Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Research on the Legal Mechanism of Personal Information Protection in Cross-border Data Flows Based on Numerical Analysis Methods

Zhongguo Lv[1,] ✉

[1] *Law School, Huainan Normal University, Huainan, Anhui, 232038, China*

ABSTRACT

The rapid growth in the scale of cross-border data flow has pushed the protection of personal information to become an important issue of global concern. This paper drafts a legal adjustment mechanism for the protection of personal information under cross-border data, and builds a data sovereignty practice system from the aspects of comprehensive strength construction and cross-border flow pilot. It utilizes civil law, criminal law and administrative law to protect personal information in cross-border data flow. Based on the numerical analysis method, the legal protection mechanism of personal information in cross-border data flow is discussed in depth. The numerical analysis results show that the probability of personal information exposure increases to about 0.35 when the ratio of malicious nodes under the legal mechanism of this paper is 0.5. The estimated accuracy of personal information protection effect increases by 65.16% to 80.52% when the enforcement strength of this paper's mechanism is 0.7 and the sample size of companies is 300. Fixing the initial ratio of cross-border data information disclosure, the smaller the initial ratio of personal information protection, the faster the speed of personal information leakage under the legal mechanism. The investigators' scores on the personal information risk indicators of a cross-border e-commerce platform are uniformly distributed between 1 and 2, and the sum of the overall scores is less than 10, demonstrating the effectiveness of the legal mechanism constructed in this paper on the protection of personal information.

Keywords: Numerical analysis, cross-border data flow, personal information protection, legal mechanism

1. Introduction

In the context of the global digital economy, the relevant legal regulation is of great importance, and some countries even elevate it to a strategic level [1-2]. In addition, China and the United States are

✉ Corresponding author.
E-mail address: lvzhongguo@edu.cn (Z. Lv).
Received 17 July 2024; Revised 03 October 2024; Accepted 12 February 2025; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-015

currently competing for the leadership of digital commerce, the importance and urgency of the relevant issues is even more self-evident [3]. Obviously, once data crosses borders, it is no longer simply a matter of domestic law, which inevitably involves a variety of value selection and realization issues [4-5]. The legal regulation of personal information in cross-border data flow contains complex value issues [6]. First, legal regulation must pursue the realization of legal values, such as fairness and justice, freedom and order, etc., secondly, in today's era, data is an important symbol of national soft power and competitiveness, and the economic value and national security issues must also be considered when carrying out relevant legal regulation, and finally, data is generated by individuals, so it is inevitable to involve social and cultural values [7-10].

As a populous country and a data powerhouse, China's data base, market base, and national policy base are gradually adapting to the trend of digital trade globalization [11]. However, in the specific cross-border practice with changing circumstances, shortcomings such as the lack of an independent personal data information regulator, fragmented data protection norms, low self-regulation of enterprises, and insufficient international participation are constantly highlighted, and while enjoying the data dividend, it is also facing the risky problem of data cross-border [12-14]. Therefore, it is necessary to improve the relevant system of cross-border data protection in China on the basis of the experience of personal data information protection between the United States and European countries, actively promote trade negotiations, and strengthen the importance of data information security while promoting the development of the digital economy [15-17].

China has established a legal framework for a cross-border regime for personal data information centered on the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, as well as relevant draft laws and regulations, which provide a legal basis and regulatory requirements for the cross-border flow of personal data information [18-19]. However, the existing rules are fragmented and lack a comprehensive and complete protection system for cross-border flow of personal data [20]. China should learn from the excellent experience of the EU, combine with China's specific practice, promote the formation of a systematic legal framework system for personal information protection, and improve China's cross-border data protection system [21].

Bu-Pasha, S analyzes the judicial practice of cross-border data information transfer and protection in the EU, while highlighting the differences between judicial theory and judicial practice [22]. Ziyi, X examines the problems in China in the area of cross-border transmission of personal privacy information and draws on the experience of advanced foreign jurisdictions and administrations in order to improve the relevant legislation on cross-border data flow [23]. Malahleka, M begins by describing the characteristics of the revolutionized cross-border transfer of information contained in cloud computing technology and uses the EU General Data Protection Regulation (GDPR) as a reference to unearth the shortcomings of the Protection of Personal Information Act No. 4 of South Africa (POPIA) [24]. Tehrani, P. M et al. examined the ecological position of the Data Protection Directive globally and where the new General Data Protection Regulation has changed, and found that the new regulation still retains the guidelines related to cross-border transfers, and also analyzes the underlying logic of the special cases and the transition from the Safe Harbor to the U.S.-European Privacy Shield, which provides some insights into the research related to cross-border data transfers [25]. Chen, M [26] discusses the need for personal information protection to reach a relative balance with the development of the digital economy, and points out that the global governance of cross-border data transmission has not matured, and that China needs to strengthen international cooperation on cross-border data transmission and gradually improve cross-border data flow regulations and rules in order to promote global data governance.

The opening chapter of the article briefly describes the connotation of personal information, the relationship between cross-border big data and personal information, and analyzes the current status of the legal mechanism for personal information protection. Accordingly, this article constructs a legal mechanism for the protection of personal information in cross-border data flows. Through the practice

system of data sovereignty under cross-border data flow, the phenomenon of legal interest infringement under cross-border data flow is reduced. Under the supervision of civil law, criminal law and administrative law, the legal adjustment normative system of personal information protection is improved. Finally, establish a numerical model for personal information protection, and evaluate the effectiveness of the legal protection mechanism established in this paper on personal information protection based on the uniqueness and convergence of the numerical solution of the model.

2. Study of legal mechanisms for the protection of personal information

Personal information [27] is information that can be used to identify a specific individual at once or based on a combination thereof. In common perception, personal information refers to all personal data, including the type of network used, news and videos viewed, specific chats, and so on. Usually when using electronic products to operate the use of APP, there will be a similar selection and collection of relevant personal information, the purpose is that the platform to use this to understand the user's good and bad, to carry out accurate push, to achieve personalized service. However, the continuous rise and development of face recognition technology, fingerprint collection, but also in the network network in the realization that personal information contains much more than the general sense of personal data, biological data is also an important part of it.

2.1. Relationship between cross-border big data and personal information

In order to clearly choose what kind of personal information protection path and its legal mechanism, it needs to be clear where the boundary of the right to personal information is located in the situation where personal information and big data are intertwined. In order to effectively balance the dichotomous values of personal information protection and cross-border big data [28] industry development, it is important to clarify the scope of personal information and cross-border commercial information that can be included in legitimate interests, and to clarify the interests enjoyed by individuals on personal information and the interests enjoyed by operators as data controllers. Personal information is information that can be used to identify a specific individual, either indirectly or directly, as described above. In order to protect personal information on one hand and develop the cross-border big data industry on the other, the rights given to individuals in personal information should not take an absolutely exclusive form. A certain amount of discretionary space can be given to data controllers, which is conducive to the development of the Internet and gives data controllers more incentives.

2.2. Analysis of the current state of legal protection of personal information

For the time being, China does not have a specific law on personal information, but its protection is dispersed in various laws. The Constitution states that individuals have the right to freedom and privacy of communication, and Amendment (VII) to the Criminal Law adds two additional crimes to regulate the sale, illegal provision and sale of personal information. The Ninth Amendment to the Criminal Law has broadened the scope of application. The General Principles of the Civil Law suggests that the law protects the security of personal information and that other subjects can only access it if they comply with the law and are able to ensure that it will not be leaked and utilized in bad faith, on which basis. In 2014, the Supreme People's Court issued a Judicial Interpretation, which for the first time clarified the path of protection under tort law. The Network Information Office's Data Security Management Measures (Draft), released in May 2019, suggests that apps cannot force individuals to consent to the collection of information, meaning that network operators cannot force or mislead information subjects to agree to default authorization bindings for the collection of personal information, etc. Overall, the increasingly frequent cases of personal information infringement need to

be addressed through relevant provisions scattered in various sectoral laws, which lack binding force on related infringement cases.

3. Construction of a legal adjustment mechanism for the protection of personal information under cross-border data

3.1. Constructing a Practical System of Data Sovereignty under Cross-border Flow of Data

Based on the analysis of the characteristics of data sovereignty in the context of data economy in the new era, a reasonable data sovereignty system can strengthen the driving effect of cross-border flow of data on international economy and trade, and the infringement of legal interests under the phenomenon of cross-border flow of data should be regulated by a complete data sovereignty system.

3.1.1. Comprehensive data sovereignty strength building. The assertion and construction of data sovereignty [29] is embodied in legal policies, "the essence of policy making is a game of interests under multiple factors such as the level of information technology in the country and other countries, the scale of the digital industry, the legal status of data protection, and the international environment, etc.", and the capacity of data technology, data market and industry system, and the capacity of data system protection are the data technology capability, data market and industry system, and data institutional guarantee capability are the three major factors that determine the comprehensive strength of national data sovereignty. At the level of data technology capability, we have continuously invested innovative funds and talents in technical strengths such as artificial intelligence, 5G communications, and industrial internet. In the field of cross-border data flow, it has set up specialized technical support services to facilitate the flow of data and improve industrial efficiency and output. At the level of the data market and industrial system, we will give full play to the role of the market regulation mechanism of the National Big Data Trading Center, eliminate the data silos of low-risk data, and ensure the legal and orderly circulation of data.

3.1.2. Pilot cross-border flow of data. On the basis of the data exit security management system, the construction of a "regulatory gateway" for cross-border data flows is being carried out in conjunction with the full-process functions of data "trading ports" in terms of transaction safeguards, governance and supervision, and dispute resolution.

1) In terms of transaction security, the "trading port" summarizes the transaction needs of multiple parties, breaks down the information asymmetry barrier, and provides basic services of data transmission, storage and settlement for the transaction process.

2) If the data exit security assessment is recognized as a low-risk data exit activity, the regulatory terms of reference include monitoring whether a data security incident occurs in the data exit activity, whether there is any violation of law on the part of the subject of the transaction, and whether the data exit activity is carried out in accordance with the exit plan, etc., and imposing legal sanctions, and establishing a mechanism for the transmission of information with the government.

3) In terms of dispute resolution, in the event of data leakage or infringement in the course of cross-border flow of data, a fast and fair dispute resolution mechanism will be established in conjunction with the technical assistance of the blockchain privacy computing system.

3.1.3. Increased participation and ownership of ICFs:

1) Enhancing Participation in International Agreements on Cross-Border Data Flows. In the past four decades since the Internet became widespread, the OECD, APEC, and digital trade cooperation among multilateral countries have contributed to the consistency of governance systems through the development of an international rules framework that accommodates as much as possible the cultural diversity of countries' laws and policies while establishing a standardized governance framework for cross-border data flows. Promoting the free flow of data in the framework of multilateral cooperation

is an important way to develop the global data economy under the principle of respecting data sovereignty.
2) Enhancing the dominance of multilateral cooperation. As a member of ASEAN and a technological powerhouse with a sizable data economy, China, when selectively joining the cooperation initiatives of international organizations, should promptly publicize China's protection path and governance experience in cross-border data flow, carry out regional cooperation and win-win situation in the data industry on the basis of China's international cooperation initiatives, and strengthen the international rules and regulations by means of scientific and complete means of the rule of law and strong technological support. Dominance.

3.2. Improvement of the legal adjustment normative system for the protection of personal information

3.2.1. Playing a central role in guaranteeing private rights under civil law:
1) Strengthening the overarching provisions on personal information protection. China's General Principles of Civil Law is still in the drafting stage. It is worth noting that the General Principles of the Civil Law has newly added the right to "personal information" and established the protection of "data" in Article 111 compared to the General Principles of the Civil Law of 1986, and that the provisions on personal information protection in this article have continued the mainstay of the legislation on personal information protection in the previous legislation. This article on the protection of personal information continues the legislative backbone of the previous legislation on the protection of personal information, and sets prohibitive obligations on the controller of personal information, without specifying that the collection of personal information should follow the rules related to the notification of consent.
2) Improvement of legislation on personal information privacy related to personality rights. As the encyclopedia of people's lives and the fundamental law of the private law system, civil law should pay more attention to the privacy protection of personal information in the era of big data. Each personal information is an equal subject in the big data network, and its privacy should be treated equally. The privacy component of personal information, as an element of personality, should be stipulated in the personality rights section of the forthcoming civil code to provide a stronger legal basis for the protection of personal information privacy.

3.2.2. Utilizing the deterrent effect of criminal law on crimes against personal information:
1) Expanding the protection of personal information under criminal law. In the absence of a specific law on the protection of personal information, the criminal law has served as a deterrent to prevent high-risk behaviors in the use and transfer of personal information from seriously infringing on the legitimate rights and interests of the subject of the information, resulting in serious personal and property damage. According to the concept of "risk-oriented", the criminal law shall only regulate the behaviors that are recognized as high-risk in the process of using personal information.
2) Establishing Dynamic Recognition Criteria for Personal Information Crimes. By setting up dynamic judgment standards for "serious situations" in personal information crimes, the criminal law will more effectively regulate personal information crimes and weaken the rigidity of the relevant standards in the current Interpretation.
3) Strengthening the horizontal and vertical three-dimensional design of the criminal law to sanction personal information crimes. Under the status quo of the involvement of multiple subjects, in order to balance the multiple legal interests of personal information, punish personal information crimes in a more detailed manner and increase the deterrent effect of the criminal law, personal information crimes should be sanctioned horizontally (to protect different legal interests) and vertically (to sanction crimes committed by individuals at different stages).

3.2.3. Refinement of the rules for supervising the protection of personal information in administrative law:

1) Establishment of a Privacy Risk Assessment Mechanism for the Use of Personal Information by Administrative Organs. Privacy risk assessment is an important part of personal information protection that abandons "dualism" and embraces "genealogy" of personal information risk perception. The assessing party will take appropriate management measures based on the risk level derived from the privacy risk assessment, and extend the assessment to the entire cycle of the development and utilization of personal information, with a view to controlling the privacy risk to a minimum. The use of the privacy risk assessment mechanism by administrative departments related to the cross-border big data industry and cybersecurity in the process of supervising the use of personal information can be targeted to determine whether the use of information by a particular individual is highly risky.

2) Improving the Supervision Mechanism of Personal Information Management. First of all, a more feasible way to supervise the current situation in China is to base on the existing administrative reconsideration system, and make the administrative reconsideration organization as the supervisory organization of personal information protection, and give it the corresponding authority. In accordance with the provisions of the Administrative Review Law, the internal organization of the administrative review authority shall perform the review duties. At the same time, detailed clarification of the powers and responsibilities of the supervisory authority is a prerequisite for compliance with the law. Too general a specification of powers will lead to the expansion of the powers of the administrative body, and the clarity or otherwise of the obligations will determine to a large extent whether the regulatory function is given full play.

4. Numerical analysis of the process of protection of personal information by legal mechanisms

4.1. Modeling

Since the coefficients of the drift and diffusion terms in the process of personal information protection are constants, such a setup is easier to get the results, however it is oversimplified. So the original model is improved to establish a reasonable and different model. The CIR model [30] is chosen as an alternative to the drift term coefficients and diffusion term coefficients. In this way, a model of the system of equations consisting of three stochastic differential equations is obtained, each of which has a Brownian motion, and the Brownian motion of the drift term equation and the diffusion term equation is correlated with the Brownian motion in the equation of the personal information protection process, while the Brownian motions of the two of them are not correlated.

Therefore the following price process with random drift and diffusion terms is created:

$$\begin{cases} dS_t = R_t S_t dt + L_t S_1 dB_t \\ dR_t = a_1\left(b_1 - R_t\right)dt + c_1\sqrt{R_t}\,dB_t^1 \\ dL_t = a_2\left(b_2 - L_t\right)dt + c_2\sqrt{L_t}\,dB_t^2 \end{cases} \tag{1}$$

where $dB_t dB_t^1 = \rho_1 dt$, $dB_t dB_t^2 = \rho_2 dt$, $dB_t^1 dB_t^2 = 0$, a_1, a_2, b_1, b_2 are constants and satisfy $a_1 > 0$ and $a_2 > 0$. the first equation in the system of equations (1) is built based on geometric Brownian motion, and b_i, $i = 1,2$ in the regular terms of the last two equations can be understood as the mean value, and when the variable exceeds the mean value, the difference is negative, and this results in a tendency for the equations to move downwards, and vice versa, and this property is called mean reversion. The non-negativity of the latter two equations is ensured by the form of their diffusion term coefficients.

4.2. Existence uniqueness of model solutions

The uniqueness of the existence of solutions for the established nonlinear price model is verified:

The first equation in the system of equations (1) is first analyzed, and since it resembles the geometric Brownian motion, drawing on it, i.e., applying Ito's formula for $\ln S_t$, the result is as follows:

$$\begin{aligned} d\ln S_t &= \frac{1}{S_t}dS_t - \frac{1}{2}\frac{1}{S_t^2}dS_t dS_t \\ &= \left(R_t - \frac{1}{2}L_t^2\right)dt + L_t dB_t \end{aligned} \tag{2}$$

So it can be obtained:

$$S_t = S_0 \exp\left(\left(R_t - 0.5L_t^2\right)t + L_t B_t\right) \tag{3}$$

This is the displayed solution of S_t with unknown parameters. If it can be shown that the equations of R_t and L_t satisfy the existence of solutions uniquely, then it follows that S_t satisfies the existence of solutions uniquely.

Observing that the equations satisfied by R_t and L_t are of the same form, consider the following unified form for ease of writing:

$$dR_t = a\left(b - R_t\right)dt + c\sqrt{R_r}dB_t \tag{4}$$

Lemma 1: For equations of the form $dx_t = f\left(x_t\right)dt + g\left(x_t\right)dB_t$, $0 \le t \le T$, the following equation is satisfied if for any integer $k \ge 1$, there exist positive numbers m_k^1 and m_k^2 satisfying, for all $t \in [0,T]$ and all $x, y \in R$, and with $\min\left\{|x|,|y|\right\} \ge 1/k$, $\max\left\{|x|,|y|\right\} \le k$:

1) $\max\left\{|f(x)-f(y)|^2, |g(x)-g(y)|^2\right\} \le m_k^i |x-y|^2$.

2) $\max\left\{|f(x)|^2, |g(x)|^2\right\} \le m_k^2\left(1+|x|^2\right)$.

Then there exists a unique solution of the equation x_t, $x_t \in \mathrm{M}^2([0,T],R)$.

Prove the two theorems about the existence of unique solutions to the solutions of the sub-model of the price model based on the existing lemmas and mathematical tools, based on which the conclusion about the existence of unique solutions to the whole model is obtained.

Theorem 1: When $R_0 > 0$, for any $T > 0$, there exists a unique solution to equation (4) on $[0,T]$.

Proof: $f\left(R_t\right) = a\left(b - R_t\right)$, $g\left(R_t\right) = c\sqrt{R_r}$, f and g in equation (4) are continuous functions, so even when k is large enough and $t \in [0,T]$, $R_t \in (1/k, k)$ is bounded at $f(x)$, $g(x)$, there exists a constant m_k that is satisfied:

$$\max\left\{f^2\left(R_t\right), g^2\left(R_t\right)\right\} \le m_k\left(1 + R_t^2\right) \tag{5}$$

If R_{1t} and $R_{2t} \in (1/k, k)$ are set at the same time, there is:

$$\left|f\left(R_{1t}\right) - f\left(R_{2t}\right)\right| = a\left|R_{tt} - R_{2t}\right| \tag{6}$$

$$\left|g\left(R_{1t}\right) - g\left(R_{2t}\right)\right| = c\left|\sqrt{R_{1t}} - \sqrt{R_{2t}}\right| \le n_k\left|R_{1t} - R_{2t}\right| \tag{7}$$

where $n_k = \max\{2c\sqrt{k}, c/2\sqrt{k}\}$.

Taking $m_k^1 = \max\left\{n_k^2, a^2\right\}$ gives:

$$\max\left\{\left|f\left(R_{1t}\right) - f\left(R_{2t}\right)\right|^2, \left|g\left(R_{1t}\right) - g\left(R_{2t}\right)\right|^2\right\} \le m_k^1\left|R_{1t} - R_{2t}\right|^2 \tag{8}$$

Thus, it follows from Lemma 1 that there exists a unique solution to equation (4) on $[0,T]$.

4.3. *Convergence of the numerical solution of the model*

From the previous subsection it is known that equation (4) has a solution, and before solving it numerically, it is important to see if the solution of the model bursts at infinity, i.e. if the limit of the solution is moment bounded. This can be obtained by integrating both sides of equation (4) before taking the expectation:

$$\begin{aligned} E\left(R_t - b\right) &= E\left(R_0 - b\right) + a\int_0^t E\left(b - R_m\right) dm \\ &= E\left(R_0 - b\right) e^{-at} \end{aligned} \tag{9}$$

The second equality sign in the above equation is obtained from Gronwall's inequality. So there is $\lim_t E\left(R_f\right) = b$, which means that the first order moments of equation (4) are bounded under $b < \infty$.

The result can be obtained by applying Ito's formula to R_r^2 and then taking the expectation and then using the R_f first order moments:

$$\begin{aligned} E\left(R_t^2 - b^2 - \frac{bc^2}{2a}\right) &= \left(2b + \frac{c^2}{a}\right)\left(E\left(S_0\right) - b\right)e^{-at} \\ &+ \left(E\left(S_0^2\right) + \left(b + \frac{c^2}{2a}\right)\left(b - 2E\left(S_0\right)\right)\right)e^{-2at} \end{aligned} \tag{10}$$

Thus when $t \to \infty$, $E\left(R_t^2\right) \to b^2 + bc^2/2a$, i.e. if a, b, and c are finite one obtains a bounded second order moment of R_t.

Next, we start analyzing the numerical solution of the model, and for the sake of brevity, only the most basic Euler's method is studied; higher-order algorithms inherit the properties of Euler's method. For step $\Delta t > 0$, the known R_0, take the discrete estimates $r_n \approx R\left(t_n\right)$, $t_n = n\Delta t$ whose discretized numerical solutions are:

$$\begin{aligned} &r_{n+1} = r_n\left(1 - a\Delta t\right) + ab\Delta t + c\sqrt{r_n}\Delta B_n \\ &Which\ \Delta B_n = B\left(t_{n+1}\right) - B\left(t_n\right) \end{aligned} \tag{11}$$

For equation (11) n iteration and then the mathematical expectation can be obtained as follows:

$$E\left(r_n\right) = \left(1 - a\Delta t\right)^n \left(E\left(r_0\right) - b\right) + b \tag{12}$$

From (12), it is clear that the choice of step size has an effect on the expectation of the numerical result

If $\Delta t < 2/a$, then there is $E\left(r_n\right) \to b$ at $n \to \infty$.

If $\Delta t = 2/a$, then there is $E\left(r_n\right) = (-1)^n E\left(r_0\right) + \left((-1)^{n+1} + 1\right)b$.

If $\Delta t > 2/a$, then there is $E\left(r_n\right) \to \infty$ at $n \to \infty$.

Only when the step size is small $(\Delta t < 2/a)$, the limit of the first order moments of the numerical solution corresponds to the true solution. And it can be obtained that the first order moments of the numerical solution are bounded, i.e. $\left|E\left(r_n\right)\right| \le \max\left(E\left(r_0\right), 2b - E\left(r_0\right)\right) = K\left(r_0, b\right)$.

The points obtained by the numerical methods used are discrete points, and the equations between the discrete points can be simulated with continuous subdivision $r(t) = r_n + a\left(b - r_n\right)\left(t - t_n\right) + c\sqrt{r_n}\left(B(t) - B\left(t_n\right)\right)$, $\forall t \in \left[t_n, t_{n+1}\right)$. Or step function $\bar{r}(t) = r_n$, $\forall t \in \left[t_n, t_{n+1}\right)$. The simulated values of the continuous subdivision simulation and the step function simulation at the discrete points are equal, i.e. $\bar{r}\left(t_n\right) = r\left(t_n\right) = r_n$.

Theorem 2: When $\Delta t < 1/2a$, there is for $\forall t \in [0,T]$:

$$E\left((r(t)-\bar{r}(t))^2\right) \le \Delta t\Big[a\left(b^2+2bK\left(r_0,b\right)+L(a,b,c,E)\right) +c^2\sqrt{L(a,b,c,E)}\Big] = \Delta t O(a,b,c,E) \tag{13}$$

PROOF: Assumption $t \in [n\Delta t,(n+1)\Delta t]$ Then there:

$$\begin{aligned} E\left((r(t)-\bar{r}(t))^2\right) &= E\left[\left(a\left(b-r_n\right)\left(t-t_n\right)+c\sqrt{r_n}\left(B(t)-B\left(t_n\right)\right)\right)^2\right] \\ &= a^2\left(t-t_n\right)^2 E\left[\left(b-r_n\right)^2\right]+c^2\left(t-t_n\right)E\left(r_n\right) \\ &\le a^2\Delta t^2 E\left[\left(b-r_n\right)^2\right]+c^2\Delta t\sqrt{E\left(r_n^2\right)} \\ &\le \Delta t\Big[a\left(b^2+2bK\left(r_0,b\right)+L(a,b,c,E)\right)+c^2\sqrt{L(a,b,c,E)}\Big] \end{aligned} \tag{14}$$

Theorem Proof Completion.

5. Results of the numerical analysis of legal mechanisms for the protection of personal information

5.1. Evaluation and analysis of personal information exposure rate

This section analyzes the effectiveness of the constructed legal mechanism on personal information protection through numerical simulation. In order to more objectively represent the ability of the legal mechanism in this paper to protect personal information and the integrity of cross-border data, this section uses the self-made cross-border data personal information protection dataset (CBDPIPDS) as the node movement trajectory. This empirical dataset was completed by 50 volunteers, recording node encounters during cross-border data flows, and the whole process took 5 days. And this dataset contains common attribute information of the nodes such as location, age, hobbies, and friendships. The above mechanism is numerically analyzed on MATLAB software. The performance metric for numerical analysis in this part is the personal information exposure rate, i.e., the ratio of the number of exposed personal information to the total number of generated personal information.

Fig. 1 shows the variation of personal information exposure probability for the theoretical analysis and numerical analysis experiments with different ratio of malicious nodes. As can be seen from the figure, with the rise of the malicious node ratio, the personal information leakage probability of both the theoretical analysis results and the numerical analysis results in this paper show an increasing trend. When the proportion of malicious nodes is 0.5, the personal information leakage probability of numerical analysis is about 0.35. The reason for this is that malicious nodes will arbitrarily intercept, discard or even tamper with the information sent by normal nodes, making the risk of information privacy leakage. Therefore, the higher the proportion of malicious nodes, the higher the number of information slices obtained by malicious nodes in cross-border data flow, the higher the probability of information being restored, and the higher the probability of privacy leakage. In addition, the theoretical analysis results have the same change trend with the numerical analysis results in this paper, and the quantitative difference of the probability of personal information leakage between the two under different malicious node ratios is maintained below 5.5%.

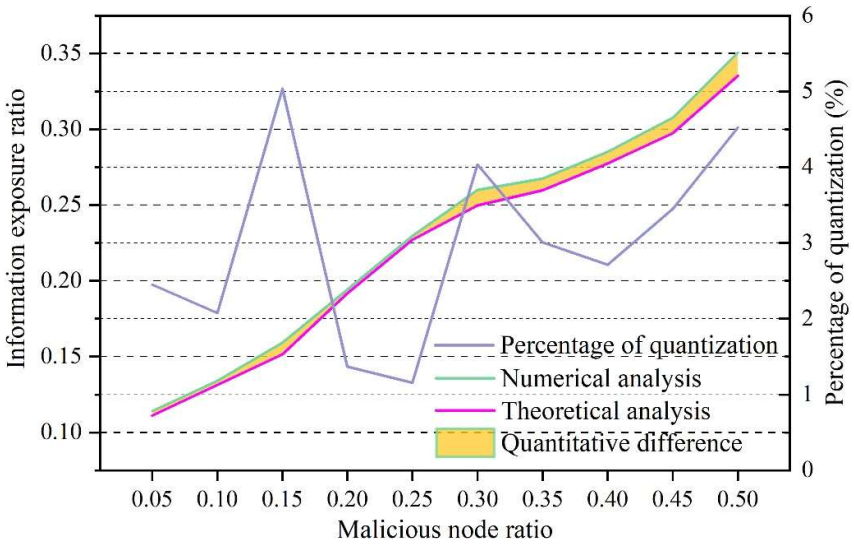


Fig. 1. Personal information leakage probability change

5.2. Impact of implementation intensity on the effectiveness of information protection

This subsection investigates the changes of the legal mechanism of personal information protection with the increase of enterprise samples, and sets the number of enterprise samples = 50, 100, 150, 200, 250, and 300, and carries out the estimation of the mean absolute difference (MAD) of the effect of personal information protection under different enforcement strengths of the legal mechanism of personal information protection of this paper by numerical simulation with different enforcement strengths of the mechanism (ES).

The mean absolute difference of personal information protection for different enforcement strengths under different sample sizes is shown in Figure 2. The data in the figure shows that for different execution strengths, when the sample size increases, the mean absolute difference decreases, and the accuracy of personal information protection effect estimation increases. And from the table, it can be seen that when the sample size is relatively large, the precision of personal information protection effect estimation increases with the increase of the enforcement intensity of the legal mechanism. For example, when the sample size of enterprises is 300, the average absolute difference of ES=0.7 is 65.16%~80.52% lower than that of other implementation strengths, and the precision of personal information protection effect estimation increases by 65.16%~80.52%. When the enforcement strength of the legal mechanism is higher, it means that the relevant law enforcement departments can strictly and effectively enforce the personal information protection laws, and investigate and deal with the illegal behaviors in a timely and accurate manner, which improves the estimation precision of the personal information protection effect in the numerical analysis.

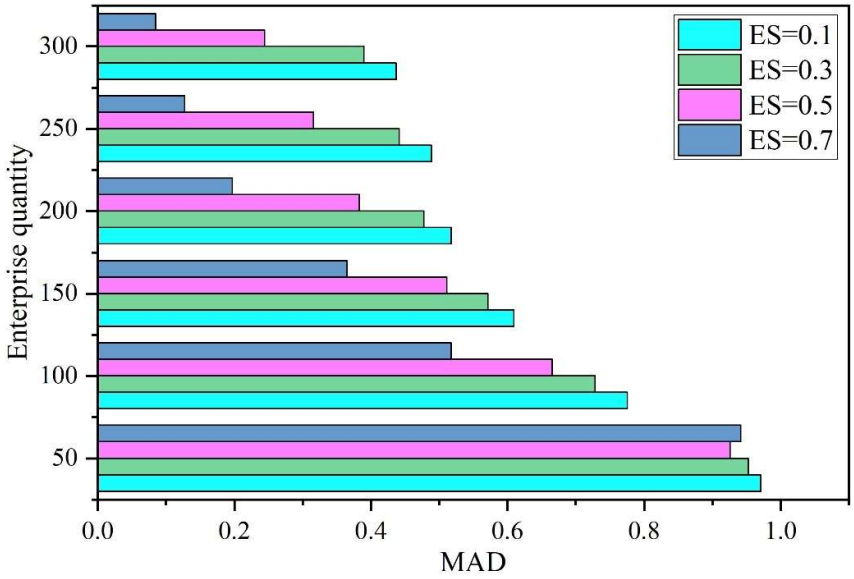


Fig. 2. The average absolute difference between different execution intensity

In this section, the effect of different number of users on the selection success rate is investigated by numerical analysis method, as well as verifying the level of personal information protection at different sensing user selection success rates among the sensing users that have been successfully selected. The selection success rate indicates the ratio of the perceived users that have been selected by applying the perceived tasks to the perception platform and finally selected.

Figure 3 shows the changes of user selection success rate and personal information protection level under the legal mechanism of this paper. From the figure, it can be seen that with the increase of the number of sensing users, the selection success rate shows an upward trend, which is due to the fact that with the increase of the number of sensing users, the type of users required for the sensing task is more extensive, and the platform has more and more choices for the users, and it can also find more sensing users that are in line with the sensing task. In addition, under the legal mechanism in this paper, the level of personal information protection gradually decreases with the increase of selection success rate, but still has a level of personal information protection of more than 70%. This is because under the legal mechanism in this paper, platforms need to follow stricter legal regulations and requirements, and for this reason, they take a higher level of protection measures to avoid a significant decrease in the level of personal information protection.

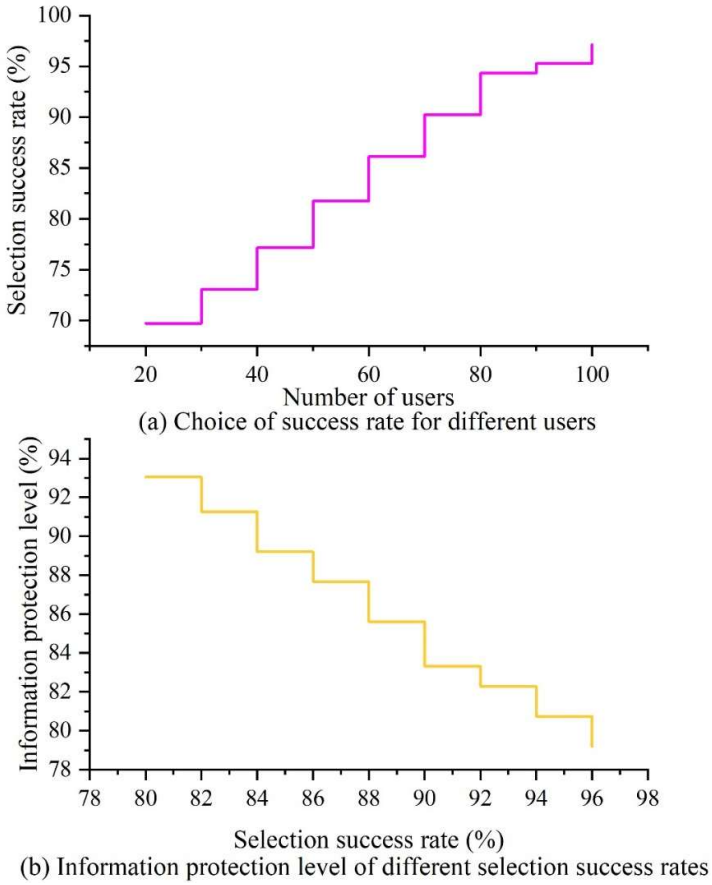


Fig. 3. Selection success rate and the level of personal information protection

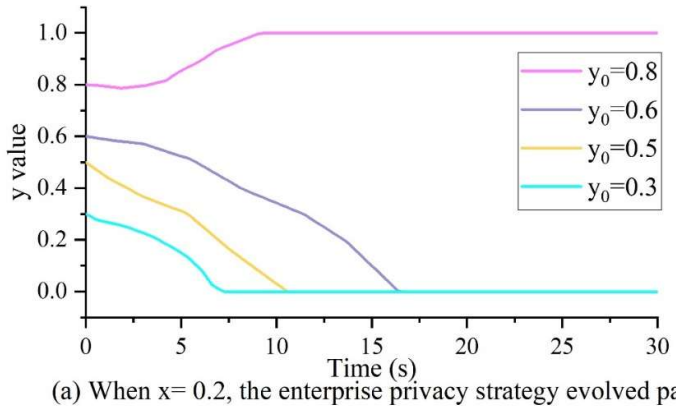
5.3. Evolution of protection strategies under cross-border data disclosure

In order to more intuitively illustrate the influence of parameters related to the legal mechanism of personal information protection on the evolutionary stabilization results of information protection, this section uses MATLAB software to simulate the dynamic evolutionary process. In this numerical analysis simulation, the proportions of personal information of cross-border data provided by consumers are set as: x = 0.2 and x = 0.4, respectively, and the evolutionary paths of the initial proportion y0 of different personal information protection are observed.

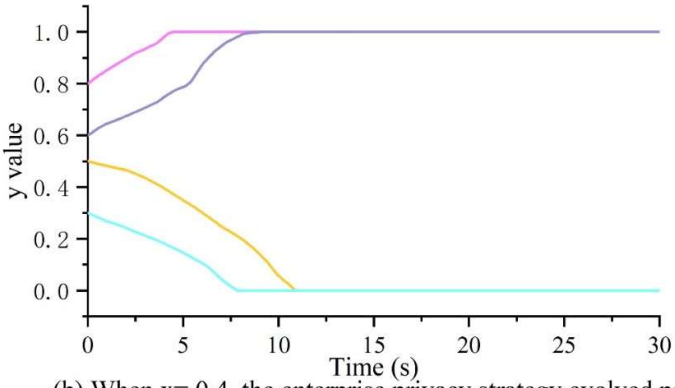
Figure 4 illustrates the evolution path of personal information protection strategies. The curve in the figure shows that when the initial proportion of cross-border data information disclosure of consumer groups is 0.2, the impact of the initial proportion y0 of different personal information protection on the evolution path of information protection strategy of legal mechanism is also different. It is clear from the figure that when the proportion y of personal information protection reaches a high threshold, the personal information protection strategy evolves to the position of 1 over time. Moreover, when the proportion x of information provided by consumers is a constant value, the smaller y0 is, the faster it tends to 0, i.e., the faster the legal mechanism makes a decision not to protect consumers' personal information.

When the initial proportion of consumer groups disclosing information x = 0.4, two of the four evolutionary paths eventually evolve to y = 1. Compared to x = 0.2, it is found that the legal mechanism increases the likelihood of consumer personal information protection when the proportion of consumers disclosing information in cross-border data increases. (Since the evolutionary path diagram at x = 0.4 is already clearly differentiated from the case at x = 0.2, as the value of x increases, the greater the likelihood that the system will evolve to, the evolutionary path diagrams will not be done here for larger values of x). Therefore, in cross-border data flows, whether consumers disclose

personal information or not will directly affect the incentives of legal mechanisms to protect the information.



(a) When x= 0.2, the enterprise privacy strategy evolved path



(b) When x= 0.4, the enterprise privacy strategy evolved path

Fig. 4. The evolutionary path of personal information protection strategy

5.4. Personal Information Protection Risk Level Assessment

In this section, the user registration and login system of a cross-border e-commerce platform is selected as the data for the study of personal information protection level. The system can collect, store, use as well as share personal information processing functions. Fifty investigators, including technical experts, business personnel, and legal personnel, were invited to conduct a comprehensive assessment of the risk of personal information protection from different perspectives. Data and information related to the system's personal information were collected through questionnaires, data analysis, and interviews. Five aspects, namely, the nature of the enterprise, the amount of data processing, the frequency of data access, whether the information can be accessed without authorization, and the number of employees' annual training, are recorded as dimensions 1-5 in order to classify the risk level. Numerical scoring is used to quantify the enterprise personal information risk index, i.e., scoring from 1 to 5, the higher the score corresponds to the higher risk, with a full score of 25. The risk is classified into three levels: low-risk ($\leqslant$10), medium-risk (10~20), and high-risk ($\geqslant$20).

The risk level evaluation results of the enterprise under the personal information protection mechanism constructed in this paper are shown in Figure 5. From the figure, it can be seen that the investigators' scores for the enterprise's personal information risk index are between 1 and 2, and the sum of the investigators' scores in the five dimensions does not exceed 9. The average score of the overall risk index is about 7.52 <10, and the personal information risk level is low. It indicates that under the legal mechanism of personal information protection constructed in this paper, the relevant regulatory authorities have strict education on the supervision of this field, and can detect and investigate the infringement of the rights and interests of personal information in a timely manner, so as to provide an effective deterrent to the potential risks.

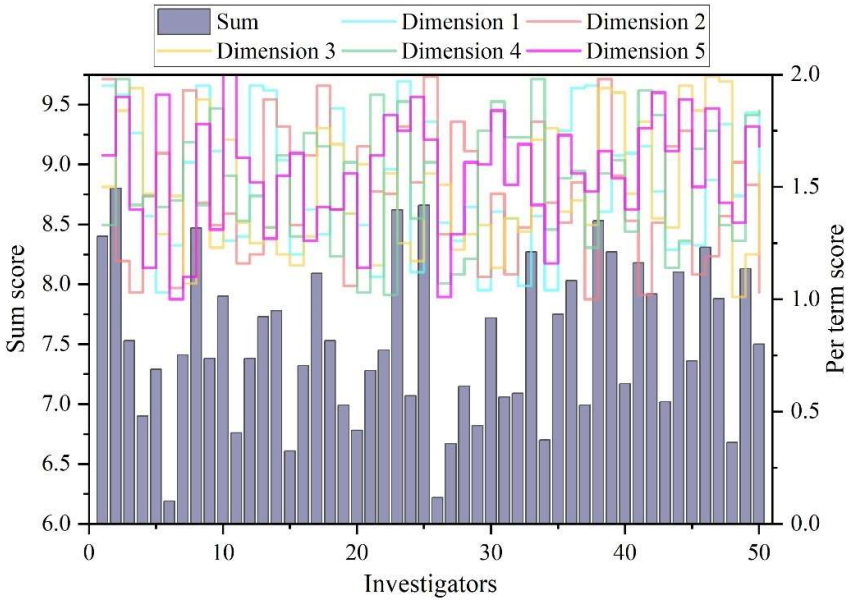


Fig. 5. The risk level of the enterprise is evaluated

6. Conclusion

This paper conducts a study on the legal mechanism for the protection of personal information in cross-border data flows. Through the construction of a comprehensive example of data sovereignty, the establishment of a pilot for cross-border data flow and the building of an international cooperation framework, the sovereignty system under data cross-border is stabilized. It gives full play to the role of civil law in safeguarding private rights, utilizes criminal law to dispose of crimes against personal information, and combines administrative law to realize the supervision of personal information protection. Based on the numerical analysis method, we quantitatively analyze the role of legal mechanism in protecting personal information in cross-border data flow.

In the numerical analysis under the legal mechanism for personal information protection constructed in this paper, the personal information exposure rate increases with the increasing proportion of malicious nodes, and the percentage of quantitative difference in the probability of personal information exposure from the theoretical results is below 5.5%. The estimation accuracy of the personal information protection effect is highest when the enforcement strength of the legal mechanism is 0.7. Different initial proportion x of personal information protection corresponds to different evolution paths of information protection strategy of legal mechanism, when x=0.4, there are two paths to reach the maximum possibility of evolution. The overall risk index of personal information of a cross-border e-commerce platform under the legal mechanism in this paper is about 7.52, with a low risk level. This paper systematically analyzes the legal mechanism of personal information protection in cross-border data flow in this paper through numerical analysis method, aiming to provide theoretical support and practical guidance for personal information protection in the era of digital economy.

Funding

This work was supported by Anhui Provincial Department of Education Humanities Key Project: "Empirical Approach to Criminal Compliance Risk Patterns and Decriminalization of Small and Medium sized Enterprises" (2024AH053234).

References

[1] Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. Wash. Int'l LJ, 29, 485.

[2] Gyanchandani, V. (2024). Cross-border flow of personal data (digital trade) ought to have data protection. Journal of Data Protection & Privacy, 7(1), 61-79.

[3] Nefedov, B., & Istomin, N. (2021). Features of the Development of Intersystem Legal Formations Designed to Regulate Personal Data Protection during Cross-Border Transfer. Russ. Jurid. J., 164.

[4] Yenlik, B., Olga, U., Rustem, B., & Saule, N. (2020). Development of an automated system model of information protection in the cross-border exchange. Cogent Engineering, 7(1), 1724597.

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

[6] Minssen, T., Seitz, C., Aboy, M., & Compagnucci, M. C. (2020). The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?. EPLR, 4, 34.

[7] Coetzee, J. (2024). Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013-Part II: The Data Transfer Provision. Potchefstroom Electronic Law Journal (PELJ), 27(1), 1-29.

[8] Vavoula, N. (2020). The 'puzzle'of EU large-scale information systems for third-country nationals: Surveillance of movement and its challenges for privacy and personal data protection. European law review.

[9] Tian, G. Y. (2016). Current issues of cross-border personal data protection in the context of cloud computing and trans-Pacific partnership agreement: join or withdraw. Wis. Int'l LJ, 34, 367.

[10] Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. Journal of Digital Technologies and Law, 2(2), 286-307.

[11] Weiwei, Z. (2020). RESEARCH ON THE MAJOR ISSUES OF DATA FLOW AND INFORMATION PRIVACY PROTECTION: A GLOBAL WATCH FROM A CHINESE PERSPECTIVE: COMPARATIVE STUDY ON THE LEGAL REGULATION OF A CROSS-BORDER FLOW OF PERSONAL DATA AND ITS INSPIRATION TO CHINA. Frontiers of Law in China, 15(3), 280-313.

[12] LeSieur, F. (2012). Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy. Int'l Data Priv. L., 2, 93.

[13] Guamán, D. S., Del Alamo, J. M., & Caiza, J. C. (2021). GDPR compliance assessment for cross-border personal data transfers in android apps. IEEE Access, 9, 15961-15982.

[14] Singh, S. (2024). Regulation of Cross-Border Data Flow and Its Privacy in the Digital Era. NUJS J. Regul. Stud., 9, 38.

[15] Bakhteev, D. V., Sosnovikova, A. M., & Kazenas, E. V. (2024). Overcoming Illegal Cross-border Transfer of Personal Data. Journal of Digital Technologies and Law, 2(4), 943-972.

[16] Guo, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation?. Computer Law & Security Review, 56, 106079.

[17] Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the US and China. Computer Law & Security Review, 43, 105610.

[18] Lee, I., & Keh, J. S. (2017). Cross-Border Transfers of Personal Data and Practical Implications. J. Korean L., 17, 33.

[19] Vavoula, N. (2020). Interoperability of EU information systems: The deathblow to the rights to privacy and personal data protection of third-country nationals?. European public law, 26(1).

[20] Chen, Y., & Song, L. (2018). China: concurring regulation of cross-border genomic data sharing for statist control and individual protection. Human Genetics, 137(8), 605-615.

[21] Zheng, W. (2020). Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China. Frontiers L. China, 15, 280.

[22] Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law, 26(3), 213-228.

[23] Ziyi, X. (2022). International Law Protection of Cross‐Border Transmission of Personal Information Based on Cloud Computing and Big Data. Mobile Information Systems, 2022(1), 9672693.

[24] Malahleka, M. (2024). The Problem of Trans-Border Information Flows in the Protection of Personal Information. Potchefstroom Electronic Law Journal (PELJ), 27(1), 1-40.

[25] Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A. (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. Computer law & security review, 34(3), 582-594.

[26] Chen, M. (2024). Developing China's Approaches to Regulate Cross-border Data Transfer: Relaxation and Integration. Computer Law & Security Review, 54, 105997.

[27] Fucai Zhou,Jintong Sun,Qiang Wang,Yun Zhang,Ruiwei Hou & Chongyang Wang. (2025). Efficient private information retrievals for single-server based on verifiable homomorphic encryption. Computer Standards & Interfaces103961-103961.

[28] Tianyu Zhang. (2024). Intellectual Property Protection Issues and Solutions in Cross-Border Big Data Streams. Applied Mathematics and Nonlinear Sciences(1).

[29] Ka'ulawena Alipio,Javier García Colón,Nima Boscarino & Keolu Fox. (2025). Indigenous Data Sovereignty, Circular Systems, and Solarpunk Solutions for a Sustainable Future. Pacific Symposium on Biocomputing. Pacific Symposium on Biocomputing717-733.

[30] Minoo Kamrani & Erika Hausenblas. (2025). An adaptive positive preserving numerical scheme based on splitting method for the solution of the CIR model. Mathematics and Computers in Simulation673-689.