ISSN 2616-5775 Vol. 8, Issue 11: 32-37, DOI: 10.25236/AJCIS.2025.081104

Research on the Trade-off Mechanism between Data Factor Marketization and Privacy Security in the Artificial Intelligence Era

Haojie Sun[1,a], Xiaodong Tang[1,b,*]

[1]*Hubei University of Automotive Technology, Shiyan, China*
[a]*haojiesun57@gmail.com*, [b]*xiaodongtang@huat.edu.cn*
**Corresponding author*

Abstract: *In the era of artificial intelligence, data factor marketization is an inevitable trend in the development of the digital economy, while privacy security risks are its core challenges. Focusing on the contradiction, this paper systematically analyses the connotative characteristics of data factor marketization and the multi-dimensional value of privacy security. Combined with the explosive growth of the global data market, it diagnoses the prominent privacy security issues from three aspects: technology, legal regulation, and social ethics. The study proposes a technology-law-market trinity trade-off mechanism: in terms of technical methods, it relies on homomorphic encryption, multi-party secure computation, and other technologies to achieve the usable but invisible effect; in terms of legal regulation, it improves the ownership definition and dynamic revision mechanism, and strengthens coordinated supervision and law enforcement deterrence; in the market dimension, it constructs flexible constraints through transaction norms, quality standards, and industry self-regulation. This mechanism provides a solution for balancing the release of data factor value and the protection of privacy security, facilitates the coordinated development of the digital economy, and offers references for interdisciplinary research, policy formulation, and enterprise practice.*

Keywords: *Artificial Intelligence, Data Factor Marketization, Privacy Security*

1. Introduction

Artificial intelligence is driving global digital transformation. As a core production factor, data marketization is an inevitable trend in the development of the digital economy [1]. Massive amounts of data lay the foundation for AI model training, but privacy security risks in circulation have become increasingly prominent, presenting a dialectical relationship of coexistence-conflict [2]. Data leakage incidents such as those of Facebook and Equifax highlight the urgency of balancing data marketization and privacy security, making the construction of a scientific trade-off mechanism a core proposition [3]. However, recent research focuses solely on technical paths (such as differential privacy parameter optimization) or legal paths (such as GDPR compliance cost estimation), lacking a dynamic coupling system interpretation framework of value release risk regulation, and lacking cross domain integration solutions that can be directly embedded in transaction processes, leading to extreme dilemmas in practice of heavy circulation while light security or heavy security while light circulation.

Technological innovation and policy regulation provide dual support for data marketization. Cloud computing, big data, and blockchain technologies have built a closed loop of storage-processing-circulation, promoting the transformation of data from raw resources to tradable assets. While, policies such as the EU's GDPR and China's Opinions on the Market-oriented Allocation of Factors of Production regulate the development of marketization, they also show differences in governance logics. However, the technological path and institutional path have not yet formed a coupling interface, and there is an urgent need for an integrated mechanism that is compatible with multiple governance logics and dynamically responds to risk and return.

This study focuses on the core contradiction between data factor marketization and privacy security, analyzes the coexistence-conflict relationship and influencing mechanisms, diagnoses challenges in technology, legal regulation, and social ethics, and ultimately constructs a technology-law-market trinity trade-off mechanism with adaptive strategies. The main contributions are as follows: (1) Propose a unified framework of coexistence conflict to break the perspective of separating data circulation from

ISSN 2616-5775 Vol. 8, Issue 11: 32-37, DOI: 10.25236/AJCIS.2025.081104

privacy security; (2) Create a complete mechanism of technology law market that can be directly embedded into the transaction process and implemented; (3) Cover the entire cycle and cross-border scenarios, providing practical reference strategies for balancing high circulation and strong security.

2. Data Factor Marketization and Privacy Security

2.1. Connotation and Characteristics of Data Factor Marketization

T Data factor marketization is a process of realizing efficient resource allocation through the entire chain of right confirmation, pricing, transaction, supervision, with the core being the completion of the value transformation from resource-asset-capital [4]. This process needs to resolve three major contradictions: the conflict between ambiguous ownership and the clarity of transaction needs, the imbalance between uncertain value evaluation and stable pricing, and the tension between circulation efficiency and security prevention and control.

The unique attributes of data exacerbate the above contradictions: non-rivalry and replicability break through scarcity constraints; value presents differentiation depending on algorithms and scenarios; timeliness and cumulativeness overlap to form trend mining value; the scale effect of near-zero marginal replication cost synchronously amplifies value release and risk diffusion.

2.2. Concept Definition and Multi-dimensional Value of Privacy Security

Privacy security are the basic guarantees for data marketization, with value spanning three dimensions: individual, enterprise, and society. At the individual level, there is a risk of rights infringement such as identity theft; at the enterprise level, security incidents will trigger trust crises and economic losses, such as the chain impact of Facebook's data leakage incident; at the social level, behaviors such as big data price discrimination undermine fairness and erode the trust foundation of the digital economy.

In the AI era, the connotation of privacy security has expanded to the entire lifecycle management and algorithmic supervision, covering the compliance of the entire process of collection-storage-use-destruction, and further extending to new areas such as algorithms, scenarios, and derivative privacy [5]. For example, the unauthorized use of wearable device data for insurance underwriting constitutes derivative privacy infringement.

2.3. Dialectical Relationship between Data Factor Marketization and Privacy Security

The two present a dialectical relationship of coexistence and mutual promotion-opposition and conflict. The symbiosis is reflected in the fact that security is the premise of marketization, which is confirmed by the fact that desensitized data transactions accounted for 83% of domestic data exchange transactions in 2024; marketization feeds back security by sharing protection costs and standardizing circulation standards through unified platforms [6]. The conflict is manifested in: increased risks due to flow and sharing, multiplied risks in cross-border transmission due to regulatory differences, and excessive collection easily caused by the massive data demand for AI training.

3. Current Situation and Challenges in the Artificial Intelligence Era

3.1. Current Situation of Data Factor Marketization

3.1.1. Market Scale and Trends

The data market shows an explosive growth trend. According to IDC data, global big data IT investment reached 354 billion US dollars in 2024 and is expected to increase to 644.1 billion US dollars by 2028 (a compound annual growth rate of 16.8%); the Chinese market leads the world in growth rate, with expenditures of 33.75 billion US dollars in 2024 and an expected 62.17 billion US dollars by 2028 (a compound annual growth rate of 24.9%). Domestic data transaction volume has also climbed synchronously, exceeding 160 billion yuan in 2024, a year-on-year increase of over 30%, among which the on-exchange transaction volume doubled (International Data Corporation, 2024).

The market ecosystem is continuously improving. Trading platforms represented by the Shanghai and Shenzhen Data Exchanges provide full-process services including registration, transaction, and settlement, promoting the expansion of transaction types from structured to semi/unstructured data, with

ISSN 2616-5775 Vol. 8, Issue 11: 32-37, DOI: 10.25236/AJCIS.2025.081104

strong supply and demand for AI training data such as images and videos. The business model has transformed from single sales to diversified innovations such as sharing and leasing. Ecological roles such as data brokers and compliance service providers have emerged, forming a complete chain of supply-demand matching-compliance guarantee-value transformation. Among them, the leasing model reduces the data acquisition cost for small and medium-sized enterprises, the sharing alliance realizes resource complementarity, and the increased proportion of unstructured data transactions accurately meets the needs of AI training [7].

3.1.2. Analysis of Main Models

Data opening focuses on public data. Provincial-level open platforms provide free datasets and interfaces to support scenario innovation such as intelligent transportation and precision agriculture, but there are problems such as low enterprise participation and restricted opening of sensitive data. Data sharing is demonstrated in the government affairs field, where cross-departmental data collaboration improves administrative efficiency; inter-enterprise sharing is limited by security concerns and only exists locally in cooperative scenarios such as supply chains, such as automobile manufacturers sharing production data with suppliers to optimize quality control [3].

Data transaction is the core channel of marketization, divided into point-to-point and on-exchange transactions. Point-to-point transactions are of considerable scale, with large banks' annual purchases exceeding 10 billion yuan, forming stable transaction scenarios such as financial risk control data and processed data products; on-exchange transactions reduce information asymmetry through rule-making. Platforms such as Shanghai Data Exchange promote the formation of price mechanisms, attract diverse participants, drive the development of supporting services such as compliance evaluation and data brokerage, and help the market transform from spontaneous circulation to standardized operation [7].

3.2. Challenges Facing Privacy Security

3.2.1. Technical Hidden Dangers

Technical risks run through the entire data lifecycle: in the training link, the risk of leakage of non-desensitized data or model inversion attacks is prominent. Research proves that gradient inversion can restore sensitive training data with an accuracy of 85% [8]; in the storage link, vulnerabilities in distributed systems are prone to attacks. In 2023, a cloud storage vulnerability of Marriott Hotels led to the leakage of information of 33 million guests; in the transmission link, man-in-the-middle attacks and cross-border regulatory differences exacerbate risks. In 2024, 41% of global cross-border data leaks originated from conflicts in regulatory rules. In addition, data abuse such as over-collection and third-party resale occurs frequently. Some platforms excessively demand permissions, infringing on users' right to know and control, forming dual pressures of technical protection and compliance control [5].

3.2.2. Legal and Regulatory Dilemmas

The legal system has three core shortcomings: first, cross-border regulatory conflicts. The conflicting power definitions between GDPR and the US Cloud Act have increased enterprises' compliance costs by 37%; second, ambiguous ownership definition. Disputes over the distribution of rights and interests of user-generated data and derivative data occur frequently, which was highlighted by data ownership lawsuits on social platforms in 2023; third, technical lag. New technologies such as generative AI lack clear regulations [9].

The regulatory level faces multiple challenges: overlapping powers and responsibilities of multiple departments lead to buck-passing or duplicate supervision; backward monitoring technology makes it difficult to identify new AI-driven attacks; insufficient punishment intensity makes the cost of violations lower than the benefits, failing to form effective deterrence. Law enforcement personnel's professional quality and technical tool adaptability are insufficient, and traditional regulatory methods cannot cope with AI-based risks. There is an urgent need to build a regulatory system of dynamic legislation-technical empowerment-precise law enforcement.

3.2.3. Social and Ethical Considerations

Privacy violations seriously impact the social trust foundation. Data leakage incidents lead to a decline in public confidence in digital services and reduce users' willingness to provide data, directly hindering the process of data marketization. Issues such as big data price discrimination and algorithmic bias highlight ethical risks. The former undermines fair market competition, while the latter exacerbates social discrimination in scenarios such as recruitment and loans, violating the principle of personality

ISSN 2616-5775 Vol. 8, Issue 11: 32-37, DOI: 10.25236/AJCIS.2025.081104

rights protection. The leakage of sensitive information such as medical and whereabouts not only causes direct damages such as financial fraud and identity theft but also may lead to hidden harms such as discriminatory treatment, forming an unbalanced pattern of technological innovation-rights protection-ethical constraints.

4. Construction and Strategies of the Trade-off Mechanism

4.1. Technical Strategies

4.1.1. Application of Encryption Technologies

Homomorphic encryption achieves the usable but invisible effect through encrypted computation [10]. Optimized solutions have broken through efficiency bottlenecks, enabling credit evaluation in encrypted state in financial risk control scenarios, with processing speed 3 times faster than traditional solutions; quantum computing technology is expected to further increase the speed of large-scale data processing by more than 10 times. Multi-party Secure Computation (MPC) is based on the Millionaire's Problem theory and supports distributed collaborative computing. Multiple hospitals in the medical field jointly train diagnostic models through MPC, improving model performance without disclosing original medical records. This technology has been applied on a large scale in government affairs and financial fields.

4.1.2. Anonymization and Differential Privacy Technologies

Anonymization obscure identity information through de-identification but has the risk of re-identification through association, requiring collaboration with other technologies. Differential privacy balances security and usability through noise injection. The optimized ε-adaptive mechanism can accurately match scenario needs: the 2020 US Census adopted this technology to control information error within 1.5%, and Google combined it with federated learning to maintain the accuracy of recommendation systems above 95%, adapting to high-sensitivity scenarios.

4.2. Legal and Regulatory Strategies

4.2.1. Improving the Legal and Regulatory System

Taking the risk-oriented approach of GDPR and the classified and hierarchical protection of China's Data Security Law as the basic framework, the data leakage rate of pilot enterprises has dropped by 45%. Three aspects need to be focused on improving: refining the hierarchical ownership rules for original and derivative data; establishing a dynamic legal revision mechanism to respond to technological iterations; formulating cross-border white lists to simplify the circulation process of low-risk data.

4.2.2. Strengthening Supervision and Law Enforcement

Clarify the powers and responsibilities of departments such as cyberspace administration, industry and information technology, and finance by field, and establish a coordinated supervision mechanism; deploy AI monitoring systems to conduct real-time risk early warning and improve the professional quality of law enforcement personnel. Increase punishment intensity to form deterrence: raise fines, pursue criminal liability for major leakage incidents and impose market entry bans; establish a double random inspection system, and force enterprises to fulfill their main responsibilities through regular supervision.

4.3. Market and Industry Self-regulation Strategies

4.3.1. Establishing Data Transaction Norms and Standards

Formulate full-process transaction rules: verify the legality of data sources and subject qualifications, standardize transaction contracts to clarify the scope of use and security responsibilities; establish quality standards centered on accuracy, completeness, and timeliness to adapt to differentiated scenario needs, such as, financial data focuses on accuracy, and traffic data focuses on timeliness, ensure transaction efficiency through third-party evaluation and certification.

4.3.2. Role of Industry Self-regulation Organizations

Industry associations formulate self-regulation guidelines, requiring enterprises to follow the principles of legality, legitimacy, and necessity; conduct regular evaluations to assess the soundness of systems and the implementation of measures through a combination of questionnaires and on-site

ISSN 2616-5775 Vol. 8, Issue 11: 32-37, DOI: 10.25236/AJCIS.2025.081104

inspections; establish a red and black list system and share information with regulatory authorities, commend compliant benchmarks, and urge rectification of problems, forming a coordinated pattern of self-regulation as well as supervision.

5. Conclusions and Prospects

5.1. Research Conclusions

The study clarifies that data factor marketization and privacy security present a dialectical relationship of coexistence-conflict: security is the prerequisite guarantee for marketization, and marketization feeds back the improvement of security capabilities. The core contradiction between the two can be resolved through the technology-law-market trinity mechanism. Technically, homomorphic encryption and MPC achieve the usable but invisible effect, while anonymization and differential privacy balance security and usability, providing underlying support; in terms of legal regulation, based on GDPR and the Data Security Law, improve the ownership definition and dynamic revision mechanism, and strengthen regulatory coordination and punishment intensity to form rigid constraints; in the market self-regulation dimension, transaction norms and quality standards regulate circulation order, and industry associations guide enterprises to comply with regulations to form flexible constraints.

5.2. Future Prospects

Future efforts should focus on technological innovation and global coordination. Technically, promote the integration of quantum encryption, blockchain, and AI: quantum encryption strengthens transmission security, blockchain ensures trusted storage, and AI realizes real-time risk early warning. At the global level, promote the implementation of cross-border governance mechanisms, build diverse governance rules, and strengthen technological R&D and law enforcement cooperation to break down cross-border flow barriers. International cooperation is a key direction. It is necessary to promote the establishment of global coordinated data privacy protection rules, and jointly address cross-border data security challenges by participating in the formulation of governance rules, technological R&D cooperation, experience exchange, and law enforcement linkage. In summary, through the coordinated improvement of the trade-off mechanism by technology, law, and the market, the coordinated development of data factor marketization and privacy security can be achieved.

Acknowledgements

This study is supported by the Doctoral Research Initiation Fund Project of Hubei University of Automotive Technology (BK202440), the Ministry of Education University-Industry Collaborative Education Program (250600116245053).

References

[1] Reimers K, Guo X. Reconciling the Conflicting Goals of Privacy Protection and Competition Policy Through Making Platform Use Data Saleable—An Institutional Perspective on Data Markets[J]. Journal of Electronic Business & Digital Economics, 2024, 3(3): 222-235.
[2] Siddiqui M A. A Comprehensive Review of AI: Ethical Frameworks, Challenges, and Development[J]. Adhyayan: A Journal of Management Sciences, 2024, 14(1): 68-75.
[3] Xu J, Hong N, Xu Z, et al. Data-Driven Learning for Data Rights, Data Pricing, and Privacy Computing[J]. Engineering, 2023, 25: 66-76.
[4] Wang D, Liao H, Liu A, et al. Natural resource saving effects of data factor marketization: Implications for green recovery[J]. Resources Policy, 2023, 85(A): 104019.
[5] Yeung K. Algorithmic regulation, A critical interrogation[J]. Regulation & governance, 2018, 12(4): 505-523.
[6] Abbas A E, van Velzen T, Ofe H, et al. Beyond Control Over Data: Conceptualizing Data Sovereignty from a Social Contract Perspective[J]. Electronic Markets, 2024, 34(1): 20.
[7] Yang Q, Liu Y, Chen T, et al. Federated Machine Learning: Concept and Applications[J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19.
[8] Aaronson S A. Data Is Different, and That's Why the World Needs a New Approach to Governing Cross-Border Data Flows[J]. Digital Policy, Regulation and Governance, 2019, 21(5): 441-460.

ISSN 2616-5775 Vol. 8, Issue 11: 32-37, DOI: 10.25236/AJCIS.2025.081104

[9] Hawes D. The Brussels Effect: How the European Union Rules the World[J]. Journal of Contemporary European Studies, 2020, 29(1): 145.
[10] Ullah S, Li J, Chen J, et al. Department of Mathematics, University of Management and Technology, Lahore, Pakistan Homomorphic Encryption Applications for IoT and Light-Weighted Environments: A Review[J]. IEEE Internet of Things Journal, 2025, 12(2): 1222-1246.