The Influence of Government, Enterprises, and the Public on the Security of Cross-border Data Flows and Optimization Strategies: An Information Ontological Perspective

Yao Zhang[12*], Yu Chen[2]
[1]People's Public Security University of China, Beijing, 100038, Beijing, China
qian2020090304@163.com
[2]Yunnan Police College, Kunming, 650223, Yunnan, China
luckyrabbit450@sohu.com

Abstract: In the technology-driven era, the rapid advancement of information technologies, particularly artificial intelligence, has led to an increase in both the scale and complexity of data cross-border flows, thereby elevating data security to a global concern. This paper addresses the issue of data security in cross-border flows by reviewing pertinent literature, delineating the distinct phases of data cross-border flow development along with the challenges encountered at each stage, and introducing the public-private partnership (PPP) theoretical framework. A three-dimensional interactive theoretical framework centered on "government guidance, corporate impetus, and public engagement" is constructed to analyze the interaction mechanisms and influencing factors among government, enterprises, and the public. Based on this analysis, the paper proposes a series of targeted strategies to enhance the coordinated governance system for data cross-border flow security: refining the legal framework and regulatory approaches in policy and supervision; fostering innovation and standardization in technology and innovation; and boosting government credibility, enhancing public participation, and reinforcing interaction mechanisms in the realm of public trust and engagement. These measures aim to facilitate the transition of data cross-border flow security coordinated governance from theoretical discourse to practical application, effectively addressing various risks and challenges while promoting the healthy and orderly growth of the global digital economy.

Keywords: Data Cross-border Flow Security; Government Guidance; Corporate Impetus; Public Engagement; Collaborative Governance

1.Introduction

In recent years, the generation of artificial intelligence represented by "ChatGPT" has developed rapidly, not only presenting significant development opportunities for human society but also introducing numerous risks and challenges. Particularly, it has heightened the urgency and complexity of governing data cross-border flow security. Specifically, these

challenges can be categorized as follows:

First, legal and regulatory differences pose compliance risks. Globally, there is currently no unified framework for data cross-border flow. Different countries and regions have developed distinct models based on their unique developmental characteristics. For instance:

- The "American model" advocates for free data cross-border flow. Led by the United States, the Trans-Pacific Partnership Agreement (TPP) promotes unrestricted data movement to maintain its leadership in the digital economy [1].

- The "EU model" prioritizes personal privacy protection. Unlike the U.S., the European Union's General Data Protection Regulation (GDPR) [2]enforces stringent data cross-border flow regulations and implements robust measures to safeguard individual data privacy [3].

- The "emerging economy model" emphasizes data localization. Countries like Russia[4], India[5], and Vietnam[6] impose general restrictions on data cross-border flow, requiring data to be stored locally and adhering to strict transmission regulations.These diverse approaches complicate international cooperation and coordination in data governance. Enterprises must establish multiple compliance systems to meet varying national and regional requirements, thereby increasing operational and time costs[7].

Second, data security risks are significant[8]. Cross-border data transmission often traverses multiple network nodes and jurisdictions, increasing the likelihood of cyberattacks, theft, or leaks. The 2024 UnitedHealth Group data breach, where millions of patients' sensitive data were compromised, underscores the vulnerabilities within the healthcare sector and highlights the critical need for enhanced data protection and cybersecurity protocols[9]. Additionally, the complex and varied network environments make data cross-border flows more susceptible to attacks from malicious actors using techniques such as malware, phishing, and DDoS attacks. These threats can lead to data breaches and disrupt business operations[10].

Third, data sovereignty and interest conflicts present another challenge[11]. Data is considered a strategic resource by many nations, leading to increased scrutiny over data sovereignty. Some countries may impose strict controls on data cross-border flow to protect national security and data sovereignty.

Fourth, technical challenges arise from differing standards and infrastructure across countries and regions. Variations in encryption technologies and transmission protocols can create technical barriers that hinder smooth data cross-border flow[12].

In summary, the challenges faced by data cross-border flow encompass legal, security, sovereignty, and technical dimensions. Therefore, optimizing and enhancing the collaborative governance system for data cross-border flow

is crucial. It serves as a key technical support for developing digital trade and forms an essential foundation for establishing global digital trade rules. Moreover, it is vital for maintaining national security and data sovereignty. Balancing the benefits of AI technology with ensuring secure data cross-border flow has become a critical issue for governments, enterprises, and individuals alike[13]. To effectively address these challenges, further analysis of the impact of "governments, enterprises, and the public" on data cross-border flow security in the AI era is necessary. This requires strengthened cooperation and coordination among governments, enterprises, and international organizations at all levels to promote the formulation and improvement of data cross-border flow regulations.

2. Literature Review and Theoretical Framework

2.1. Literature Review

Currently, policymakers and academics widely recognize that data security has emerged as a critical issue in the era of generative AI, propelled by the digitalization trend. Beyond technical aspects such as encryption and access control, it profoundly impacts the protection of individual privacy rights, national security, and global economic stability[14]. Reviewing existing literature on cross-border data flow safety can facilitate the development of more comprehensive and scientifically grounded data security strategies and legal frameworks.

2.1.1 Initial Exploration Period (1970s-80s)

Following the OECD's introduction of the concept of cross-border data flow, this period was characterized by initial theoretical exploration[15]. The establishment of the Computer User Group (CUG) drew attention to the potential implications of cross-border information transmission. However, actual cross-border data flows were limited, primarily confined to internal business management data exchanges within multinational corporations, such as financial statements and inventory data between branches, to support operational decision-making. Technologically, data transmission capabilities were rudimentary, with low network bandwidth, slow speeds, and limited storage and processing power, which constrained the scope and efficiency of cross-border data flows. Globally, there was little regulation or management of cross-border data flows, as countries focused on developing their domestic IT industries without establishing systematic regulatory frameworks.

2.1.2 Slow Development Period (1990s-2010s)

The commercialization of the Internet and advancements in information technology spurred gradual growth in cross-border data flows. E-commerce became a significant driver, generating substantial cross-border data transmission needs involving personal and transactional data from consumer activities on online platforms[16]. Despite this growth, challenges persisted. On one hand, cybersecurity technologies were immature, leading to frequent data breaches and malicious attacks, causing concerns among businesses and

consumers. On the other hand, the lack of harmonized international standards for data protection and privacy created complex compliance issues for multinational enterprises operating across jurisdictions[17].

2.1.3 Accelerated Expansion Period (2010s-Present)

The rapid development of cloud computing, big data, and mobile internet has significantly accelerated cross-border data flows. These technologies enable seamless global data storage and processing, while big data analytics rely on vast cross-border datasets. Mobile internet proliferation allows individuals to generate and transmit data anytime, anywhere, expanding data flows into sectors like finance, healthcare, education, and entertainment. This expansion has heightened concerns over data security and privacy. Major data breaches, such as those at Yahoo and Facebook, have intensified public scrutiny, prompting governments worldwide to enhance regulatory oversight. The EU's General Data Protection Regulation (GDPR)[18], known for stringent data protection standards and hefty fines, has imposed strict requirements on entities handling EU citizens' data, including data subject rights, legal bases for processing, and restrictions on cross-border transfers. GDPR's implementation has reshaped the global data flow landscape, compelling multinational enterprises to invest heavily in compliance efforts.

2.2. Theoretical Framework

Public-Private Partnership (PPP)[19] is a crucial concept in economics and finance, highlighting an innovative financial cooperation model between the public and private sectors. This theory originated from the UK's public-private partnership financing mechanism, first introduced by the British government in 1982 [20]. It specifically refers to "a partnership between the government and private organizations for constructing urban infrastructure projects or providing certain public goods and services based on a concession agreement. Both parties form a cooperative relationship and define their rights and obligations through a contract." As an optimized project financing model developed in the field of public infrastructure construction, the core of this theory lies in deep cooperation between the government and social capital, jointly bearing risks and sharing benefits, thereby achieving more flexible and efficient construction, operation, and management of public projects . The broad concept of "PPP" encompasses various forms of cooperation between the public and private sectors aimed at providing public goods or services [21], applicable in diverse scenarios. In other words, as a cross-boundary cooperation framework, the broad concept of "PPP" transcends simple combinations of funds and technology, establishing a three-dimensional interactive theoretical framework centered on government leadership (public sector), enterprise drive (private sector), and public participation (private sector). This aims to reshape the data security governance system through deep integration and cooperation among the three parties based on common goals, constructing an interactive framework with government leadership,

enterprise drive, and public participation as its core. Within this framework:

2.2.1 Government Leadership (G)

The government is not merely a policymaker and supervisor but also a cultivator and coordinator of collaborative ecosystems. By formulating forward-looking strategic plans, the government clarifies the goals and direction of public services while creating an open, transparent, and fair cooperation environment to attract active enterprise participation. Additionally, the government serves as a bridge, promoting information exchange and resource sharing between the public and private sectors to ensure the smooth progress and continuous optimization of cooperative projects. Moreover, the government places significant emphasis on public opinions and needs, establishing:

$$G=f(LG,RG,IG)=\alpha\cdot LG+\beta\cdot RG+\gamma\cdot IG$$

2.2.2 Enterprise Motivation (E)

The private sector, leveraging its keen market insight, extensive management experience, and robust technological innovation capabilities, continuously infuses vitality and creativity into collaborative projects. The private sector not only oversees the specific implementation and operational management of projects but also actively engages in the planning and design phases, proposing innovative solutions to enhance the efficiency and quality of public services. Additionally, enterprises optimize resource allocation through market mechanisms, thereby reducing operating costs and achieving a win-win scenario for economic and social benefits. Consequently, enterprise motivation (E) represents the private sector's contributions in "technological innovation, market expansion, and business model innovation" within the context of cross-border data flow. This involves variables such as "technological innovation (TE), compliance costs (CE), and market expansion efforts (ME)". The functional relationship is defined as:

$$E=g(TE,CE,ME)=\delta\cdot TE-\epsilon\cdot CE+\zeta\cdot ME$$

2.2.3 Public Participation (P)

The public, as the beneficiaries of the "PPP" model, play a crucial role in the success of cooperative projects. By participating in various stages of the project, such as consultation, supervision, and evaluation, the public can not only stay informed about the project's progress and achievements but also express their needs and expectations, providing valuable suggestions and feedback for the optimization of the project. Additionally, the public's active involvement enhances the transparency and credibility of the project and fosters communication and collaboration between the government and private (business) sectors, contributing to a well-structured governance system.

Therefore, public participation (P) represents the public's awareness, trust, and engagement in cross-border data flow, encompassing variables such as "awareness level (AP), trust level (TP), and participation level (EP)". That is:

$$P=h(AP,TP,EP)=\mu\cdot AP+\nu\cdot TP+\xi\cdot EP$$

Among them, μ, ν, and ξ are weighting coefficients, indicating the importance or influence of different variables on public participation.

In summary, by integrating the above three functions, where CTF represents the effectiveness or level of collaborative governance, λG, λE, and λP represent the relative importance weights of "government pull, enterprise drive, and public participation" in collaborative governance, and "..." denotes other unspecified factors and their corresponding weights and contributions, a function model of collaborative governance is formed, namely:

$$CTF=\lambda G\cdot G+\lambda E\cdot E+\lambda P\cdot P$$

$$CTF=\lambda G(\alpha\cdot LG+\beta\cdot RG+\gamma\cdot IG)+\lambda E(\delta\cdot TE-\epsilon\cdot CE+\zeta\cdot ME)+\lambda P(\mu\cdot AP+\nu\cdot TP+\xi\cdot EP)+\ldots$$

3. Analysis and Discussion

3.1 Interactive Analysis

3.1.1 Government-Enterprise Interaction Model

The government's regulatory intensity (RG) affects the enterprise's compliance cost (CE), which in turn affects the enterprise's technological investment (TE) and market expansion efforts (ME). At the same time, the enterprise's technological innovation (TE) and compliance operation (CE) will feed back to the government, affecting the government's policy formulation and regulatory strategy.

（1）Regulatory intensity affects compliance cost:

$$CE(t+1)=CE(t)+\alpha\cdot RG(t)+\xi_1(t)$$

In this model, $\alpha > 0$ is the direct impact coefficient of regulatory intensity on compliance cost, and $\xi_1(t)$ is a random disturbance term, representing the impact of other unmodeled factors on compliance cost.

（2）Compliance cost affects technological investment and market expansion:

$$TE(t+1)=TE(t)-\beta\cdot\frac{CE(t)}{1+k\cdot CE(t)}$$

$$ME(t+1)=ME(t)-\gamma\cdot(1-\exp(-\lambda\cdot CE(t)))$$

In this model, $\beta,\gamma > 0$ are coefficients, $\kappa > 0$ controls the marginal diminishing effect of compliance cost on technological investment, $\lambda > 0$ controls the rate at which market expansion efforts decrease as compliance cost increases.

（3）Enterprise technological innovation and compliance operation feedback to the government:

$$RG(t+1)=max(0,\mu\cdot(I(t)-\theta\cdot C(t))+\xi_2(t))$$

I(t) is the enterprise's technological innovation index (such as patent numbers, R&D investment ratio, etc.), C(t) is the enterprise's compliance score, $\mu,\theta > 0$ are weighting coefficients, $\xi_2(t)$ is a random disturbance term. The regulatory intensity cannot be negative, so the use of the max function ensures that $RG(t + 1) \geq 0$.

3.1.2 Government-Public Interaction Model

The government's transparency, policy implementation effectiveness, etc. directly affect the public's trust (TP) and participation (EP), and the public's trust will affect the government's credibility and policy implementation efficiency.

The government's transparency and policy implementation effectiveness affect the public's trust and participation:

$$TP(t+1)=TP(t)+\delta\cdot GO(t)-\epsilon\cdot PF(t)+\zeta_1(t)$$

$$EP(t+1)=EP(t)+\eta\cdot TP(t)-\phi\cdot\left(1-\frac{TP(t)}{TP\ max}\right)_2+\zeta_2(t)$$

Specifically, GO(t) represents government transparency, PF(t) represents the number of policy failures, δ and ϵ are coefficients, $\zeta1(t)$ and $\zeta2(t)$ are random disturbance terms. Participation rate EP is positively correlated with trust level TP, but is affected by the upper limit of trust level TPmax, which takes the form of an upward-convex curve.

3.1.3 Interaction Model Between Enterprises and the Public

The behaviors of enterprises (such as data protection measures, service quality, etc.) directly affect the public's trust level (TP) and participation level (EP), while the public's feedback (such as consumption choices, public pressure) will encourage enterprises to improve their behaviors. The behaviors of enterprises affect the public's trust level and participation level:

$$TP(t+1)=TP(t)+\eta'\cdot BP(t)-\theta'\cdot NI(t)+\zeta_3(t)$$

Specifically, BP(t) represents the positive behavior index of the enterprise, such as data protection measures and service quality, NI(t) represents the number of negative events, $\eta',\theta'>0$ are coefficients, and $\zeta3(t)$ is

a random disturbance term.

3.2 Factors Analysis

In the data cross-border flow security governance system, the government, enterprises, and the public play distinct roles that interact, influence, and promote each other. However, in practical operation, as the scale of data elements continues to expand and artificial intelligence technology advances, the proportion of data production elements participating in traditional production increases, introducing more variables and associated risks.

3.2.1 Government Level: Policy and Regulatory Risks

From the perspective of government traction (G), an incomplete legal framework can blur the boundaries of data cross-border flow legality. This is particularly evident in areas such as classification management and protection of data subject rights, where regulatory gaps or ambiguities can expose enterprises to compliance risks during cross-border data operations. Additionally, it leaves the government without a clear legal basis for supervision. Therefore, the completeness of regulatory policies (LG) is a critical variable. The imperfection of these policies impacts enterprise compliance and government oversight. Let the degree of compliance risk be Rrisk; the relationship between enterprise compliance risk and regulatory policy completeness (LG) is inversely proportional:

$$R_{risk} = \frac{\kappa_1}{LG + \epsilon_1}$$

where K_1 is a positive proportional constant, and ε1 is a very small positive number (>0), indicating that lower regulatory completeness leads to higher compliance risk for enterprises. Simultaneously, the clarity of the government's regulatory basis (G_{basis}) is positively correlated with regulatory completeness (LG):

$$G_{basis}=K_2 \cdot LG$$

where K_2 is a positive coefficient, indicating that more complete regulations lead to clearer regulatory bases.

From the perspectives of regulatory intensity (RG) and efficiency, on the one hand, overly stringent regulation can lead to excessively high compliance costs (CE) for enterprises. For instance, in the interaction between the government and enterprises, increased regulatory intensity (RG) directly raises compliance costs, which may inhibit technology investment (TE) and market expansion efforts (ME), thereby affecting the efficiency and innovation in data cross-border flow. On the other hand, insufficient regulation may fail to effectively prevent data leaks, illegal data transactions, and other risks, thereby threatening the security of data cross-border flow.

(1) The impact of regulatory intensity (RG) on enterprise compliance costs (CE), technology investment (TE), and market expansion efforts (ME)

For the impact of regulatory intensity (RG) on enterprise technology

investment (TE), a functional relationship exists:

$$TE = (t+1) = TE\ (t) - \beta \cdot \frac{RG(t)}{1+\phi_2}$$

Among them, $\beta > 0$ is a coefficient representing a very small positive number. This implies that, under unchanged conditions, the greater the regulatory intensity (RG), the lower the relative technology investment (TE) of enterprises in the next stage, reflecting an inhibitory effect.

(2) The impact of regulatory intensity (RG) on data cross-border flow security (S)

Let the degree of data cross-border flow security be S. There exists a positive correlation between regulatory intensity (RG) and data cross-border flow security (S). Specifically, insufficient regulation leads to lower security, while appropriate or stronger regulation results in higher security. This relationship can be expressed as:

$$S = \begin{cases} k_3 \cdot RG, & RG \leq RG_{optimal} \\ k_4, & RG > RG_{optimal} \end{cases}$$

Specifically, K_3 and K_4 are positive coefficients, and RGoptimal represents the optimal regulatory intensity value that can ensure good security while considering efficiency and other factors. When the regulatory intensity (RG) is less than the optimal value, the security level (S) increases linearly with the strengthening of the regulatory intensity (RG); after the regulatory intensity exceeds the optimal value, due to situations such as suppressing business development that affect the overall efficiency and other factors, the security level remains at a relatively fixed and good level.

3.2.2 Enterprise Level: Technological and Innovation Risks

The technical innovation (TE) variable in the enterprise driver (E) faces significant challenges in the context of cross-border data flow. In this context, enterprises must continuously invest in technological innovation to meet the requirements of data security and privacy protection. On the one hand, the increase in compliance costs (CE) can reduce the resources available for technological innovation, thereby affecting technology investment. This may cause enterprises to lag behind in the rapid development of cross-border data technologies, as evidenced by delays in updating data encryption and cross-border transmission security protocols. On the other hand, differences in data infrastructure and technical standards across countries and regions require enterprises to address technical compatibility issues when promoting cross-border data flow. As a result, the technological innovations of enterprises may not be effectively applied in certain data environments, impacting the smooth implementation of cross-border data flow.

(1) The impact of compliance costs (CE) on technology innovation (TE)

resource allocation

Let the total resources available for technological innovation be denoted as R_{TE}. There is a negative correlation between Rtotal and compliance costs (CE), which can be expressed as:

$$R_{TE} = R_{TE}^{0} - \omega \cdot CE$$

In this model, R_{TE}^{0} represents the initial resource available to the enterprise for technological innovation before the impact of compliance costs, which is assumed to be positive. The coefficient $\omega > 0$ represents the impact factor, indicating that for every unit increase in compliance costs, the amount of resources available for technological innovation is reduced by that amount. The actual level of technological innovation (TE) is influenced not only by resource inputs, but also by other factors. It is assumed that there is a function f(·) that converts resource inputs into actual levels of technological innovation, so that technological innovation (TE) can be expressed as:

$$TE = f(R_{TE}) = f(R_{TE}^{0} - \omega \cdot CE)$$

Here, the function f(·) can be a monotonically increasing function that satisfies reasonable properties such as an increase in technological innovation levels with increasing resource inputs.

$$TE = k_5 \cdot (R_{TE}^{0} - \omega \cdot CE)$$

Specifically, $k_5 > 0$ is the coefficient that converts resources into technological innovation levels, reflecting the relationship that the increase of compliance costs (CE) will lead to a lower level of technological innovation (TE), i.e., it may cause enterprises to fall behind in the pace of technological development.

(2) Technical compatibility affects the smoothness of data cross-border flow

Let the smoothness of data cross-border flow be represented by S_{flow}, which is affected by the adaptability of enterprise technological innovation achievements in different national and regional data environments. Assuming there are n different countries or regions, for the i-th country or region, the adaptability coefficient of enterprise technological innovation achievements is α_i (taking a value range within [0,1], 0 representing complete incompatibility, and 1 representing complete compatibility). Let A_i represent the weight of the importance of that country or region in the data cross-border flow project

(satisfying $\sum_{i=1}^{n} A_i = 1$), then the smoothness of data cross-border flow (S_{flow}) can be expressed as:

$$S_{flow} = \sum_{i=1}^{n} A_i \cdot \alpha_i$$

This further indicates that the data environment adaptation coefficients in different countries or regions, as well as their respective weights in the overall project, jointly determine the smoothness of data cross-border flow. If the adaptation coefficients are low in many important countries or regions, it will be difficult to smoothly carry out data cross-border flow as a whole.

3.2.3 Social Dimension: Public Trust and Participation in Risk Management

Research indicates that public participation (P) is influenced by various factors, including the level of trust (TP) in government. Insufficient government transparency (GO), poor policy implementation outcomes, and negative events involving businesses (NI) all contribute to lowering public trust. An increase in the number of government policy failures (PF) and corporate negative events (NI) further reduces public trust. Data cross-border flow involves sensitive issues such as data privacy, and insufficient public trust may lead to public resistance against data cross-border security measures. Moreover, public participation (EP) is not only related to trust (TP) but also affected by other factors. If the public participation mechanism is not well-established, lacks effective channels for project consultation, oversight, and evaluation, and the public cannot timely learn about project progress or express their needs, it will result in low participation. Low participation can prevent data cross-border flow projects from fully considering public needs, thereby affecting the sustainability and social acceptance of these projects.

(1) Impact of Trust Level (TP) on Various Factors

Let the public trust level (TP) vary over time (t), influenced by government transparency (GO), the number of policy failures (PF), and the number of corporate negative events (NI). The functional relationship can be expressed as:

$$TP(t+1) = TP(t) + \delta \cdot GO(t) - \in \cdot PF(t) - \theta \cdot NI(t) + \xi_1(t)$$

Where $\delta > 0$ represents the positive impact coefficient of government transparency on public trust level, meaning that an increase in government transparency by one unit leads to a corresponding increase in public trust; $\gamma > 0$ is the negative impact coefficient of the number of policy failures on public trust level, indicating that each additional policy failure decreases public trust by a certain amount; $\theta > 0$ is the negative impact coefficient of the number of corporate negative events on public trust level; $\xi_1(t)$ is a random disturbance term representing the influence of other unconsidered factors on the change in public trust level from time t to t+1.

(2) Influence of Trust Level (TP) and Other Factors on Participation Level (EP)

Assuming that the public participation level (EP) varies with time (t), it is positively correlated with trust level (TP) and affected by the soundness of the public participation mechanism (M), measured on a scale from 0 to 1, where 0 indicates a completely unsound mechanism and 1 indicates a very sound mechanism. The functional relationship can be expressed as:

$$EP(t+1)=EP(t)+\eta \cdot TP(t) \cdot M(t)+\xi_2(t)$$

Where $\eta > 0$ is the coefficient of influence of trust degree (TP) on participation degree (EP), reflecting the extent to which participation increases when trust improves by one unit, given a fixed level of participation mechanism soundness; $\xi_2(t)$ is a random disturbance term indicating the influence of other unaccounted factors on the change in participation level from time t to t+1.

(3) Comprehensive Function Relationship of Public Participation Degree (P)

Given that public participation degree (P) is composed of awareness degree (AP), trust degree (TP), and participation degree (EP), the function relationship is as follows:

$$P=h(AP,TP,EP)=\mu \cdot AP+\nu \cdot TP+\xi \cdot EP$$

Substituting the relationships between TP(t+1) and EP(t+1) into this equation, we obtain a comprehensive function model of public participation (P) over time that accounts for the dynamic changes of various influencing factors. Through this integrated model, we can analyze how changes in these factors affect public participation and, consequently, the sustainability and social acceptance of data cross-border flow projects.

4 Results

Based on the above analysis, through the in-depth cooperation between "government, enterprises (including technology providers, service providers, etc.) and the public" (see Figure 1), the variables ($\alpha,\beta,\gamma,\delta,\epsilon,\zeta,\mu,\nu,\xi,\lambda G,\lambda E,\lambda P$) in "government traction force (G), enterprise driving force (E), and public participation (P)" are continuously optimized and corrected. In order to realize the cross border data flow security collaborative governance (CTF) from the "theoretical framework" to "practical operation" leap.

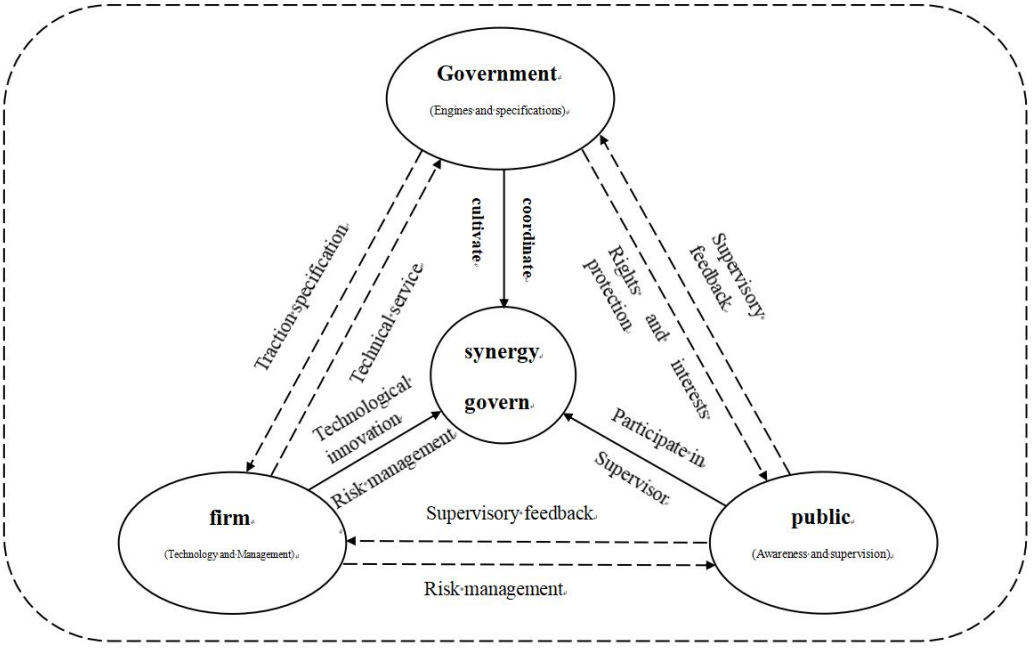

FIG. 1: Three-Dimensional Interactive Theoretical Model of "Government Leadership, Enterprise Drive, and Public Participation" in Collaborative Governance of Cross-Border Data Flow Security

4.1 Optimization of Policy and Supervision

To improve the legal system, it is essential to strengthen the research and formulation of relevant laws and regulations on cross-border data flows. This includes clarifying the classification standards for cross-border data flows, the rights and obligations of data subjects, and the rules for data storage and processing. Targeted cross-border rules should be developed for different types of data (such as personal sensitive data[22], business data[23], and national security data[24]) to ensure that regulations cover all aspects of cross-border data flow. Additionally, a mechanism for updating regulations should be established to adjust and improve regulatory content in a timely manner in light of technological developments and changes in the international situation. To optimize the regulatory strategy, a risk-oriented regulatory model should be adopted. This involves conducting differentiated supervision based on the degree of risk of cross-border data flow projects. High-risk cross-border data activities (such as those involving large amounts of sensitive personal information) should be subject to stricter supervision, while regulatory requirements for low-risk data sharing activities should be relaxed to reduce compliance costs for enterprises. Furthermore, a cross-border data flow monitoring platform should be established[25]. Utilizing big data analysis,

artificial intelligence, and other technologies, this platform will monitor the flow, direction, and content of cross-border data in real time, promptly detect and address violations, and improve regulatory efficiency through technical means.

4.2 Optimization of Technology and Innovation

First, to encourage technological innovation, the government can use fiscal subsidies, tax incentives, and other policy tools to encourage enterprises to increase their investment in technological innovation for cross-border data flow. A special fund should be established to provide financial support to enterprises that develop new data encryption technologies and cross-border data privacy protection schemes.Second, an industry-university-research cooperation mechanism should be established to promote collaboration among universities, research institutions, and enterprises in cross-border data technological innovation. Joint research projects on the safe storage of cross-border data and the optimization of cross-border data transmission should be conducted to accelerate the transformation of technological innovation results.Third, efforts should be made to promote the unification of technical standards[26]. International technical exchanges and cooperation should be strengthened to promote the international standardization of cross-border data flow technology. Active participation in the activities of international standards organizations and joint development of common cross-border data technical standards with other countries (such as data format standards and security certification standards) will reduce technical adaptation costs. Enterprises should also strengthen the research and development of technical compatibility to improve the applicability of technology in different data environments. Tools for cross-border data transfer that are compatible with multiple data infrastructures and security protocols should be developed.

4.3 Optimization of Public Trust and Participation

To enhance government credibility and transparency, a platform for information disclosure on cross-border data flows should be established to timely release policy information, project progress, and data security status[27]. Regular reports should be provided to the public on the supervision of cross-border data and the results of data breach incidents. The effectiveness of policy implementation should be evaluated, and any issues identified during the implementation process should be promptly corrected to ensure the realization of policy objectives. Third-party evaluators can be used to assess the implementation of policies on cross-border data flows, and the results should be made available to the public.Public participation should be increased by improving public participation mechanisms and expanding channels for public engagement. A public advisory committee on cross-border data flow projects should be established to solicit public views. An online feedback platform should be opened to facilitate the public's ability to express their suggestions and concerns about cross-border data flow projects at any

time. Public education should be strengthened to raise public awareness of cross-border data flows. Through publicity activities and the release of educational materials, the public should be informed about the significance, risks, and safeguard measures of cross-border data flow, enhancing public understanding and support for these projects[28].The interaction mechanism should be strengthened by establishing a regular communication mechanism between the government, enterprises, and the public. Regular trilateral forums on cross-border data flow should be held to share information and needs, and to promptly address any issues arising from the interaction process. Information technology should be used to build an interactive platform to achieve real-time information sharing and feedback. Through this platform, enterprises can timely report their technological innovation achievements and compliance operations to the government, the government can communicate policy adjustments to enterprises and the public, and the public can provide feedback and suggestions to the government and enterprises.

5 Outlook

Currently, data cross-border flow has emerged as a pivotal force driving economic globalization and international trade development. It not only accelerates the global allocation of data resources but also profoundly transforms traditional business models. As emerging technologies such as artificial intelligence (AI), the Internet of Things , and blockchain continue to advance and gain widespread adoption, cross-border data flow plays an increasingly central role in the global digital economy, serving as a key driver of economic growth and innovation.

Looking ahead, the scale and complexity of data cross-border flow are expected to grow significantly, presenting numerous uncertainties and challenges. Ensuring data security, privacy, and national sovereignty while facilitating the free flow of data across borders remains a critical issue for the international community. To address this, countries are anticipated to enhance their data governance capabilities, refine relevant laws and regulations, and intensify regulatory efforts on data cross-border activities. Simultaneously, international cooperation will become more robust. Establishing multilateral frameworks for data governance, formulating unified international standards and norms, and coordinating the positions and interests of various countries on data cross-border flow issues will be essential. These measures aim to build a fairer, more reasonable, and secure order for data cross-border flow, thereby addressing the global challenges posed by the digital age[29]. Moreover, technological innovation will play a crucial role in resolving the security and trust issues associated with data cross-border flow. Emerging solutions such as privacy-enhancing computing technology and decentralized data storage and sharing models are expected to gain wider application, providing technical support for the sustainable development of data cross-border flow.

References

[1] Jung Jaewon.(2022).The Effects of China's Participation in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP): A Quantitative Assessment.Sustainability(1),344-344.

[2] Musch Sean,Borrelli Michael Charles & Kerrigan Charles.(2024).Bridging compliance and innovation: A comparative analysis of the EU AI Act and GDPR for enhanced organisational strategy.Journal of Data Protection & Privacy(1),14-40.

[3] Rolf Schwartmann,Tobias Keber,Kai Zenner & Sonja Kurth.(2024).Data Protection Aspects of the Use of Artificial Intelligence — Initial overview of the intersection between GDPR and AI Act.Computer Law Review International(5),145-150.

[4] Wang Anna.(2022).Challenges faced by Russian companies involved in cross-border data flows.The Frontiers of Society, Science and Technology(7.0),

[5] Chakraborty Nilanjan.(2020).Data Security and Privacy of Individuals in Data Mining: A Critical Analysis of Data Mining in India.International Journal of Data Mining And Emerging Technologies(1),1-7.

[6] Nguyen Mau,Dinh MBA,Nguyen Hien,Master Master,Nguyen Bao & Mac Mac.(2020).Factors Affecting Disclosure of Accounting Information and Tax Rates Effects on The Risk Level of Listed Viet Nam Medicine Firms During Global Economic Crisis - And Roles of IT governance and Data Security in Risk Management- And Rol.Journal of Complementary Medicine Research(1),139.

[7] BMJ Publishing Group Limited.(2018).Data compliance in practice.Veterinary Record(8),214-214.
[8] B. Hema Kumari & V. Surya Narayana Reddy.(2019).Data Synthesis and Importance of Big Data Security Analytics for Securing the Enterprise Data.International Journal of Recent Technology and Engineering (IJRTE)(2),4808-4811.
[9] David DiMolfetta.(2024).Flaws in public records management tool could let hackers nab sensitive data linked to requests.Nextgov.com (Online)
[10] Rains Tim.(2020).Cybersecurity Threats, Malware Trends, and Strategies:Learn to mitigate exploits, malware, phishing, and other social engineering attacks.
[11] Enrico Del Re.(2024).Technologies of Data Protection and Institutional Decisions for Data Sovereignty.Information(8),444-444.
[12] Emmanuel Kasseris,Kasseris Emmanuel,Goteti Naga Srujana,Kumari Sapna,Clinton Bentley,Engelkemier Seiji... & Gençer Emre.(2020).Highlighting and overcoming data barriers: creating open data for retrospective analysis of US electric power systems by consolidating publicly available sources.Environmental Research Communications(11),115001-.
[13] Rongxin Bao,Zhikui Chen & Mohammad S. Obaidat.(2018).Challenges and techniques in Big data security and privacy: A review.Security and Privacy(4),n/a-n/a.
[14] Titilayo Modupe Kolade,Nsidibe Taiwo Aideyan,Seun Michael Oyekunle,Olumide Samuel Ogungbemi,Dooshima Louisa Dapo Oyewole & Oluwaseun Oladeji Olaniyi.(2024).Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security.Asian Journal of Research in Computer Science(12),36-57.
[15] Gyanchandani Vandana.(2024).Cross-border flow of personal data (digital trade) ought to have data protection.Journal of Data Protection & Privacy(1),61-79.
[16] Satish Rupraoji Billewar,Karuna Jadhav,V.P. Sriram,Dr. A. Arun,Sikandar Mohd Abdul,Kamal Gulati & Dr Narinder Kumar Kumar Bhasin.(2021).The rise of 3D E-Commerce: the online shopping gets real with virtual reality and augmented

reality during COVID-19.World Journal of Engineering(2),244-253.
[17] Labadie Clément & Legner Christine.(2023).Building data management capabilities to address data protection regulations: Learnings from EU-GDPR.Journal of Information Technology(1),16-44.
[18] MolnárGábor Fruzsina.(2023).[Protecting the rights and freedoms of individuals with regard to health data processing: the risk approach of the EU General Data Protection Regulation (GDPR)]..Bundesgesundheitsblatt, Gesundheitsforschung, Gesundheitsschutz(2),143-153.
[19] Jie Tan& Zhirong Jerry Zhao.(2024).Cost-Saving or Cream-Skimming? Partner Ownership and the Project Returns of Public-Private Partnerships in China.Journal of Chinese Political Science(prepublish),1-21.
[20] Jiang Lu & Wu Zetao.(2019). International Development Cooperation PPP: A New Model of More Effective Development Cooperation? International Outlook (06),46-67+151-152.
[21] [Liu W. (2015). Theoretical interpretation of PPP model and practical examples.] Reform (01),78-89.
[22] Nadine Nibigira,Vincent Havyarimana & Zhu Xiao.(2024).Sensitive Information Security Based on Elliptic Curves.World Journal of Engineering and Technology(02),274-285.
[23] Haodi Deng.(2024).Paradigm shift of commercial data protection: From an IP approach to a sui generis approach.Academic Journal of Humanities & Social Sciences(2),
[24] Kirstie Ball,Sara Degli Esposti,Sally Dibb,Vincenzo Pavone & Elvira Santiago-Gomez.(2019).Institutional trustworthiness and national security governance: Evidence from six European countries.Governance(1),103-121.
[25] Glasze Georg,Cattaruzza Amaël,Douzet Frédérick,Dammann Finn,Bertran Marie Gabrielle,Bômont Clotilde... & Zanin Caroline.(2023).Contested Spatialities of Digital Sovereignty.Geopolitics(2),919-958.

[26] Varda Mone & Sugana Mitharwal.(2024).Guardians of privacy: exploring the viability of a United Nations-backed global data governance.International Journal of Intellectual Property Management(2),194-216.
[27] Matusiak Matthew C,Cavanaugh Michael R & Stephenson Matthew.(2020).An Assessment of Officer-Involved Shooting Data Transparency in the United States..Journal of interpersonal violence(1-2),886260520913646.
[28] Rosilah Hassan,Wahiza Wahi,Nurul Halimatul Asmak Ismail & Samer Adnan Bani Awwad.(2022).Data Security Awareness in Online Learning.International Journal of Advanced Computer Science and Applications (IJACSA)(4),
[29] Chensha Wang,Yu Li & Lijing Liu.(2024).Algorithm Innovation and Integration with Big Data Technology in the Field of Information Security: Current Status and Future Development.Academic Journal of Engineering and Technology Science(2),