symmetry

MDPI

Article

Dynamic Evolution Analysis of Incentive Strategies and Symmetry Enhancement in the Personal-Data Valorization Industry Chain

Jun Ma [1,*], Junhao Yu [2] and Yingying Cheng [2]

[1] School of Information Management, Zhengzhou University, Zhengzhou 450001, China
[2] School of Business, Henan University of Science and Technology, Luoyang 471023, China; 230320291684@stu.haust.edu.cn (J.Y.); 9906180@haust.edu.cn (Y.C.)
* Correspondence: skcg@haust.edu.cn

Abstract

The value of personal data can only be unlocked through efficient circulation. This study explores a multi-party collaborative mechanism for personal-data trading, aiming to improve data quality and market vitality via incentive-compatible institutional design, thereby supporting the high-quality development of the digital economy. Symmetry enhancement refers to the use of strategies and mechanisms to narrow the information gap among data controllers, operators, and demanders, enabling all parties to facilitate personal-data transactions on relatively equal footing. Drawing on evolutionary-game theory, we construct a tripartite dynamic-game model that incorporates data controllers, data operators, and data demanders. We analyze how initial willingness, payoff structures, breach costs, and risk factors (e.g., data leakage) shape each party's strategic choices (cooperate vs. defect) and their evolutionary trajectories, in search of stable equilibrium conditions and core incentive mechanisms for a healthy market. We find that (1) the initial willingness to cooperate among participants is the foundation of a virtuous cycle; (2) the net revenue of data products significantly influences operators' and demanders' propensity to cooperate; and (3) the severity of breach penalties and the potential losses from data leakage jointly affect the strategies of all three parties, serving as key levers for maintaining market trust and compliance. Accordingly, we recommend strengthening contract enforcement and trust-building; refining the legal and regulatory framework for data rights confirmation, circulation, trading, and security; and promoting stable supply–demand cooperation and market education to enhance awareness of data value and compliance, thereby stimulating individuals' willingness to authorize the use of their data and maximizing its value.

Keywords: personal data; data trusteeship; value realization; evolutionary game; multi-agent

check for updates

Academic Editor: Sergei Odintsov

Received: 27 August 2025
Revised: 16 September 2025
Accepted: 20 September 2025
Published: 3 October 2025

Citation: Ma, J.; Yu, J.; Cheng, Y. Dynamic Evolution Analysis of Incentive Strategies and Symmetry Enhancement in the Personal-Data Valorization Industry Chain. *Symmetry* **2025**, *17*, 1639. https://doi.org/10.3390/sym17101639

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In the digital-economy era, personal data has become a core production factor whose value is being continuously unlocked in fields such as smart transportation, precision marketing, and health management. China's data-factor market is expanding rapidly, with an average annual compound growth rate of roughly 20%, and is expected to exceed CNY 174.9 billion by 2025 [1]. Driving the market-oriented circulation and efficient utilization of personal data has become a key pathway for activating data value and empowering the real economy. The establishment of a personal-data valuation industry chain will create a win–win ecosystem: it not only accelerates the circulation of personal data in the

marketplace but also provides convenience for data-demand parties, thereby fostering the development of both personal-data flows and the data-element market at large.

President Xi Jinping has emphasized the need to "promote efficient data circulation on the basis of data security." In response, policies such as the "20 Data Articles" and the Personal-Information Protection Law have been formulated to build an institutional framework that clarifies corporate responsibility and safeguards individual rights [2]. Academia has also actively explored solutions, identifying core bottlenecks such as incomplete top-level design [3], low levels of circulation and sharing, generalized contracts [4], and deficiencies in public-power governance [5], and has proposed industry-chain models led by operators or governments [6]. Today, "data chimneys" are everywhere: personal data are scattered among government agencies and a multitude of internet platforms, each hoarding its own slice of the population's digital footprint. Across firms the information never moves, so every database becomes an island. Incumbents whose existing holdings are already sufficient for day-to-day operations shy away from releasing data to the market, worried about the security bill and the legal liability that could follow. At the other extreme, some players chase illicit profit by leaking or selling personal datasets, trampling on privacy and individual rights. The root problem is a double asymmetry—of information and of incentives—between those who control the data and those who could create value from it. Although existing studies have noted the multi-stakeholder conflicts of interest, they have yet to adequately investigate the dynamic incentive mechanisms that drive coordinated industry-chain evolution and the micro-level behavioral interaction patterns. Against this backdrop, to fully unlock the value of personal data and facilitate its circulation, there is an urgent need for a new incentive mechanism within an industrial model that monetizes personal data to promote its utilization.

In the marketization of personal data, three actors coexist in specific scenarios: data controllers, personal-data operators, and data buyers. Their decisions are intertwined across multiple margins: controllers must choose whether to release or withhold data; operators must decide whether to monetize or leave the asset idle; buyers, when analytics require the data, must opt to purchase or go without. To capture these trade-offs, we build an evolutionary-game model that simulates the strategy spaces of all three parties and solves for their equilibrium. Comparative runs then trace how costs, revenues, potential losses, and breach penalties shift behavior in the personal-data marketplace. The findings yield targeted policy recommendations and practical guidance for constructing a secure and efficient industrial chain for personal-data valuation. The remainder of the paper is organized as follows. Section 2 reviews the domestic and international literature. Section 3 formulates the research question and constructs the game-theoretic model. Section 4 derives and analyzes the equilibrium solutions and examines their stability. Section 5 presents numerical simulations and discusses the results. Section 6 concludes the study and offers policy recommendations.

2. Literature Review

2.1. The Value Chain for Personal-Data Monetization

With the digital economy rapidly expanding, personal data has become a critical production factor, and constructing its monetization value chain has drawn intense attention from both academia and industry. The circulation of personal data is inherently risky; scholars have therefore focused on data security and privacy protection throughout the process. Gu et al. employed text content analysis to examine six representative privacy policies of digital resource providers, analyzing the collection and compliant use of library users' personal data, and proposed insights for personal-data security management in libraries [7]. Song categorized personal data into three types: subject-supplied data, subject behavior data, and processed derivative data, and proposed corresponding legal protection measures for the property rights of each type. Based on multi-granular data, he explored

differential privacy protection, classifying personal data according to "personal value" and "social attributes" to clarify the boundary between privacy protection and reasonable data use, making privacy protection more targeted [8].

Before personal data can be commercialized, their ownership must be allocated—a step that cannot be bypassed. How to distribute data rights in a way that energizes market participants' initiative and creativity has become a central question in the academic debate. Wang, focusing on the characteristics of data and the configuration of rights, proposes separating the rights to possess, process, and operate personal data, and assigning the resulting property interests to the parties that contribute labor, thereby realizing the social value of data [9]. Cui proposes a "residual control right over data" regime that seeks to balance industrial development with data security. By clarifying the scope and subject of these rights, the regime offers an institutional basis for data transactions [10]. Xiang and Gao, employing literature analysis and comparative methods, expound on the fundamental content of personal-data rights, pointing out that the protection of personal-data personality rights is becoming increasingly mature, whereas the safeguarding of personal-data property rights is confined to preventing illegal transactions [11]. Xu analyzes the distinctions and connections between personal-information rights and data rights, proposing a flexible data-protection mechanism that balances and reconciles personal-information rights (as personality rights) with data rights (as property rights) [12].

Regarding data-trading mechanisms, scholars have focused on issues such as contractual constraints, benefit distribution, and trust-building mechanisms. Fei and Chen argue that current contracts are insufficient to handle the invalidation caused by consent withdrawal [13]. Xia, approaching the issue from private-law theory, contends that existing law fails to curb the loss of control over personal data or to ensure fair value, and suggests using contract-law doctrines to rebalance the parties' positions [14]. Cheng, from the standpoint of personal-information protection, stresses that individuals should enjoy not only autonomy interests but also economic ones; they should be able to authorize others to commercialize their information and receive monetary returns [15]. Fu builds on trust-law theory, crafting a governance structure composed of beneficiaries, data processors, trust administrators, and trust oversight bodies, and advances a data-trust system that allows the benefits of data assets to be shared [16]. Rao further observes that the crisis of trust in data markets stems from concerns over security and quality; he recommends instruments such as registries of data holdings, cybersecurity insurance, and self-regulation by exchanges to dismantle these barriers [4]. In summary, scholars have examined the personal-data value chain from multiple angles—covering privacy protection in circulation, rights allocation, and trading mechanisms—providing a rich foundation for further research and practice.

2.2. Applications of Evolutionary-Game Theory

As a tool for studying multiple agents' strategic choice and its dynamic evolution, evolutionary-game theory has been increasingly applied to data governance in recent years, furnishing a rigorous foundation for dissecting the interests and behavioral options that shape data markets. Rooted in the assumption of bounded rationality, the theory effectively captures the mutual influences among agents when they select behavioral strategies. It has already been successfully employed in such areas as data-value assessment, authorization-mechanism design, privacy and security protection, and benefit distribution.

The sharing of personal data is hindered by privacy concerns, prompting scholars to explore how to strike a balance between securing such data and exploiting its value. Wei examines the strategic choices and dynamic evolution of both data subjects and data firms from the perspective of personal-information protection, concluding that an optimal mix of policy instruments—administrative regulation, internal industry governance, and judicial

liability—is required to simultaneously promote data sharing and safeguard personal information [17]. Wang Zhong and others argue that authorization rules can mitigate the conflict between privacy protection and the circulation of personal data. Taking the personal-data authorization mechanism as their research object, they analyze the selection of authorization mechanisms under varying levels of data sensitivity and their dynamic evolution patterns [18]. Wan employs a Stackelberg game model to examine the impact of external attacks on large-scale genomic data sharing, finding that the majority of data can be shared effectively with a low risk of re-identification [19]. Zhang et al. construct an evolutionary game involving government, data suppliers, and data demanders to tackle the absence of a trusted circulation system and the resulting data-flow shortage, showing that government plays a pivotal role in bringing both sides to market and building a trusted trading environment [20].

Scholars have also conducted research on questions such as how to reasonably assess the value of personal data and how to distribute the resulting benefits. Liu et al. address the data-pricing problem in large-language-model settings by proposing an evaluation method for data-privacy levels that incorporates differential privacy [21]. Shang et al. introduce the concept of a data-benefit right and employ evolutionary-game analysis to achieve fairness and efficiency in benefit distribution [22]. Huang constructs a personal-data-pricing model based on the value measurement of privacy utility for personal big data and, through a labor–capital game, analyzes the benefit-allocation problem in data transactions [23]. Guo et al. design trading rules for personal health data via an iterative double-auction approach and use a distributed iterative algorithm to mitigate the supply–demand imbalance in health-data markets [24].

In sum, researchers have intensively investigated personal-data governance and value realization from four inter-related perspectives—privacy protection, rights allocation, trading mechanisms, and value assessment/distribution—laying a solid foundation for the present study. Yet micro-level, dynamic analyses of the incentives that animate the personal-data value chain remain scarce. The overarching goal of the digital economy is to strengthen personal-data protection, refine the ways data are traded and used, and guarantee that every use is lawful, legitimate, and transparent, thereby fostering a healthy data ecosystem. Evolutionary-game theory has proved fruitful in studying information-sharing behaviors such as medical-data exchange [25] and knowledge interaction [26]; we therefore apply it to personal-data transactions. By embedding cost, benefit, and risk parameters into the payoff structure, we simulate the strategic choices and evolutionary trajectories of the three key actors—data controllers, personal-data operators, and data buyers—uncovering the inner workings of the incentive mechanisms that drive the commercialization process. The findings offer both theoretical insight and practical guidance for building a secure, efficient, and sustainable personal-data value chain.

3. Model Construction

3.1. Problem Description

In the realm of personal-data development, individual-data operators leverage blockchain-based virtual platforms to create a new model for personal-data operation and services that simultaneously safeguard the rights of both data controllers and data demanders. Acting as the pivotal node linking upstream and downstream participants in the personal-data market, the operator's primary responsibility is to aggregate the data resources controlled by upstream data controllers, perform secondary development and utilization of these resources, and then trade the resulting data products with downstream demanders. Individuals retain control over their data; accordingly, both corporate data-circulation decisions and any development or sale of personal data by the operator must obtain the individuals' consent. To simplify the model, the paper assumes that every request for consent—whether from a data controller or from the operator—is always granted.

Because data demanders have highly individualized needs that the operator cannot fully anticipate, demanders must specify their exact requirements to the operator in advance. The two parties then formalize these requirements in a data-service contract. This contract mitigates information asymmetry among data controllers, the operator, and data demanders, thereby strengthening trust and collaboration. It also binds all parties: any participant who unilaterally and unjustifiably exits the value chain is liable for stipulated damages. To streamline the process, the model posits that a contract is deemed signed if and only if at least two of the three parties—data controller, operator, and data demander—remain active in the value chain. Conversely, if only one or none of the parties participates, the contract is regarded as unsigned.

To further investigate how contracts function during the nascent phase of the personal-data market and how the resulting outcomes feed back into participants' behavior, the study explores how to optimize incentive mechanisms that unlock the value of personal data and foster effective cooperation among relevant stakeholders. Under the given contractual framework, the research examines how various parameters—such as data-collection costs, data-development revenues, and breach-of-contract penalties—affect the path toward equilibrium, providing a scientific basis for informed decision-making.

3.2. Model Assumptions

The tripartite strategic relationship among the data controller, the personal-data operator, and the data demander is illustrated in Figure 1. Specifically, the data controller conducts its business and, with the data subject's consent, provides services in the course of which personal data are generated and stored. The controller then decides whether to allow the data to circulate. Choosing circulation enables data appreciation and thus yields additional revenue, yet it also exposes the controller to reputational losses stemming from potential data breaches; the controller's strategy set is {Circulate, Not Circulate}. The personal-data operator determines whether to utilize the circulated data. Opting to utilize entails investing in data-product development costs while bearing the risks of fluctuating market demand and the possibility of losses if no demand materializes after development; the operator's strategy set is {Utilize, Not Utilize}. The data demander decides whether to purchase the required data resources or products from the value chain. Choosing to purchase allows the demander to acquire the needed data products or services at a relatively low cost, whereas choosing not to purchase means the demander does not participate in personal-data trading; the demander's strategy set is {Purchase, Not Purchase}.

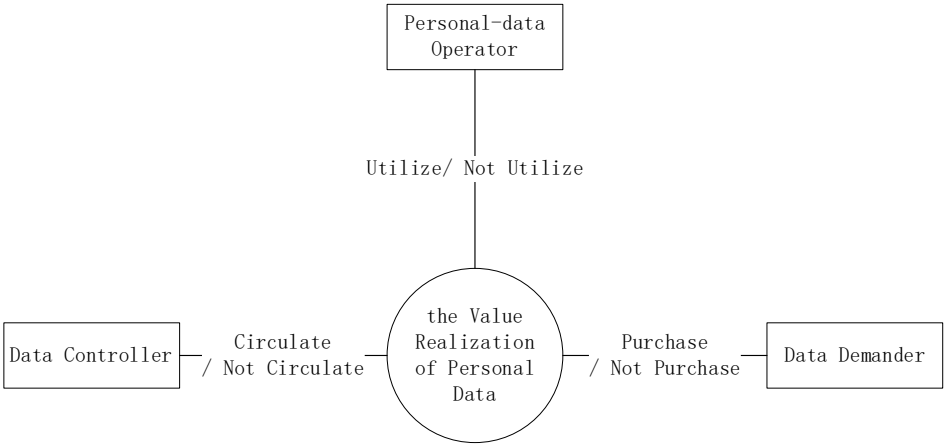


Figure 1. Evolutionary-game model among the data controller, the personal-data operator, and the data demander.

Assumption 1. *The data controller, the personal-data operator, and the data demander are all boundedly rational agents who exhibit cognitive biases regarding external risks, the usability of data resources, and the value those resources generate. In the short run, each of the three strategic actors is oriented toward profit maximization, and its behavior follows a probabilistic distribution. Over the long run, however, the three parties will establish a stable cooperative relationship, actively contribute their data resources, and develop more valuable data products.*

Assumption 2. *Let x denote the proportion of data controllers who choose to circulate data, and $1-x$ the proportion who choose not to circulate, with $x \in [0,1]$. Let y denote the proportion of personal-data operators who choose to utilize the data, and $1-y$ the proportion who choose not to utilize, with $y \in [0,1]$. Let z denote the proportion of data demanders who choose to purchase, and $1-z$ the proportion who choose not to purchase, with $z \in [0,1]$.*

Assumption 3. *Revenues and costs of the data controller. When the data controller chooses to circulate data, the controller obtains a data-circulation revenue $ra1$ whenever the personal-data operator participates, regardless of whether the data demander joins. Likewise, whenever the data demander participates, the controller receives a data-product sharing revenue $ra2$, regardless of whether the personal-data operator joins. When the data controller opts to circulate data, the total cost incurred is $ca1$, which comprises both (1) the time and monetary costs expended in negotiating contract terms and profit-sharing arrangements before the agreement is reached, and (2) the mandatory entry costs stipulated by the government, such as investments in machinery, equipment, and technological infrastructure.*

Assumption 4. *Revenues and costs of the personal-data operator. Let $cb1$ denote the total cost borne by the personal-data operator when the data controller chooses to circulate data, and $cb2$ the corresponding cost when the controller refrains from circulation. Each of these costs encompasses (1) the time and monetary expenditures incurred in pre-contract negotiations over contract terms and profit-sharing arrangements, and (2) the expenses required to develop and utilize the data, such as personnel and equipment outlays. Because the controller's decision to circulate data reduces the operator's difficulty in obtaining data, we have $cb2 > cb1$. If the controller chooses to circulate data and the data demander opts to purchase, the personal-data operator earns a revenue $rb1$ from selling the data product.*

Assumption 5. *Benefits and costs of the data demander. The data demander's requirement is fixed: regardless of whether data are obtained from a personal-data operator or directly from the data controller, the final benefit is the same. If the data controller chooses to circulate the data and the personal-data operator chooses to use them, the data demander's benefit is $rc1$ and the cost of collecting and processing the data is $cc1$. If the data controller chooses to circulate the data but the personal-data operator chooses not to use them, the data demander's benefit is $rc1$ and the cost of collecting and processing the data is $cc2$. If the data controller chooses not to circulate the data, the data demander's benefit and cost are both zero.*

Assumption 6. *Breach-of-contract damages. Subject to the existence of a concluded agreement, the damages payable in the following contingencies are as follows: Scenario 1: All three parties participate and, although the agreement sets out obligations, none defaults; no party is liable for breach-of-contract damages $cc3$. Scenario 2: Under the agreement, the data controller and the personal-data operator participate, but the data requester does not; the data requester must pay the personal-data operator breach-of-contract damages $cb3$. Scenario 3: Under the agreement, the data controller and the data requester participate, but the personal-data operator does not; the personal-data operator must pay the data requester breach-of-contract damages $ca3$. The variables and parameters involved in the above model are detailed in* Appendix A.

3.3. Payoff Matrix

Based on the above assumptions, when the data controller of circulating data chooses the strategy of "circulation," the personal-data developer chooses "utilization," and the data demander chooses "purchase," the data controller's payoff equals the sum of the circulation revenue from personal data ($ra1$) and the revenue from the data product ($ra2$), minus the indispensable cost of entering the industrial chain ($cb1$) and the reputational loss caused by a data leak during the circulation and use of personal data ($s1$). In the same way, the payoff formulas for data controllers, personal-data operators, and the data demanders can be derived; they are shown in Table 1.

Table 1. Payoff matrix for the tripartite game of personal-data valorization.

Data Controllers	Personal-Data Operators	Data Demanders	
		Purchase	**Not Purchase**
Circulate	Utilize	$ra1 + ra2 - ca1 - s1$, $rb1 - cb1 - s2$, $rc1 - cc1 - s3$	$ra1 - ca1 - s1$, $rb1 - cb1 + cc3 - s2$, $-cc3$
	Not Utilize	$ra1 - ca1 - s1$, $-cb3$, $rc1 - cc2 + cb3 - s3$	$-ca1$, 0, 0
Not Circulate	Utilize	$-ca3$, $-cb2 + ca3$, $-cc1$	0, $-cb2$, 0
	Not Utilize	0, 0, $-cc2$	0, 0, 0

Suppose the data controller's expected payoff when choosing to circulate personal data is U_{11}, the expected payoff when choosing not to circulate personal data is U_{12}, and the data controller's average payoff is U_1.

$$U_{11} = y*z*(ra1 + ra2 - ca1 - s1) + y*(1-z)*(ra1 - ca1 - s1) + (1-y)*z*(ra2 - ca1 - s1) + (1-y)*(1-z)*(-ca1) \quad (1)$$

$$U_{12} = -ca3*y*z \quad (2)$$

$$U_1 = x*U_{11} + (1-x)*U_{12} = ca3*y*z*(x-1) - x*(y*z*(ca1 - ra1 - ra2 + s1) + ca1*(y-1)*(z-1) - y*(z-1)*(ca1 - ra1 + s1) - z*(y-1)*(ca1 - ra2 + s1)) \quad (3)$$

Similarly, according to the calculation formula of the replicator dynamic equation, the replicator dynamic equations for the data controller, the personal-data operator, and the data demander are, respectively, as follows:

$$f(x) = x(U_{11} - U_1) = -x*(x-1)*(ra1*y - ca1 - s1*y + ra2*z - s1*z + ca3*y*z + s1*y*z) \quad (4)$$

$$f(y) = y(U_{21} - U_2) = y*(y-1)*(cb2 + cb1*x - cb2*x - cc3*x - ca3*z - rb1*x + s2*x + ca3*x*z - cb3*x*z + cc3*x*z) \quad (5)$$

$$f(z) = z(U_{31} - U_3) = z*(z-1)*(cc2 - cb3*x + cc1*y - cc2*y - rc1*x + s3*x + cb3*x*y - cc3*x*y) \quad (6)$$

4. Evolutionary-Game Model Analysis

The strategic choices of the data controller, the personal-data operator, and the data demander constitute a dynamic process. When each party's replicator dynamic equation equals zero, the game reaches stability. Setting $f(x) = f(y) = f(z) = 0$ yields nine potential equilibrium points: [$E_1(0,0,0)$, $E_2(1,0,0)$, $E_3(0,1,0)$, $E_4(0,0,1)$, $E_5(1,1,0)$, $E_6(0,1,1)$, $E_7(1,1,0)$, $E_8(1,1,1)$, $E_9(x^*,y^*,z^*)$]. Because potential stable points in evolutionary games must satisfy strict Nash equilibrium conditions, only the eight pure-strategy solutions are analyzed.

Stability Assessment

According to evolutionary-game stability theory, the Jacobian matrix is employed to examine the local stability of equilibrium points in the strategy space [27]. One computes the eigenvalues of the Jacobian and evaluates them at each candidate equilibrium. If the real parts of all eigenvalues are negative, the equilibrium is asymptotically stable. Using the replicator dynamic equations for data controllers, personal-data operators, and data demanders, the Jacobian matrix J is constructed as shown in Equation (7).

$$J = \begin{bmatrix} \frac{f(x)}{\partial x} & \frac{f(x)}{\partial y} & \frac{f(x)}{\partial z} \\ \frac{f(y)}{\partial x} & \frac{f(y)}{\partial y} & \frac{f(y)}{\partial z} \\ \frac{f(z)}{\partial x} & \frac{f(z)}{\partial y} & \frac{f(z)}{\partial z} \end{bmatrix} = \begin{bmatrix} f_{11} & f_{12} & f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{bmatrix} \tag{7}$$

where,

$$f_{11} = -(x-1)*(ra1*y - ca1 - s1*y + ra2*z - s1*z + ca3*y*z + s1*y*z) \\ -x*(ra1*y - ca1 - s1*y + ra2*z - s1*z + ca3*y*z + s1*y*z)$$

$$f_{12} = -x*(x-1)*(ra1 - s1 + ca3*z + s1*z)$$

$$f_{13} = -x*(x-1)*(ra2 - s1 + ca3*y + s1*y)$$

$$f_{21} = y*(y-1)*(cb1 - cb2 - cc3 - rb1 + s2 + ca3*z - cb3*z + cc3*z)$$

$$f_{22} = y*(cb2 + cb1*x - cb2*x - cc3*x - ca3*z - rb1*x + s2*x + ca3*x*z \\ -cb3*x*z + cc3*x*z) + (y-1)*(cb2 + cb1*x - cb2*x - cc3*x - ca3*z - rb1*x \\ +s2*x + ca3*x*z - cb3*x*z + cc3*x*z)$$

$$f_{23} = -y*(y-1)*(ca3 - ca3*x + cb3*x - cc3*x)$$

$$f_{31} = -z*(z-1)*(cb3 + rc1 - s3 - cb3*y + cc3*y)$$

$$f_{32} = z*(z-1)*(cc1 - cc2 + cb3*x - cc3*x)$$

$$f_{33} = z*(cc2 - cb3*x + cc1*y - cc2*y - rc1*x + s3*x + cb3*x*y - cc3*x*y) \\ +(z-1)*(cc2 - cb3*x + cc1*y - cc2*y - rc1*x + s3*x + cb3*x*y - cc3*x*y)$$

By substituting each equilibrium point into the Jacobian matrix in turn, the corresponding eigenvalues are obtained as shown in Table 2.

According to Lyapunov's indirect method, an equilibrium is judged asymptotically stable only if **all** eigenvalues of its Jacobian matrix are strictly negative. If at least one eigenvalue is positive, the equilibrium is a saddle (i.e., unstable). When the Jacobian possesses both zero and negative eigenvalues, the equilibrium is in a critical state and its stability cannot be determined from the linearization alone. Under these criteria and assumptions, the four candidate equilibria $E_2(1,0,0)$, $E_3(0,1,0)$, $E_4(0,0,1)$, $E_7(0,1,1)$ are unstable, whereas the remaining four candidates $E_1(0,0,0)$, $E_5(1,1,0)$, $E_6(1,0,1)$, $E_8(1,1,1)$

are stable. Proceeding from this, we now perform a **local stability analysis** of these four stable equilibria.

Table 2. Stability analysis of equilibria in the tripartite evolutionary game.

Equilibrium Point	Eigenvalues λ_1	Eigenvalues λ_2	Eigenvalues λ_3	Stability Analysis
$E_1(0,0,0)$	$-ca1 < 0$	$-cb2 < 0$	$-cc2 < 0$	ESS
$E_2(1,0,0)$	$ca1 > 0$	$cc3 - cb1 + rb1 - s2$	$cb3 - cc2 + rc1 - s3$	Unstable
$E_3(0,1,0)$	$cb2 > 0$	$-cc1 < 0$	$ra1 - ca1 - s1$	Unstable
$E_4(0,0,1)$	$cc2 > 0$	$ca3 - cb2$	$ra2 - ca1 - s1$	Unstable
$E_5(1,1,0)$	$ca1 - ra1 + s1$	$cb1 - cc3 - rb1 + s2$	$cc3 - cc1 + rc1 - s3$	Saddle OR ESS
$E_6(0,1,1)$	$ca1 - ra1 + s1$	$cb3 - cb1 + rb1 - s2$	$cc2 - cb3 - rc1 + s3$	Saddle OR ESS
$E_7(1,0,1)$	$cc1 > 0$	$cb2 - ca3$	$ca3 - ca1 + ra1 + ra2 - s1$	Unstable
$E_8(1,1,1)$	$ca1 - ca3 - ra1 - ra2 + s1$	$cb1 - cb3 - rb1 + s2$	$cc1 - cc3 - rc1 + s3$	Saddle OR ESS

Scenario 1. *For equilibrium point $E_1(0,0,0)$, it is asymptotically stable when the conditions $ca1 > 0$, $cb2 > 0$, and $cc2 > 0$ are simultaneously satisfied. For personal-data operators, any attempt to produce data products would require acquiring data through informal channels, incurring exorbitant collection costs and making the development of data products unprofitable. In practice, once data controllers adopt a strategy of withholding personal data from circulation, the choices of personal-data operators and data demanders become irrelevant: for data demanders, the risk–cost of participation is prohibitively high. This corresponds to the initial stage of the personal-data value chain, when the market for personal data is still nascent. Both supply and demand sides show limited enthusiasm for trading personal-data products; data controllers participate only reluctantly, personal-data resources remain largely immobile, and data value is difficult to realize. The stability of point $E_1(0,0,0)$ therefore illustrates that low participation incentives across all parties foster an overriding concern with costs and a fear of losses. Ultimately, this breeds distrust and deters cooperation throughout the value chain.*

Scenario 2. *For equilibrium point $E_5(1,1,0)$, asymptotic stability is achieved under the joint conditions $ra1 > ca1 + s1$, $cc3 + rb1 > cb1 + s2$, and $cc3 + rc1 < cc1 + s3$. By assumption, when the payoff that data controllers derive from data circulation is sufficiently large, they become willing to circulate personal data. At the same time, once the indemnity that personal-data operators receive exceeds their total development costs, these operators are inclined to exploit the data. However, if the penalty that data demanders must pay for breach of contract plus the benefit they obtain from purchasing the data product is still lower than their total cost of acquiring and using the product, the contractual constraint on demanders is effectively weak. Consequently, whenever the expected benefit from the data product falls short, demanders will opt not to purchase it from the operators. This configuration corresponds to the **growth stage** of the personal-data value chain.*

Scenario 3. *For equilibrium point $E_6(1,0,1)$, asymptotic stability is achieved under the joint conditions $ra1 > ca1 + s1$, $cb3 + rb1 < cb1 + s2$, and $cb3 + rc1 > cc2 + s3$. Under the assumed conditions, it can be observed that when the combined costs of developing personal-data circulation and the potential losses from a data breach outweigh both regulatory penalties and the revenues from data-product development, neither data controllers nor personal-data operators will choose to participate in the value chain. This reveals that, given the prevailing contractual safeguards and privacy technologies, if these stakeholders perceive the risk of a data leak as excessively high—or the resulting damage as too severe—the strategic choices of the other two parties cannot induce them to alter their decision to stay out. Such a scenario corresponds to an early stage of the personal-data monetization value chain.*

Scenario 4. *For equilibrium point $E_8(1,1,1)$, asymptotic stability is achieved under the joint conditions $ra1 + ra2 + ca3 > ca1 + s1$, $cb3 + rb1 > cb1 + s2$, and $cc3 + rc1 > cc1 + s3$. At*

this point, the penalty for breach paid by the data controller, together with the gains from circulating personal data and the revenues from personal-data products, exceeds the sum of total circulation costs and reputational losses; consequently, the data controller is inclined to opt for the circulation of personal data. Because the controller circulates the data, data buyers purchase the resulting products, and the personal-data operator earns additional revenue from developing and selling those products. Since the operator's losses are smaller than the proceeds from product sales, the operator is strongly motivated to participate actively. The engagement of both the data controller and the operator lowers the acquisition-and-processing costs for data buyers; moreover, as long as buyers do not breach their agreements, the value they derive from the data products surpasses their acquisition costs. This constellation forms an ideal state of cooperation among all value-chain participants, fostering the realization of personal-data value. Such a scenario corresponds to the mature stage of the personal-data monetization value chain and constitutes the focus of the subsequent analysis.

5. Data Simulation and Results Analysis

5.1. Parameter Analysis

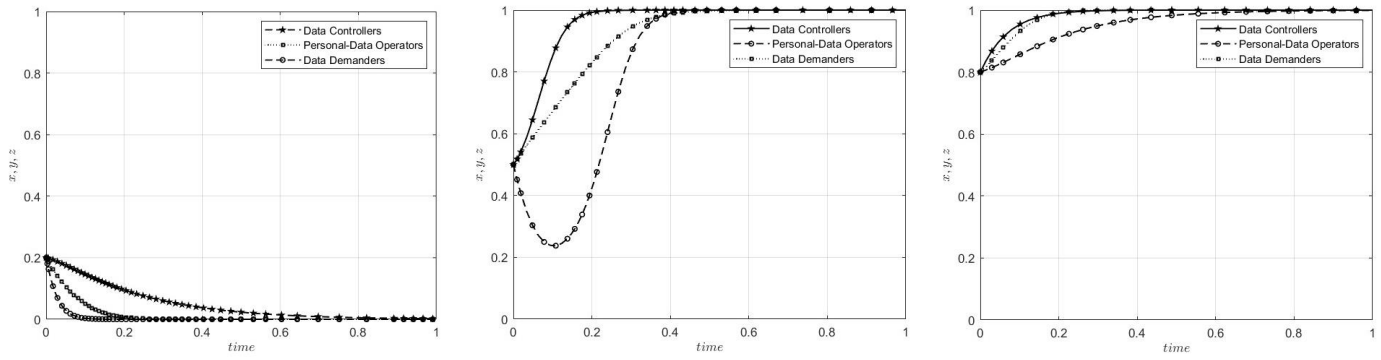
The asymptotic stability of the model is influenced by the initial values assigned to the relevant parameters. To achieve the desired stable state of $E_8(1,1,1)$, and under the constraints $ra1 + ra2 + ca3 > ca1 + s1$, $cb3 + rb1 > cb1 + s2$, and $cc3 + rc1 > cc1 + s3$, this study—guided by expert recommendations—first sets the initial probabilities of the tripartite behavioral strategies to [0.5, 0.5, 0.5]. Benchmark initial values for all parameters are then assigned as shown in Table 3. On this basis, parameters such as initial willingness, default compensation, net data-product revenue, and privacy-breach losses are adjusted to investigate their influence on the strategic evolution of the three stakeholders.

Table 3. Initial parameter values for simulation analysis.

Parameter	$ra1$	$ra2$	$ca1$	$ca3$	$s1$	$rb1$	$cb1$	$cb2$
Initial Value	10	15	5	4	5	25	12	18
Parameter	$cb3$	s2	$rc1$	$cc1$	$cc2$	$cc3$	$s3$	
Initial Value	7	5	15	10	12	2	5	

5.1.1. Impact of Initial Willingness

While keeping all other parameters at their benchmark values, only the initial willingness of the three parties—data controllers, personal-data operators, and data demanders—to participate in the personal-data value chain is varied. Three scenarios are examined: low, medium, and high willingness. The parameter settings are as follows: low willingness: (0.2, 0.2, 0.2), medium willingness: (0.5, 0.5, 0.5), high willingness: (0.8, 0.8, 0.8). The resulting evolutionary trajectories are shown in Figure 2. When the initial willingness is low (0.2, 0.2, 0.2), y and z rapidly approach 0, and x—under their influence—slowly converges to 0 as well, driving the final equilibrium toward (0, 0, 0). In contrast, when initial willingness is medium or high, x first converges to 1, followed sequentially by y and z, so the system ultimately settles at (1, 1, 1). Moreover, the high-willingness scenario (0.8, 0.8, 0.8) reaches equilibrium faster than the medium-willingness scenario (0.5, 0.5, 0.5). Therefore, maintaining a high initial willingness across data controllers, personal-data operators, and data demanders facilitates the attainment of the desired equilibrium (1, 1, 1).

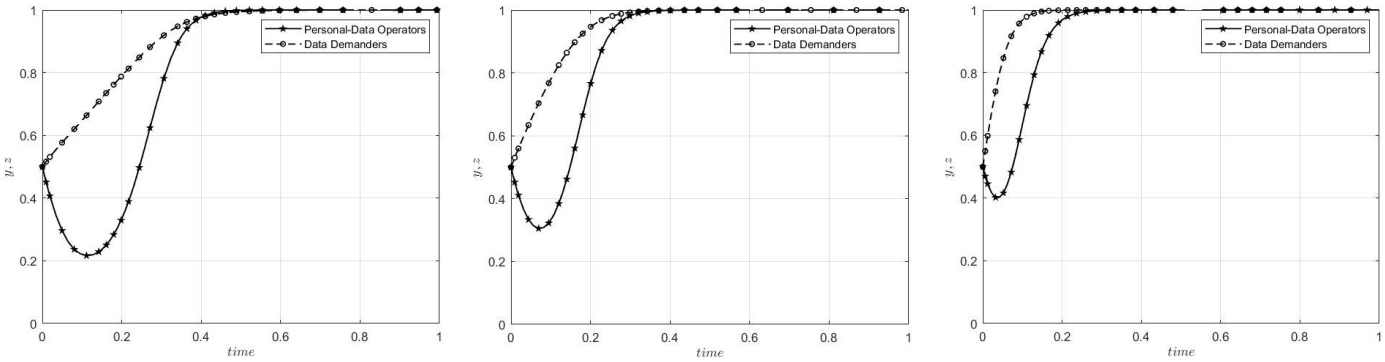


(**a**) (**b**) (**c**)

Figure 2. (**a**) Evolutionary trajectory of strategies for various participants under low initial willingness; (**b**) evolutionary trajectory of strategies for various participants under moderate initial willingness; (**c**) evolutionary trajectory of strategies for various participants under high initial willingness.

5.1.2. Impact of Breach Penalties on Personal-Data Operators and Data Demanders

While holding all other parameters at their benchmark values, only the breach-penalty amounts for personal-data operators and data demanders are varied simultaneously to examine how these penalties influence the evolutionary paths of their strategic choices. Based on the baseline values *cb*3 and *cc*3, the penalties are scaled proportionally to (7, 2), (14, 4), and (28, 8). The resulting evolutionary trajectories are shown in Figure 3. Figure 3 reveals that altering the breach-penalty values affects the strategic decisions of both personal-data operators and data demanders. As the compensation for unjustified withdrawal from the contract increases, the probability and speed with which both parties converge toward 1 rise markedly. This indicates that higher breach penalties enhance the incentives for personal-data operators and data demanders to actively engage in personal-data transactions. Specifically, the larger the penalties, the stronger the willingness of personal-data operators to "utilize" the data and of data demanders to "purchase" it.



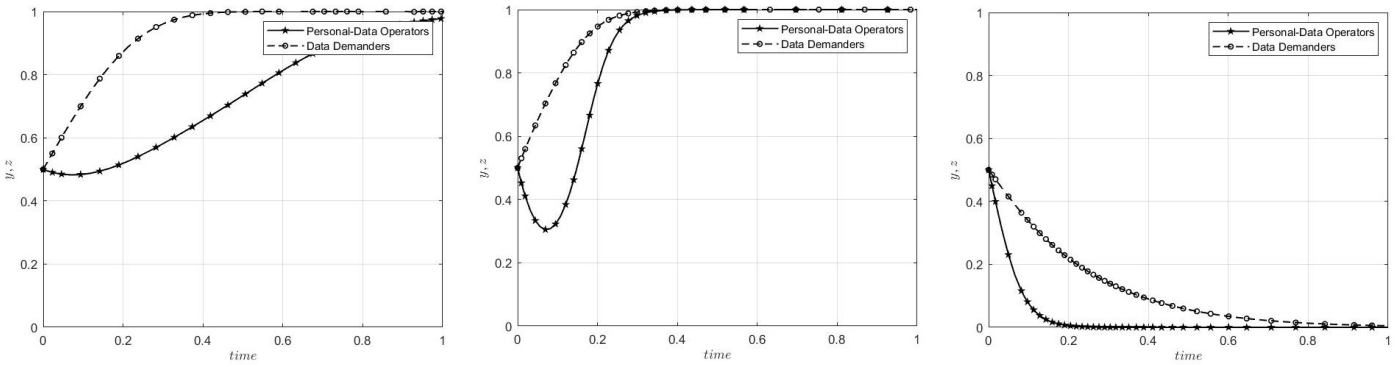
(**a**) (cb3,cc3) = (7,2) (**b**) (cb3,cc3) = (14,4) (**c**) (cb3,cc3) = (28,8)

Figure 3. The evolutionary trajectory of personal-data operators and data demanders when breach compensation parameters cb3 and cc3 change.

5.1.3. Impact of Net Data-Product Revenue on Personal-Data Operators and Data Demanders

While keeping all other parameters at their benchmark values, only the net revenue from the data product is varied to examine its influence on the evolutionary trajectories of personal-data operators and data demanders. The evolution under the benchmark revenue is shown in Figure 4b. Based on the baseline earnings (*rb*1, *rc*1) and costs (*cb*1, *cb*2, *cc*1, *cc*2) for both parties, the net revenue is simultaneously reduced by 50% and increased by 50%; the resulting trajectories are displayed in Figures 4a and 4c, respectively. Figure 4a shows

that a lower net revenue lengthens the time required for y and z to converge to 1, yet it slightly strengthens operators' willingness to utilize the data. Conversely, Figure 4c reveals that a higher net revenue reverses the convergence trend, causing y and z to move toward 0 instead. These findings indicate that excessively high net revenue can actually diminish the willingness of both personal-data operators and data demanders to participate in data transactions.

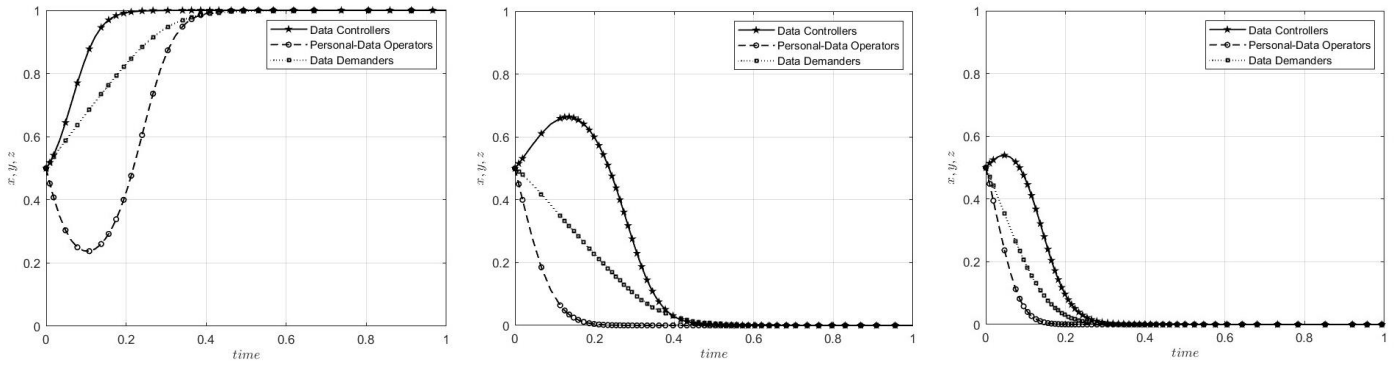


(**a**) (**b**) (**c**)

Figure 4. (**a**) Evolutionary trajectories of personal-data operators and data demanders when the net payoff is reduced by 50%; (**b**) evolutionary trajectories of personal-data operators and data demanders under the initial net payoff; (**c**) evolutionary trajectory of personal-data operators and data demanders when net returns increase by 50%.

5.1.4. Impact of Losses from Personal-Data Privacy Breaches on the Three Parties

With all other parameters held constant, only the magnitude of losses resulting from personal-data breaches is varied to examine its influence on the evolutionary trajectories of the three stakeholders' strategic choices. Given that the parties have already entered into a contract, they share both the gains and the losses arising from data-resource development; accordingly, the losses caused by any privacy breach are assumed to be identical across all parties, i.e., $S = s_1 = s_2 = s_3$. Building on the baseline value of S, the loss is progressively increased to 5, 10, and 15. The corresponding evolutionary outcomes are shown in Figure 5. The results indicate that as the loss from privacy breaches rises, the probability and speed with which data controllers switch from "circulation" to "non-circulation" increase markedly. Personal-data operators and data demanders likewise shift from participation to non-participation at an accelerating pace. This demonstrates that heightened risks of personal-data privacy breaches significantly diminish all three parties' willingness to engage in data transactions.



(**a**) (**b**) (**c**)

Figure 5. (**a**) The evolutionary trajectories of the tripartite strategies when the privacy-breach loss S is 5; (**b**) the evolutionary trajectories of the tripartite strategies when the privacy-breach loss S is 10; (**c**) the evolutionary trajectories of the tripartite strategies when the privacy-breach loss S is 15.

5.1.5. Impact of Breach Penalties and Data-Leakage Losses on the Personal-Data Operator

Figure 6 illustrates how the breach penalties (*cb*3, *cc*3) and data-leakage losses jointly influence the evolution of the personal-data operator's "utilize" strategy. When the penalties (*cb*3, *cc*3) are held constant, an increase in data-leakage losses reduces the operator's fitness for choosing "utilize," leading to a lower probability of participation. Conversely, when the data-leakage loss is fixed, raising the penalties (*cb*3, *cc*3) enhances the fitness for "utilize," thereby increasing the participation probability. Under high penalty levels (*cb*3, *cc*3), the operator still opts for "utilize" even when data-leakage losses are substantial. However, once the leakage losses become too large, the operator switches to "non-utilize" regardless of the penalty level. This indicates that the deterrent effect of fines is effective only under low-to-moderate risk; it becomes ineffective when risk is high.

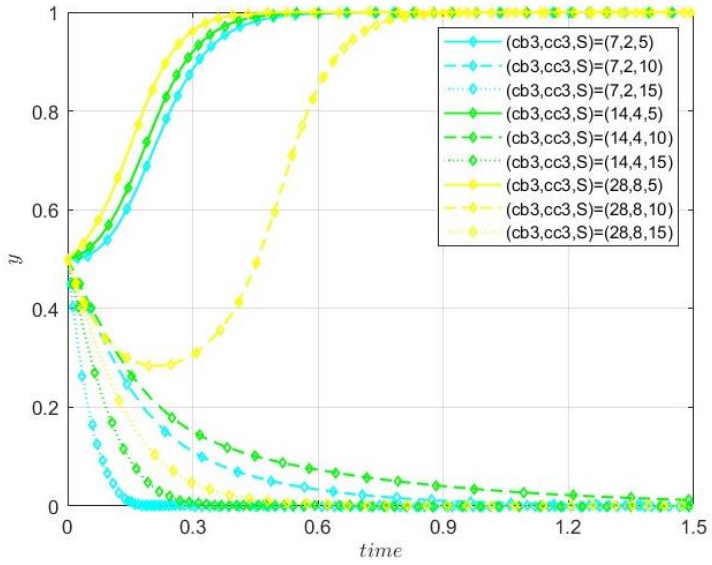


Figure 6. Evolutionary trajectory of personal-data operators when breach damages and data-breach losses change.

6. Conclusions and Policy Implications

6.1. Main Conclusions

Based on evolutionary-game theory, this study constructs a tripartite dynamic evolutionary-game model that comprises data controllers, personal-data operators, and data demanders. By analyzing the behavioral strategies and their dynamic evolution within the personal-data valorization chain, we obtain the following results:

1. Initial willingness exerts a pronounced influence on strategy evolution. The initial willingness of data controllers, personal-data operators, and data demanders positively drives the evolution of data-trading behaviors. When the initial willingness of all three parties is high, the data controller's choice to "circulate" data is only weakly affected by the willingness of operators or demanders, whereas the operator's willingness to participate is strongly driven by the demanders' intentions. Conversely, when initial willingness is low, all parties tend to withdraw from trading, creating a vicious cycle of "unwillingness to circulate."
2. Breach-penalty mechanisms regulate the equilibrium state. Penalties for breach constrain the behaviors of all parties and incentivize the ideal equilibrium of "circulate–utilize–purchase." Stronger penalties impose tighter constraints on potential violators and better protect compliant parties, thereby enhancing the stability and sustainability of data trading. Excessively high penalties, however, may induce risk-averse parties

to exit the market; hence, a balance must be struck between punitive severity and trading incentives.

3. Net benefits exert a dual effect on participation willingness. An increase in the net benefit of data products markedly raises the willingness of operators and demanders to participate, boosting their confidence in data-value development. Yet overly high net benefits may trigger opportunistic behavior on the demand side, causing demanders to bypass operators and obtain data directly. Such circumvention undermines the operators' willingness to participate and negatively affects the stability of the entire value chain.
4. Privacy-leakage risk inhibits trading behaviors. The sensitivity of personal data and the high risk of privacy leakage significantly dampen the willingness of all parties to trade. When supporting infrastructure is weak and the trading environment insecure, the potential loss from a privacy incident is magnified, intensifying participants' concerns. Breach-of-contract damages can still discipline stakeholders under low-to-moderate risk and encourage them to join the personal-data value chain; however, once external risk becomes sufficiently high, the contract ceases to have any deterrent effect.

6.2. Policy Recommendations

Based on the above research findings, this paper proposes the following recommendations:

Build a contract-enforcement mechanism to strengthen trust and cooperation. a. Refine contract clauses. Specify the rights, obligations, and consequences of breach for every party, and draft legally binding terms that prevent any side from withdrawing from the transaction at will. b. Establish a supervisory body. Create an independent, authoritative agency to monitor and evaluate the behavior of all parties, guaranteeing strict enforcement of contractual provisions. c. Introduce technological tools. Employ blockchain and smart contracts to make the trading process transparent and automated, reduce human-intervention risk, and improve trading efficiency.

Improve the legal framework and clarify data ownership. a. Specify data-property rights. Through legislation, unequivocally define the ownership of personal data, providing a clear legal basis for data transactions and bolstering the confidence of all participants. b. Strengthen privacy protection. Rigorously enforce laws such as the Data Security Law and the Personal-Information Protection Law, and impose severe penalties for non-compliance to lower privacy-leakage risks. c. Promote institutional innovation. Draw on the "three-rights separation" approach proposed in the "Twenty Data Provisions" to explore new mechanisms for allocating data-property rights, thereby offering institutional safeguards for data trading.

Optimize supply–demand interaction and enhance market cognition. a. Unlock data value. Through healthy interaction between suppliers and demanders, explore new application scenarios for personal data, raise data-standardization levels, and increase market value. b. Upgrade operator capabilities. Support personal-data operators in adopting advanced technologies, improving data-processing capacity and service quality, lowering management costs, and establishing a more competitive pricing system. c. Strengthen pre-trade communication. Suppliers and demanders should communicate fully before transactions, evaluate prices rationally, and avoid deal failures caused by divergent price expectations.

6.3. Research Limitations and Future Directions

Although this study has achieved certain results in analyzing the dynamic evolution of incentive mechanisms within the personal-data value chain, it still has the following limitations. First, the quantification of each party's costs and benefits is overly simplified, and only the interaction between the breach-of-contract damage parameter and the privacy-

leakage loss parameter is examined. Second, the study is primarily based on theoretical models and lacks in-depth analysis of real scenarios and representative cases. Future research can be deepened in the following ways: (1) combine empirical methods—such as interviews and questionnaires—to collect first-hand data for empirically testing model parameters; and (2) more appropriate payoff functions can be adopted to further explore how the breach-of-contract damage parameter interacts with other parameters, thereby furnishing more precise guidance for policy-making. By integrating theory and practice, the scientific rigor and operability of the research can be further enhanced, offering stronger theoretical support for the healthy development of the personal-data value chain.

Author Contributions: Conceptualization, J.M.; project administration, J.M.; writing—original draft, J.M. and J.Y.; writing—review and editing, J.M., J.Y. and Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Social Science Foundation of China, grant number 23BTQ068. This research was also funded by the Soft Science Project of Henan Province, grant number: 252400411280.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Parameter Symbols and Their Meanings.

Parameter	Meaning
x	Probability that the data controller elects to circulate personal data, $0 \leq x \leq 1$
$ra1$	Personal-data circulation payoff to the data controller when the data controller chooses to circulate and the personal-data operator chooses to exploit, $ra1 > 0$
$ra2$	Personal-data product payoff to the data controller when the data controller chooses to circulate, the personal-data operator chooses to exploit, and the data requester chooses to purchase, $ra2 > 0$
$ca1$	Aggregate cost incurred by the data controller when it chooses to circulate personal data, $ca1 > 0$
$ca3$	Breach-of-contract damages payable by the data controller for an unjustified withdrawal, $ca3 > 0$
$s1$	Loss suffered by the data controller owing to privacy leakage arising from the circulation and use of personal data, $s1 > 0$
y	Probability that the personal-data operator's trading platform elects to exploit the data resource, $0 \leq y \leq 1$
$rb1$	Personal-data product payoff to the personal-data operator when the data controller chooses to circulate, the personal-data operator chooses to exploit, and the data requester chooses to purchase, $rb1 > 0$
$cb1$	Aggregate cost borne by the personal-data operator when the data controller chooses to circulate personal data and the personal-data operator chooses to exploit, $cb1 > 0$
$cb2$	Aggregate cost borne by the personal-data operator when the data controller chooses not to circulate personal data and the personal-data operator chooses to exploit, $cb2 > cb1 > 0$

Table A1. *Cont.*

Parameter	Meaning
$cb3$	Breach-of-contract damages payable by the personal-data operator for an unjustified withdrawal, $ca3 > 0$
$s2$	Loss suffered by the personal-data operator owing to privacy leakage arising from the circulation and use of personal data, $s1 > 0$
z	Probability that the data requester elects to purchase the data resource or product, $0 \leq z \leq 1$
$rc1$	Payoff to the data requester from processing and analyzing personal data when the data controller chooses to circulate, $rc1 > 0$
$cc1$	Aggregate cost incurred by the data requester to collect, process, and use personal data when the data controller chooses to circulate and the personal-data operator chooses to exploit, $cc2 > cc1 > 0$
$cc2$	Aggregate cost incurred by the data requester to collect, process, and use personal data when the data controller chooses to circulate and the personal-data operator chooses not to exploit, $cc2 > 0$
$cc3$	Breach-of-contract damages payable by the data requester for an unjustified withdrawal, $cc3 > 0$
$s3$	Loss suffered by the data requester owing to privacy leakage arising from the circulation and use of personal data, $s3 > 0$

References

1. China Center for Information Industry Development. China Data Factor Market Development Report (2020–2021). Available online: http://www.100ec.cn/detail{-}{-}6591616.html (accessed on 15 March 2025).
2. Opinions of the General Office of the Communist Party of China Central Committee and the General Office of the State Council on Accelerating the Development and Utilization of Public Data Resources. Available online: https://www.gov.cn/zhengce/202410/content_6978911.htm (accessed on 25 February 2025).
3. Ji, W.; Weng, Z. The Justification and Interpretation of Property Rights in Personal Data. *Law Soc. Dev.* **2024**, *30*, 168–189.
4. Rao, C. The Legal Dilemma and Institutional Reshaping of Trust Mechanisms in Data Transactions. *Acad. J. Zhongzhou* **2025**, *2*, 73–80.
5. Wan, F. Right Confirmation and Authorization Mechanism for Public Data: An Investigation Based on "Data Mitosis". *J. Dalian Univ. Technol. Soc. Sci.* **2024**, *45*, 70–80.
6. Zhang, S. On the Realization of the Structural Division of Data Property Rights in Law. *Orient. Law* **2023**, *2*, 73–85.
7. Gu, W.; Fan, Z.; Fan, X. Research on the Personal Data Collection, Compliant Use and Management Enlightenment: Based on Text Analysis of Privacy Policies of Digital Resource Vendors. *Inf. Stud. Theory Appl.* **2025**, *48*, 56–64.
8. Song, H. Types and Protection of Personal Data Property Rights. *South China Financ.* **2024**, *12*, 85–97.
9. Wang, X. The Legal Application Dilemma and Outlet of the "Three New" Elements of the New Quality Productive Forces Enabled by Data Elements. *Sci. Technol. Prog. Policy* **2025**, *42*, 21–32.
10. Cui, C. The Normative Expression of Residual Control over Data—Reflections on and Reconstruction of Personal Information Rights and Interests. *Soc. Sci. J.* **2024**, *3*, 120–129.
11. Xiang, L.; Gao, Q. Analysis of the Characteristics, Basic Attributes and Contents of Personal Data Right in the Era of Big Data. *Inf. Stud. Theory Appl.* **2018**, *41*, 45–50+36.
12. Xu, K. Three Approaches to Data Protection: Comment on the Case of Weibo Accusing Maimai of Unfair Competition. *J. Shanghai Univ. Soc. Sci.* **2017**, *34*, 15–27.
13. Fei, A.; Chen, C. The Right of Withdraw of Consent in Personal Data Transactions—Conflict with the Contractual Bindingness as an Entry Point. *J. Guangxi Univ. Philos. Soc. Sci.* **2024**, *46*, 171–182.
14. Xia, Q. A Study on the Construction of Private Law Institutions for Personal Data Transactions. *China Leg. Sci.* **2024**, *5*, 144–164.
15. Cheng, X. On Legal Framework of the Personal Data Authorization Mechanism. *Trib. Political Sci. Law* **2023**, *41*, 77–89.
16. Fu, X. On the Data Trust Model in the Distribution of Personal Data Interests. *Orient. Law* **2025**, *1*, 60–74.
17. Wei, Y.; Chen, X.; Zou, X. Evolutionary Game Analysis of Personal Information Protection based on Data Sharing. *Inq. Into Econ. Issue* **2019**, *12*, 79–88.
18. Wang, Z.; Deng, Y.; Liang, L. User Authorization Mechanism Design for Personal Data Circulation: An Evolutionary Game Among Individuals, Enterprises, and Government. *J. Zhengzhou Univ. Philos. Soc. Sci.* **2023**, *56*, 61–69.

19. Wan, Z.; Vorobeychik, Y.; Xia, W.; Liu, Y.; Wooders, M.; Guo, J.; Yin, Z.; Clayton, E.W.; Kantarcioglu, M.; Malin, B.A. Using Game Theory to Thwart Multistage Privacy Intrusions When Sharing Data. *Sci. Adv.* **2021**, *7*, eabe9986. [CrossRef]
20. Zhang, L.; Zhang, Z. Study on Data Entry Transaction and Trusted Circulation System Construction Based on Multi-agent Evolutionary Game Equilibrium Model. *Comput. Sci.* **2025**, *52*, 127–136.
21. Liu, X. Personal Data Pricing for Large Language Models Based on Privacy compensation. *Data Anal. Knowl. Discov.* **2025**, *9*, 106–116.
22. Shang, X.; Han, H.; Zhu, Z. Mechanism Design of Right to Earnings of Data Utilization Based on Evolutionary Game Model. *Comput. Sci.* **2021**, *48*, 144–150.
23. Huang, W. Research on the Pricing of Personal Big Data Using Labor Game and Privacy Utility. Master's Thesis, Zhongnan University of Economics and Law, Wuhan, China, 16 March 2025.
24. Guo, X.; Wang, H.; Kong, N. Two-sided pricing strategy for personal health data trading under information asymmetry. *J. Ind. Eng. Eng. Manag.* **2022**, *36*, 129–139.
25. Su, Q.; Ji, L. The Coordination Mechanism of Medical Data Sharing Based on Stochastic Evolutionary Game. *Inf. Sci.* **2023**, *41*, 37–47.
26. Huang, Z.; Xiong, H. Evolution of Users' Knowledge Sharing and Hiding Behaviors in Online Health Community. *Data Anal. Knowl. Discov.* **2023**, *7*, 125–139.
27. Alexander, J.M. Evolutionary Game Theory. In *The Stanford Encyclopedia of Philosophy*; Zalta, E.N., Ed.; Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2021.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.