope of Personal Information Rights

Government, individuals who hold personal information, and organizations that collect and use personal information (such as data brokers) during the process of data transactions are guided not only by their interests but primarily by the definition of rights and obligations. Among other considerations, personal information rights form the primary legal basis of data transactions. Understanding the legal aspects of these rights and determining the scope of their application is essential to comprehend personal information protection issues in data transactions.

One of the legal bases of the right to personal information in the process of transaction with data is the individual right to control, manage, and protect personal information from any encroachment. A clear definition of the legal features and classification of this right is necessary for ensuring the privacy of personal information and protecting its security.

From the point of view of legal features, the right to personal information has the attributes of personality right, because it provides an individual with exclusive ownership of personal information. The right to personal information includes an individual's right to control and manage his/her personal information. The essence of personal information rights lies in protecting personal honor and integrity from illegal collection, usage, and leakage of personal information. The nature of personal information right is absolute and grants exclusive control over one's information by the individual; no one can have access to information without being granted this right. Personal information rights are also comprehensive because they include confidentially, correction, and deletion of data.

Moreover, personal information rights also have the attributes of property rights, because personal information is a highly valuable resource. The value of personal information means that personal information rights show to some extent proprietary features concerning information resources of the individual. However, personal information rights are personality rights in essence.

In data transactions, individuals' rights to control and manage their information must be fully respected and protected to prevent misuse or infringement.

Regarding the legal rules involved in the protection of personal information in data transactions, the rules include definitions of personal information, principles for collecting and using personal information, and the transfer of personal data across national borders. The scope of personal information should be elaborated upon, including personal identification information, biometric information, online behavioral information, and more. Personal information needs to be collected and used in accordance with the principles of legality, legitimacy, and necessity. Organizations engaged in data transactions need to collect and use personal information after obtaining lawful consent from individuals and clearly explaining the purposes, ways, and extent of collecting such information to them. Personal information is also needed to be protected with the help of corresponding technical measures and management measures.

It is not only because personal information rights have much to do with personal information security and personal privacy that the legal properties and scope of personal information rights need to be clarified; it is also because it is of much importance to healthy data transactions and socio-economic stability. Therefore, personal information rights must be respected and protected in any case of data transaction, and the legal properties and scope of personal information rights must be clarified.

2.3.2 Analysis of Legal Conflicts Between Data Transactions and Personal Information Protection

In determining that personal information rights are legally classified as a composite right that covers aspects of personality and property in a transaction involving personal information, further analysis of data transaction practices shows an underlying struggle between the requirement for efficiency in data exchange and the necessity of protecting personal information. This struggle can be seen in academic discussions regarding the essence of rights as well as in the actual processes of processing personal information through the various parties involved in the transactions.

However, the conflict arising from the need for the effective circulation of information and the stringent requirement of protecting personal information poses obstacles to the healthy growth of the market of data transactions.

It is important to note that the key aim of the transactions of data should be geared towards improving the flow of data and its application. While it is true that the flow of data can help spur innovations in technology, industries, and socio-economic developments, it may also entail the exchange and processing of information related to individuals, which can run contrary to the laws on personal data protection. It is the purpose of the Personal Information Protection Law to protect the privacy rights of people and to ensure that no one misuses or leaks personal data. This creates a clash between the efficiency of data flow and personal data protection.

There are various ways in which the above legal issue can be manifested. The data suppliers, who seek to gain maximum advantage from their use of the data, might fail to protect the data sufficiently such that the data is leaked or mishandled in the process of transferring it. The data transfer platforms might also overlook security concerns in their efforts to conduct transactions quickly, hence compromising the security of data in transit.

This legal conflict plays an important role in both the development of the data trading market and protection of privacy rights. The efficient development of the data trading market requires the effective flow of data. Any legal conflicts have the potential to create distrust among people in the data trading market, thus affecting data flow and utilization, and hampering the development of the digital economy. On the other hand, privacy rights are the basic human rights of any individual. Legal disputes may affect such rights, causing loss of money and emotions of individuals.

The resolution of such legal disputes calls for a balance between the operations of data transactions and the safeguarding of personal information. It demands not only the development of the proper laws and regulations regarding the legal obligations and duties of the parties concerned in such data transactions in terms of protecting personal information, which would serve as solid legal grounds, but also the development of appropriate security protection systems for the data. These security protection systems may involve data encryption, data access control, and data security auditing to guarantee that data will be secure from theft at any point in time.

3 Simulation Analysis of the Tripartite Game in Personal Information Protection

3.1 Evolutionary Game Analysis

3.1.1 Model Derivation and Decision Process Analysis

The stability analysis results for equilibrium points in Scenarios 1-3 are shown in Table 1.

Scenario 1: When $sR4 + vR4 + (1-\beta)\theta R4 - \beta(F + I) - C2 > 0$ and $(r1 - l1 + r2 - l2)R2 + L - \beta(1-C3) - C1 > 0$, the system converges to four equilibrium points in the replication dynamic

system: (0, 0), (0, 1), (1, 0), and (1, 1). Following dynamic evolutionary game theory, when the net benefit generated by data utilization by the data provider and public sharing is positive, the equilibrium point is (1, 1). The decision-making process for both parties is as follows: From the public's perspective, when the benefit of authorizing sharing exceeds the benefit of not authorizing, the public will choose the sharing strategy regardless of whether the data provider utilizes the data. From the data provider's perspective, when the public authorizes data sharing, the profits generated by utilizing personal data exceed those from non-utilization. Thus, profit-maximizing data providers will choose the utilization strategy to increase their gains.

Scenario 2: When sR4 + vR4 + (1-β)θR4 - β(F + I) - C2 > 0 and (r1 - l1 + r2 - l2)R2 + L - β(1-C3) - C1 < 0, the system reaches four equilibrium points in the replicator dynamics: (0, 0), (0, 1), (1, 0), and (1, 1). According to the principles of evolutionary dynamics, the data provider receives positive net benefits through the use of personal data while the net benefits related to public data use are negative. The Nash equilibrium point of the game is (0, 1). The rationale for the decisions made by the players can be described as follows: the data providers will choose to use the personal data if the utility of use is higher than the utility of non-use, which means that it would be the most beneficial thing to do based on profit maximization regardless of public permission. It, in turn, lowers the probability of allowing use by the public. Not sharing the data will lower possible harms and, thus, increase the public's unwillingness to share.

Scenario 3: When $sR_4 + vR_4 + (1-\beta)\theta R_4 - \beta(F + I) - C_2 < 0$, $(r_1 - l1 + r_2 - l2)R_2 + L - \beta(1-C_3) - C_1 > 0$, and $R_4 + vR_4 + 0R_4 - C_2 > 0$, the replicator dynamic system reaches four equilibrium points: (0, 0), (0, 1), (1, 0), and (1, 1). If the data provider adopts the negative net benefit while the public enjoys positive net benefits after the evolutionary process, the equilibria of the game become (0, 0) or (1, 1). If the data provider chooses not to use the data, the public-sharing strategy results in the net benefit value of -C1. In light of the economic agent hypothesis, the optimal strategy for the public to adopt is not to share any personal data. Thus, the game shifts to the lower-left part, approaching the (0, 0) point. At this point, the strategy adopted by the public and the data provider will be (not sharing, not using). The resulting outcome is a prisoner's dilemma. However, due to the absolute technological and informational advantage of the data provider, it is unlikely that they reveal their utilization of the data. Even if the infringement occurs, it is still largely hidden from the public eye, preventing its prompt identification. Moreover, because of the condition that sR4 + vR4 + θR4 − C2 > 0, which indicates that the data provider should use data in order to maximize net benefit. As it has been found out, when data providers use data, the net benefit that public enjoys is $(r_1 - l_1 + r_2 - l_2)R_2 + L - \beta(I - C_3) - C_1 > 0$. Thus, the best strategy for the public becomes sharing. The game moves towards the upper-left part and reaches the point (1, 1).

Table 1: Stability Analysis of Equilibrium Points (Scenarios 1-3)

		(0,0)	(0,1)	(1,0)	(1,1)	(x*, y*)
Situation 1	detJ	-	-	+	+	Uncertain
	trJ	Uncertain	Uncertain	+	-	0
	Stability	Saddle point	Saddle point	Unstable	ESS	Center point or saddle point
Situation 2	detJ	-	+	+	-	Uncertain
	trJ	Uncertain	-	+	Uncertain	0
	Stability	Unstable	ESS	Unstable	Unstable	Center point or saddle point
Situation 3	detJ	+	+	+	-	-
	trJ	-	+	+	-	0
	Stability	ESS	Unstable	Unstable	ESS	Saddle point

The equilibrium point stability analysis results for Scenarios 4-6 are shown in Table 2.

Scenario 4: When $sR_4 + vR_4 + (1-\beta)\theta R_4 - \beta(F + I) - C_2 < 0$, $(r_1 - l_1 + r_2 - l_2)R_2 + L - \beta(I - C_3) - C_1 > 0$, and $sR_4 + vR_4 + \theta R_4 - C_2 < 0$, the replicator dynamic system converges to four equilibrium points: (0, 0), (0, 1), (1, 0), and (1, 1). Based on the theory of dynamic evolutionary game, the net benefit of exploitation will be negative while the net benefit of sharing public data will be positive, thus creating a Nash equilibrium at (0, 0). If the net benefit of sharing by the public is positive, then the utility benefit of sharing will be greater than the utility of not sharing, thus motivating authorization of sharing of data. For data providers, the cost incurred through utilization of data is greater, hence, net benefit will be negative, therefore, data providers will avoid utilization of personal data. With data providers utilizing the strategy of not utilizing personal data, the net benefit obtained from authorization of sharing by the public will be equal to -C1.

Scenario 5: When $sR_4 + vR_4 + (1-\beta)\theta R_4 - \beta(F + I) - C_2 < 0$, $(r_1 - l_1 + r_2 - l_2)R_2 + L - \beta(I - C_3) - C_1 < 0$, and $sR_4 + vR_4 + \theta R_4 - C_2 > 0$, the replicator dynamic system reaches four equilibrium points: (0, 0), (0, 1), (1, 0), and (1, 1). Based on the analysis using the dynamic evolutionary game model, the net benefits gained by data providers in exploiting data and those gained by the public in sharing data are negative, tending towards the equilibrium position at (0, 0). If the net benefits of the public strategy of sharing data are negative, then the members of the public, being rational, will adopt the strategy of not sharing data. Since the members of the public have adopted this strategy, the net gains earned by the data providers through the illegal exploitation of personal data become less than the cost of compensating the losses.

Scenario 6: When sR4 + vR4 + (1-β)θR4 - β(F + I) - C2 < 0, (r1 - l1 + r2 - l2)R2 + L - β(I - C3) - C1 < 0, and $sR4 + vR4 + \theta R4 - C_2 < 0$, the replicator dynamic system reaches four equilibrium points: (0, 0), (0, 1), (1, 0), and (1, 1). Under dynamic evolutionary game theory, both the benefits derived from using the data by the providers and public data sharing are negative. This means that the equilibrium point lies on (0, 0). The providers experience negative profits due to high costs involved in data usage. At the same time, the public is exposed to greater danger if they allow their data to be used. In the long run, the evolutionary process makes the providers use non-data usage strategies to avoid excess cost. The public benefits more from not giving out their data than allowing them to be shared.

Table 2: Stability Analysis of Equilibrium Points (Scenarios 4-6)

		(0,0)	(0,1)	(1,0)	(1,1)	(x*, y*)
Situation 4	detJ	+	+	-	-	Uncertain
	trJ	-	+	Uncertain	Uncertain	0
	Stability	ESS	Unstable	Saddle point	Saddle point	Center point or saddle point
Situation 5	detJ	+	-	+	-	Uncertain
	trJ	-	Uncertain	+	Uncertain	0
	Stability	ESS	Saddle point	Unstable	Saddle point	Center point or saddle point
Situation 6	detJ	+	-	-	+	Uncertain
	trJ	-	Uncertain	Uncertain	+	0
	Stability	ESS	Saddle point	Saddle point	Unstable	Center point or saddle point

3.1.2 Numerical Simulation

In order to enable an easier analysis of the evolutionary path taken by data suppliers and the general population and validate the proposed evolutionary game theory, this paper uses MATLAB simulation tools to conduct numerical simulation under different situations. The analysis is based on the evolutionary path of the equilibrium point of both sides of the game.

Particularly, Scenarios 3 and 4 will be considered, whereby the starting point of the system state is defined in the range of [15%, 75%], and the simulation period [0, 20].

Scenario 3: Assuming parameters R2=8, R4=3, F=6, I=7, C1=3, C2=4, C3=5, L=4, s=0.6, v=0.9, β=0.3, θ=0.5, r1=0.6, l1=0.2, r2=0.5, l2=0.3, The following conditions are satisfied: sR4 + vR4 + (1-β)θR4 - β(F + I) - C2 < 0, (r1 - l1 + r2 - l2)R2 + L - β(I - C3) - C1 > 0, and sR4 + vR4 + θR4 - C2 > 0. Figure 2 shows the dynamic evolution process of Scenario 3. In Scenario 3, the equilibrium point of the game when the public will not provide any personal data and the data brokers will not use the data is (0, 0). The dynamic evolution process of the model shows that, starting from the first point, the x-point grows at first, then falls, and the y-point keeps decreasing until reaching the equilibrium point (0, 0). From the dynamic evolution of the model, it can be seen that some data suppliers adopt a proactive approach at the start of their interaction, but later they give up because the cost exceeds the benefits of usage.

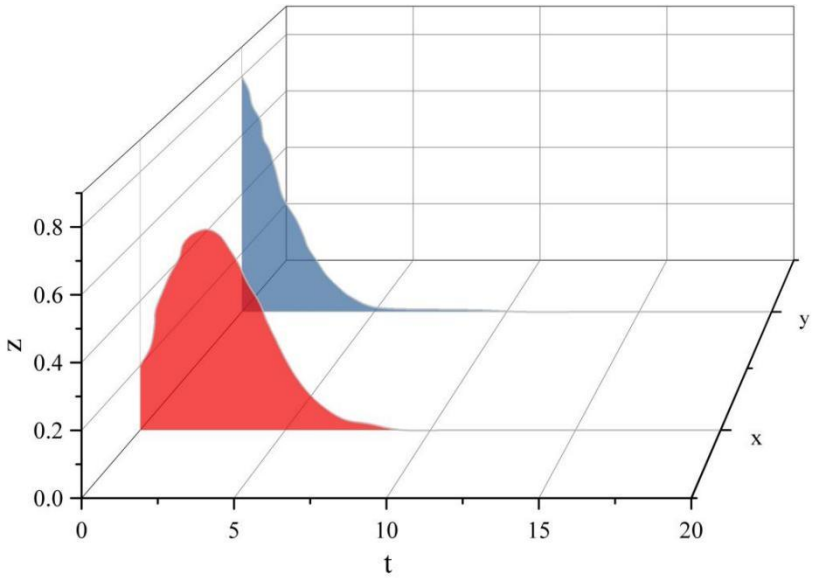


Figure 2: The dynamic evolution process under Scenario 3

Scenario 4: Assuming parameters R2=8, R4=3, F=6, I=7, C1=3, C2=5, C3=5, L=4, s=0.6, v=0.9, β=0.3, θ=0.5, r1=0.6, l1=0.2, r2=0.5, l2=0.3, The following conditions are satisfied: sR4 + vR4 + (1-β)θR4 - β(F + I) - C2 < 0, (r1 - l1 + r2 - l2)R2 + L - β(I - C3) - C1 > 0, and sR4 + vR4 + θR4 - C2 < 0. The dynamic evolution chart for Scenario 4 is shown in Figure 3. The point of equilibrium where the public does not share personal data and where no utilization takes place on the part of the data broker is denoted by (0, 0). Starting from the initial condition, the value of x increases rapidly before decreasing rapidly, whereas the value of y continually decreases until it converges towards the stable equilibrium at (0, 0). From the diagram of the dynamic evolution path, it can be observed that the path of Scenario 4 follows a pattern similar to Scenario 3, although with a higher rate of change in x and y. With an increase in utilization costs for the data provider, the utilization costs exceed the advantages associated with the same, leading to the conversion of the net benefit of the data provider from positive to negative. Hence, the data provider decides against utilizing personal data.

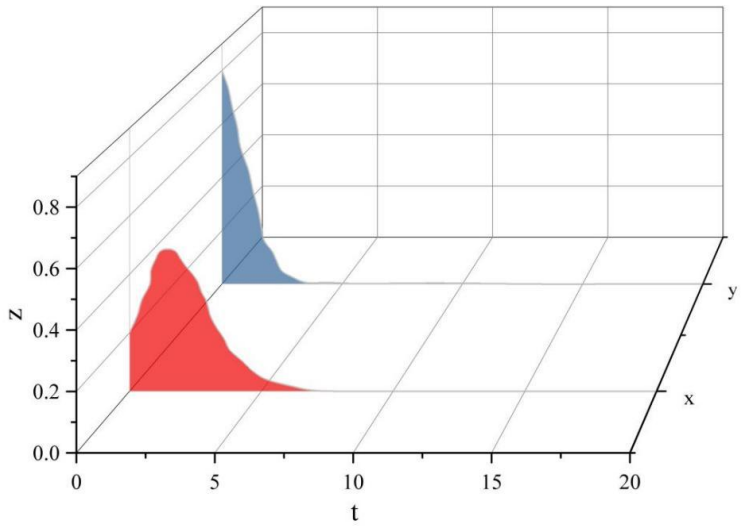
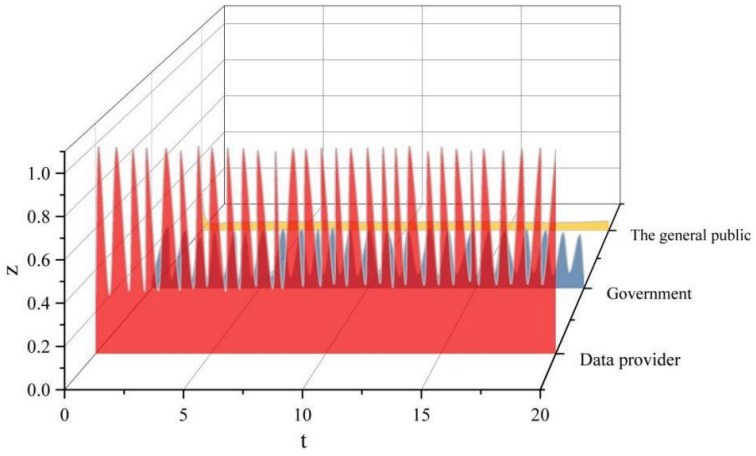


Figure 3: The dynamic evolution process under Scenario 4

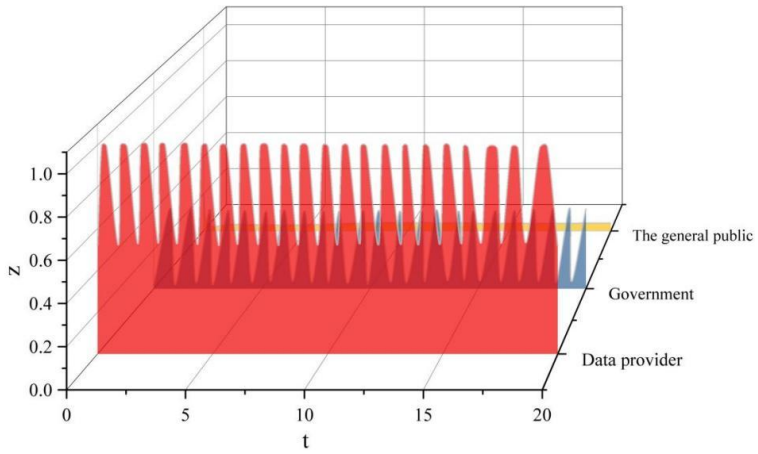
3.2 Stability Analysis

3.2.1 Impact of Government-Related Variables

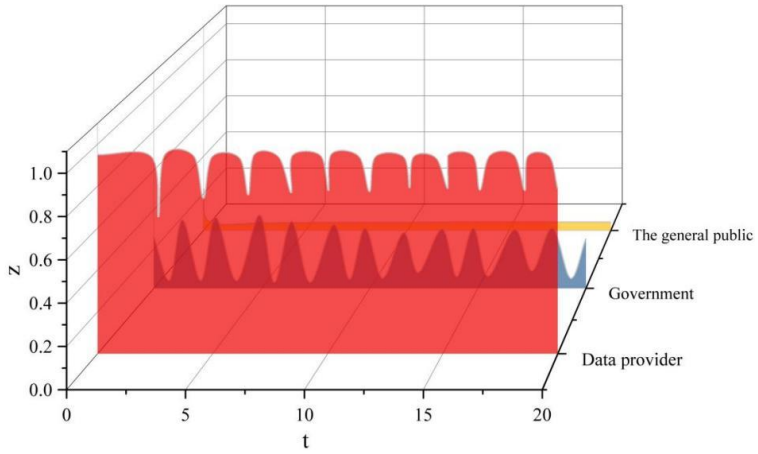
The initial values for proportions of the strategy in the course of system development are set to lie in the range of [15%, 75%] and the time interval is given by [0, 20]. Under the condition that the policy adopted by the government is strict regulation, the cost of the strategy will be 15, 8, and 4, respectively. The level of government strict regulation costs not only influences the strategic evolution trends of government departments but also affects the strategic evolution trends of other stakeholders, with the most noticeable change being the strategic evolution trend of data providers. As the costs required for government strict regulation decrease, the probability of data providers adopting the “Standardize Protection of Information Security” strategy significantly increases, and the duration they remain stable on this pure strategy grows longer. Therefore, reducing the cost of strict regulation can incentivize data providers to adopt the “Standardize Protection of Information Security” strategy. When data providers consistently choose this strategy, the frequency of information security incidents decreases. Consequently, the public's trust in data providers increases, leading them to choose not to actively protect information security.



(a) C=15



(b) C=8



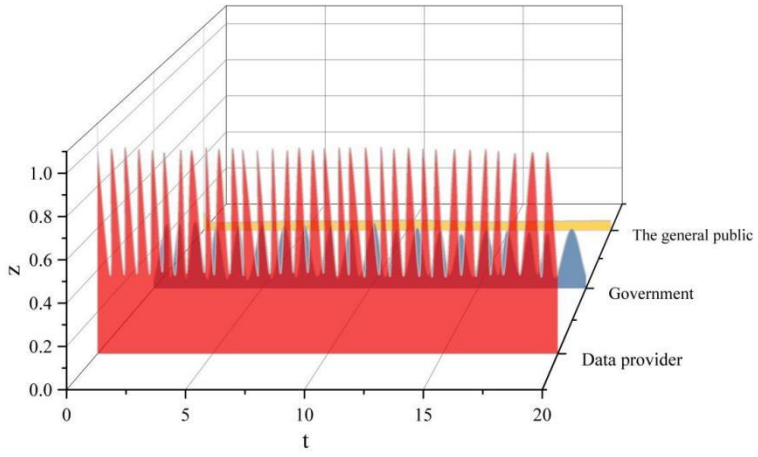
(c) C=4

Figure 4: Evolution process and results of the strategies of the three parties in the game

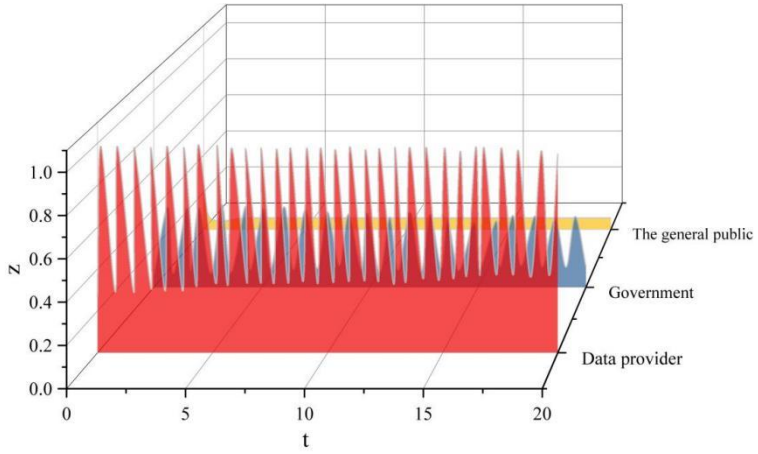
3.2.2 Impact of Variables Related to the General Public

Assuming the public understands and can reasonably utilize tools such as agreements to protect information security at costs of 50, 20, and 5 respectively, the strategy evolution process and outcomes for the three-party game are illustrated in Figure 5 (a–c). The level of cost for the public to understand and reasonably utilize tools like agreements to protect information security not only influences the public's own strategy evolution trends but also affects the strategy evolution trends of other stakeholders. As the cost for the public to understand and reasonably utilize tools like agreements to protect information security decreases, the probability of data providers engaging in compliant information acquisition and utilization increases over time on the pure strategy of “standardized information security protection.” However, this increase occurs at a relatively slow pace. Only when costs become significantly lower will data providers be driven to increase the probability of compliant utilization. During this process, the government finds it difficult to achieve a stable state and ultimately settles into a strategy of lax regulation. This occurs because data provider oversight partially replaces the regulatory functions of the government. Therefore, establishing third-party oversight institutions or employing other market mechanisms within society can reduce the discernment costs for the public to understand and reasonably utilize agreements to protect their information rights. This, in turn, stimulates data providers to choose the “Standardized Protection of Information

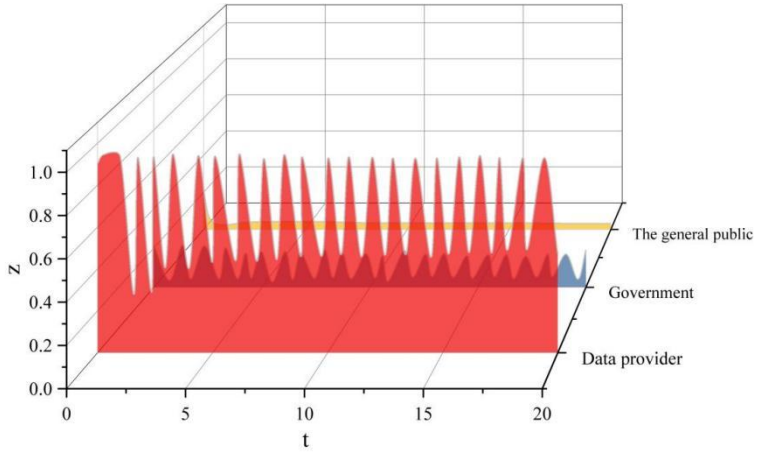
Security" strategy.



(a) C=50



(b) C=20



(c) C=5

Figure 5: Evolution process and results of the strategies of the three parties in the game

4 Optimizing Legal Pathways for Personal Information Protection

4.1 Defining the Boundaries Between Personal Information and Privacy Rights

For the vast majority of people, the issue of personal information protection may be seen as part of privacy protection. Within judicial practices, in considering cases where citizens' rights have been violated, personal information being among them, the violated rights and interests will generally be referred to as personal rights, which include the right to privacy or reputation. While it is beyond doubt that personal information and privacy rights have much in common, differences between them continue to exist. First of all, terminologically speaking, it becomes evident that the right to privacy involves elements of confidentiality and private affairs. The right to privacy pertains to personal activities, the concealment from which from any outsiders is preferred, having an element of confidentiality about it. It involves aspects of citizens' lives that would be concealed rather than disclosed. Because the content of such issues is not supposed to be known to others, people do not disclose them. Even where the two seem to overlap, they have different essences. Personal information, by definition, refers to a collection of information that identifies one's identity. The aggregated data does not have any inherent attributes that relate to privacy. The data can include information that is both public and not public at all and does not relate to private spheres in the lives of citizens. Moreover, even if it were leaked, it would not have much of an effect on the person, causing little trouble or harm. On the other hand, the information and data that are held by organizations and companies have some public value. Another key difference between the two is the type of rights associated with each case and the methods of dealing with violations of these rights. Legally, both rights fall under personality rights. However, the right to privacy is a passive right and has clear personal attributes. Legal actions regarding the violation of this right are focused on resolving issues relating to the encroachment upon personal space. If the personal information of someone is violated, then the owner of the data may initiate active measures and force the violator to delete or modify the data. Individuals have the right to decide how their data should be managed and protected from any potential interference. Personal information covers all areas of everyday life, and when it is collected in large amounts and from many different people, it is referred to as big data. Personal information is very important both for the country and for citizens, so the need to protect it arises.

4.2 Legal Protection of Personal Information Balancing Public and Private Law

The Personal Information Protection Law is a unique regulation system concerning the use of personal information, which contains elements from both public and private law. The combination of the two kinds of laws in the domain of personal information protection is an opportunity for innovation and development in traditional laws in history. As mentioned by the western experts, imaginations of public law and private law are both created in history. This idea is closely related to the ideologies on the global political field after the 1980s, which still has been lasting till now. However, in the era of big data, due to the fast development of some forces in society such as platforms, algorithms, and data, the focus of the law area is drawn unprecedentedly in this way. Therefore, the particularity of philosophy and legal system of Personal Information Protection Law well reflects this era while bringing great challenges to the classification of public and private laws. From this point, studying the features of the

integration can deepen our cognition on the laws while creating new institutions for public and private laws.

First of all, the Personal Information Protection Law is far away from equality-based operation. Generally speaking, laws concerning personal information protection in the world usually regulate persistent unequal relationships and exclude relationships among people of equal status from the category of those protected by personal information protection. In most cases, the rights of individuals guaranteed through personal information law could interchangeably be converted into collective rights; besides, the right to personal information protection itself is not an absolute right. In the age of the Internet, personal information possesses the dual identity of being both publicly circulating information and having individual characteristics. It means that there could be both excesses and insufficiencies of the protection of personal information which could result in externalities on behalf of social interests. At the same time, the protected interests have a certain degree of differences from the above-mentioned protection approaches.

5 Conclusion

This paper systematically explores the optimization pathways for legal mechanisms protecting personal information in the digital economy through theoretical modeling and normative analysis.

When $sR_4 + vR_4 + (1-\beta)\theta R_4 - \beta(F + I) - C_2 < 0$, $(r_1 - 11 + r_2 - 12)R_2 + L - \beta(1 - C_3) - C_1 > 0$, and $R_4 + vR_4 + 0R_4 - C_2 > 0$, the value of x first exhibits an increasing trend from the initial point, then shifts to a decreasing trend, while the y-value continuously decreases, both converging to the game equilibrium point (0, 0). When sR4 + vR4 + (1 - β)θR4 - β(F + I) - C2 < 0, (r1 - l1 + r2 - l2)R2 + L - β(I - C3) - C1 > 0, and sR4 + vR4 + θR4 - C2 < 0, starting from the initial point, the x-value first exhibits a rapid increasing trend followed by a rapid decreasing trend, while the y-value continuously decreases, both converging toward the stable game point (0, 0). This scenario closely resembles the evolutionary path of Scenario 3, but the rates of increase and decrease for both x and y values are faster than in Scenario 3.

The level of government oversight over costs not only influences the strategic evolution of government departments but also impacts the strategic evolution of other stakeholders, with data providers exhibiting particularly noticeable shifts in their strategic evolution. The level of public awareness and ability to reasonably utilize tools such as agreements to protect information security not only shapes the strategic evolution of the public itself but also influences the strategic evolution of other stakeholders.

About the Author

Daiwei Zhang was born in Zhenlai, Jilin, P.R. China, in 1973. I obtained a bachelor's degree from Northeast Normal University in China. I am currently an associate professor at the Public Security Department of Jilin Police College. My main research direction is Public Security Studies.

References

[1] WANG, Q. (2024). Promote deep integration of real economy and digital economy. Bulletin of Chinese Academy of Sciences (Chinese Version), 39(11), 1830-1833.

[2] Kenderdine, T. (2017). China's industrial policy, strategic emerging industries and space law. Asia & the Pacific Policy Studies, 4(2), 325-342.

[3] Niyazbekova, S. U., Moldashbayeva, L. P., Zhumatayeva, B. A., Mezentseva, T. M., & Shirshova, L. V. (2021). Digital economy development as an important factor for the country's economic growth. In Socio-economic systems: Paradigms for the future (pp. 361-366). Cham: Springer International Publishing.

[4] Pan, W., Xie, T., Wang, Z., & Ma, L. (2022). Digital economy: An innovation driver for total factor productivity. Journal of business research, 139, 303-311.

[5] Ignatov, A. (2020). The digital economy of BRICS: Prospects for multilateral cooperation. International Organisations Research Journal, 15(1), 31-62.

[6] Chen, Y., Xu, S., Lyulyov, O., & Pimonenko, T. (2023). China's digital economy development: Incentives and challenges. Technological and Economic Development of Economy, 29(2), 518-538.

[7] Zainuddin, M., Al Mahi, M., Hassan, M. K., & Khan, S. A. (2024). Platform economy deconstructed: intellectual bases and emerging ethical issues. Research in International Business and Finance, 71, 102497.

[8] Blundo, C., De Maio, C., Parente, M., & Siniscalchi, L. (2021). Targeted advertising that protects the privacy of social networks users. Human-centric Computing and Information Sciences, 11(18).

[9] Montes, R., Sand-Zantman, W., & Valletti, T. (2019). The value of personal information in online markets with endogenous privacy. Management Science, 65(3), 1342-1362.

[10] Lin, H. (2023). Determination of Infringement in Personal Information Leakage under the Accountability Principle and the Security Principle. Law Sci., 2, 263.

[11] Goliński, M. (2021). GAFA: Internal innovators and disruptive monopolists. In Disruptive Platforms (pp. 18-38). Routledge.

[12] Cui, S., & Qi, P. (2021). The legal construction of personal information protection and privacy under the Chinese Civil Code. Computer Law & Security Review, 41, 105560.

[13] Schäfer, H. B. (2023). Current Legal and Economic Problems of Privacy Protection, Data Sharing, and Market-Opening in the Digital Economy. The Antitrust Bulletin, 68(4), 641-656.

[14] Boyne, S. M. (2018). Data protection in the United States. The American Journal of Comparative Law, 66(suppl_1), 299-343.

[15] Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98.

[16] Iaia, V. (2021). The strengthening liaison between data protection, antitrust and consumer law in the German and Italian big data-driven economies. Białostockie Studia Prawnicze,

26(5), 63-74.

[17] Das, A. K. (2018). European Union's General Data ProtectionRegulation, 2018: A brief overview. Annals of Library and Information Studies (ALIS), 65(2), 139-140.

[18] Dhar, T. (2021). The California Consumer Privacy Act: The ethos, similarities and differences vis-a-vis the General Data Protection Regulation and the road ahead in light of California Privacy Rights Act. Journal of Data Protection & Privacy, 4(2), 170-192.

[19] Marelli, L., & Testa, G. (2018). Scrutinizing the EU general data protection regulation. Science, 360(6388), 496-498.

[20] Dayalu, P., & Punnagai, M. (2019). GDPR: A Privacy Regime. International Journal of Trend in Scientific Research and Development, 713.

[21] Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. computer law & security review, 35(4), 380-397.

[22] Poladov, A. (2020). Data Protection Rules in the United States Legal System. Law Rev. Kyiv UL, 481.

[23] Stallings, W. (2020). Handling of personal information and deidentified, aggregated, and pseudonymized information under the California consumer privacy act. IEEE Security & Privacy, 18(1), 61-64.

[24] Cramer, J. (2023). Privacy, data sharing, and other legal considerations. The Surgical Clinics of North America, 103(2), 347-356.

[25] Shao, Y. (2021). Personal information protection: China's path choice. US-China L. Rev., 18, 227.

[26] Gong, N. (2023). Protection of personal data in China: Legislation in the digital age. Vestnik Saint Petersburg UL, 159.

[27] Cheng, W. (2021). Selection of a model for civil law protection of personal information. Social Sciences in China, 42(1), 117-134.

[28] Ren, H. (2024, July). International Law Protection of Cross-Border Transfers of Personal Information Based on Cloud Computing and Big Data. In Forum on Research and Innovation Management (Vol. 2, No. 3).

[29] Chungang, M. (2024). Consumer Personal Information Protection from a Comparative Law Perspective. Journal of Global Research in Education and Social Science, 18(4), 30-34.

[30] Creemers, R. (2022). China’s emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011.

[31] Li, Q., Jiang, T., & Fan, X. (2023). Examining Sensitive Personal Information Protection in China: Framework, Obstacles, and Solutions. Information & Culture, 58(3), 247-273.

[32] Hu, C. (2022). Protection of personal information in the era of big data. Front. Human. Soc. Sci, 2, 184-193.

[33] Kimmelman, E., Feld, H., & Rossi, A. (2018). The limits of antitrust in privacy protection. International Data Privacy Law, 8(3), 270-276.

[34] Shapiro, C. (2019). Protecting competition in the American economy: Merger control, tech titans, labor markets. Journal of Economic Perspectives, 33(3), 69-93.

[35] Schrepel, T. (2018). Is Blockchain the death of antitrust law? The Blockchain antitrust paradox. Geo. L. Tech. Rev., 3, 281.

[36] Iman, N. (2024). The fight for our personal data: analyzing the economics of data and privacy on digital platforms. International Journal of Law and Management, 66(6), 774-791.

[37] Malgieri, G., & Custers, B. (2018). Pricing privacy–the right to know the value of your personal data. Computer Law & Security Review, 34(2), 289-303.