Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.35129

Research on Infringement of Personal Information in Cross-border Flow of AI Financial Data — From the Perspective of Platform Liability

Shitao Li

Law School, University ofInternational Relations, Beijing, China
947447633@qq.com

Abstract. With the development of generative artificial intelligence, cloud computing and the platform economy, the scale of cross-border flow of financial data is continuously expanding. In AI financial applications, the processing of personal information is characterized by automation, continuity and concealment, which may render traditional personal information protection methods ineffective. The dominant position of platforms in data collection, algorithm training and cross-border transmission has gradually transformed them from traditional technical intermediaries into important subjects of risk control and rule-making. China has now formed a data governance model centered on the *Personal Information Protection Law*, the *Data Security Law* and the *Cybersecurity Law*, but there is still a lack of effective institutional responses to the issue of platform liability in the cross-border flow of AI financial data. From the perspective of platform liability, this paper analyzes the types of personal information infringement, the logic of platform liability, the current regulatory dilemmas and the paths for institutional improvement in the cross-border flow of AI financial data, and proposes a platform governance model with Chinese characteristics on the basis of drawing on foreign institutional experience.

Keywords: Artificial Intelligence, Financial Data, Cross-border Data Flow, Personal Information Protection, Platform Liability

1. Introduction

In recent years, the application of artificial intelligence technology in the financial field has been continuously increasing. Banks, securities, insurance and internet financial platforms widely use algorithmic models for intelligent credit granting, risk prediction, precision marketing and anti-fraud identification. During this period, the scale of data cross-border flow in financial activities has been expanding continuously. Cross-border payments, international credit investigation, global asset allocation and cloud-based financial services all rely heavily on cross-border data transmission. With the accelerated development of digital finance, the security issue of cross-border flow of personal financial information has gradually become an important topic in data governance.

In traditional financial activities, data flow has relatively clear geographical and regulatory boundaries. In AI financial scenarios, data processing is characterized by decentralization and

DOI: 10.54254/2753-7048/2026.35129

platformization. Platforms can continuously collect user data through algorithms and expand the scope of data processing using machine learning technologies. Under the current situation, personal information infringement not only includes traditional data leakage, but also gradually evolves into overall risks such as algorithmic discrimination, imbalance in automated decision-making, expansion of platform control and failure of cross-border supervision.

China has now formed a data governance model centered on the *Personal Information Protection Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China* and the *Cybersecurity Law of the People's Republic of China*, and has strengthened the supervision of cross-border data through systems such as data exit security assessment and standard contract filing. However, the current system still follows the traditional notice-and-consent model and does not pay sufficient attention to the liability structure of platforms in the cross-border flow of AI financial data. Especially on issues such as algorithmic black boxes, platform monopoly and cross-border data collaboration, existing rules are still difficult to respond effectively.

Foreign scholars began to study cross-border data flow and platform liability at an earlier stage. The EU's *General Data Protection Regulation (GDPR)* attaches importance to the liability of data controllers and establishes a risk-based regulatory model, while the United States focuses more on industry autonomy and market regulation. Countries such as Japan and Singapore emphasize the balance between free cross-border data flow and security protection. China's analysis of platform liability for cross-border flow of AI financial data is still in the development process, and the discussion on the relationship between the sensitivity of financial data and the logic of platform governance is not sufficient.

From the perspective of platform liability, this paper conducts an overall analysis of personal information protection issues in the cross-border flow of AI financial data, and puts forward suggestions for institutional improvement in combination with the actual situation of China's digital finance development.

2. Typological sorting of personal information infringement issues in cross-border flow of AI financial data

2.1. Infringement of information autonomy caused by over-collection and concealed processing

The normal operation of AI financial platforms requires the continuous supply of massive amounts of data. Traditional financial institutions generally only use identity authentication information, account information and transaction records. To improve the predictive ability and commercial value of algorithmic models, AI financial platforms collect users' full life cycle data and conduct dynamic analysis. In addition to collecting personal information actively provided by users, platforms also obtain a large amount of derivative data through technical means such as device fingerprinting, location tracking, browsing history analysis, consumption behavior monitoring and associated account matching, and form more detailed user profiles through data cleaning, data mining and algorithm training. In this process, the scope of personal information collection has exceeded the necessary limit required by traditional financial services, and has gradually expanded to behavioral information, preference information and predictive information [1].

Especially in the context of cross-border data flow, platforms often send personal financial information to overseas servers, cloud computing centers or affiliated enterprises for storage and processing to meet the needs of global data allocation. The cross-border data processing chain involves multiple subjects and multiple jurisdictions, and it is usually difficult for personal information subjects to accurately understand the data circulation path, actual purpose and the

DOI: 10.54254/2753-7048/2026.35129

situation of overseas recipients. Platforms generally fulfill their notification obligations through privacy policies and user agreements, but the relevant clauses often contain a large number of professional terms, are too long, and have an overly broad authorization scope, making it difficult for users to make true and effective expressions of intention under limited cognitive ability [2]. In practical applications, clicking "agree" is more regarded as a necessary prerequisite for using financial services, rather than a real choice of users to handle their personal information.

Legally speaking, the modern personal information protection system is based on the theory of individual self-determination, and individuals have the right to decide whether their information is collected, how it is used and to whom it is disclosed [3]. This institutional design has two main premises: first, individuals can fully understand the specific content of information processing activities; second, individuals have the ability to make rational judgments and independent choices. However, in AI financial scenarios, these premises are gradually being eliminated by technological reality. The high complexity of algorithmic models and the relatively concealed data processing chain make it difficult for users to fully understand the information processing situation. On the other hand, platforms have formed a de facto dominant position relying on technological, data and market advantages, and users usually have no opportunity to negotiate equally with platforms [4].

More importantly, the advancement of artificial intelligence technology has gradually shifted the value of data from single data to data association and data inference. Platforms not only use users' existing information to provide services, but also use machine learning technology to calculate users' credit levels, consumption levels, investment tendencies and future behavioral trends. The data inferred by algorithms is not actively provided by users, but it will have a substantial impact on users' personal and property interests. Therefore, the traditional "notice-and-consent" approach is difficult to effectively control data processing activities, and the right to self-determination of personal information is changing from a substantive right to a formal right [5].

In essence, the risks arising from over-collection and concealed processing are manifested in the compression of personal privacy space, and also reflect the obvious changes in the information power structure in the digital age. The ability to control data is continuously concentrating on platforms, and the information power relationship between individuals and platforms shows a significant imbalance. Personal information protection is gradually shifting from an individual control model to a platform governance model, and the requirement for this institutional transformation has become increasingly prominent.

2.2. Infringement of personality interests caused by algorithmic profiling and automated decision-making

In AI financial application scenarios, algorithmic profiling has become the main tool for financial platforms to carry out risk control and commercial decision-making. Algorithmic profiling refers to a data labeling model in which platforms integrate, classify and predict personal information using technologies such as machine learning, big data analysis and user behavior modeling to reflect users' characteristics, preferences and risk status [6]. Financial platforms generally use various data such as users' transaction records, consumption habits, search behaviors, social relationships, geographic locations and device information to conduct credit evaluation and risk identification for users, and widely apply the relevant results to financial service fields such as loan approval, insurance pricing, investment recommendation and precision marketing. With the development of artificial intelligence technology, algorithmic profiling has gradually transformed from traditional static classification to dynamic prediction, which can reflect users' existing behaviors and make probabilistic inferences about their future behaviors.

DOI: 10.54254/2753-7048/2026.35129

However, the formation process of algorithmic profiling involves high complexity and concealment. Ordinary users usually cannot understand the way platforms collect data, the process of building models and the process of forming final decision results, which are usually contained in the "algorithmic black box". Although users have become data producers, it is difficult for them to know how their data is processed and used, and it is also difficult for them to participate in the algorithmic decision-making process [7]. Platforms generally refuse to disclose algorithmic logic on the grounds of protecting trade secrets, and users can only see the final decision results and cannot judge whether the relevant decisions are based on true and accurate data. This information asymmetry makes it difficult for individuals to supervise algorithmic decisions, and also makes it difficult for their right to correction and right to objection to be fully realized.

The development of artificial intelligence technology has allowed platforms to gradually get rid of traditional data collection models and instead rely on data association and behavioral inference to form so-called "invisible profiling". Invisible profiling refers to platforms deriving potential characteristics such as users' income levels, occupational status, risk preferences, health status and even political tendencies by analyzing users' behavior trajectories, consumption habits, social relationships and online activities, rather than directly using information provided by users for judgment [8]. Such inferred information is not actively disclosed by users, but it will affect the opportunities for financial services. The continuous enhancement of platforms' data association capabilities has made individuals gradually become subjects who are predicted, analyzed and evaluated, which has further intensified the trend of data power concentrating on platforms.

The risks brought by algorithmic profiling are not only manifested in the expansion of data control capabilities, but also lead to algorithmic bias and algorithmic discrimination. Algorithmic models mainly rely on historical data for training, and historical data contains existing prejudices and structural discrimination, so algorithmic decisions will show a "bias inheritance effect" [9]. For example, if a certain region, occupational group or consumer group is given a higher risk label in historical data, the algorithmic model will automatically strengthen this judgment logic, putting relevant groups at a disadvantage in the process of loan approval, insurance underwriting and credit rating. Although platforms do not subjectively discriminate, algorithms can cause actual differential treatment through data screening and model training.

In financial practice, algorithmic discrimination is mainly manifested as differential pricing and differentiated services. For example, for users with strong consumption capacity and high willingness to pay, platforms can provide higher product quotations through algorithmic analysis. For users judged to be high-risk groups, banks may raise loan interest rates, reduce credit lines, or even refuse to provide financial services [10]. Some users may also be included in the high-risk list due to algorithmic errors, thus losing the qualification to obtain normal financial services. Due to the lack of transparency in algorithmic decisions, users usually do not understand the reasons for the relevant results, and it is not easy to protect their rights through traditional legal remedies.

Legally speaking, the damage caused by algorithmic profiling has exceeded the scope of traditional property interest infringement and has begun to involve the field of personality right protection. Algorithmic labels may have a negative impact on individuals' social evaluation and damage human dignity. Secondly, algorithmic discrimination will cause unequal treatment of different subjects in obtaining financial resources and damage the value of equality stipulated in the Constitution. Platforms using algorithmic models to predict and intervene in individuals' future behaviors will fundamentally affect the autonomous development of personality [11]. In this sense, personal information is no longer just a usable data resource, but has gradually become the main carrier of personality interests.

DOI: 10.54254/2753-7048/2026.35129

Therefore, the issue of algorithmic profiling in AI financial scenarios is not only a technical issue, but also a new challenge faced by personality right protection in the digital age. After platforms gradually obtain the right to credit evaluation, risk identification and resource allocation, algorithms have actually become the main governance method affecting individuals' financial opportunities and social evaluation. Preventing the transformation of algorithmic power, avoiding algorithmic discrimination, and ensuring individuals' rights to participate and obtain remedies in automated decision-making are important issues that the personal information protection system needs to address [12].

3. Current platform liability for cross-border flow of AI data — the internal connection with personal information protection

3.1. Jurisprudential basis of platform liability

The emergence of platform liability is closely related to the platform-based structure in the era of digital economy. Traditional internet platforms mainly undertake the function of information intermediaries, and their legal obligations revolve around the "notice-and-takedown" rule and content review, with clear and relatively passive liability boundaries [13]. However, the development of AI financial platforms has completely changed this situation. Such platforms not only collect a large amount of user data, but also participate in the allocation of financial resources using deep learning models, credit scoring algorithms and automated decision-making systems, and have gradually evolved into the main participants in data control and risk diffusion [14]. Platforms determine the scope of data collection, including biometric information, transaction behavior trajectories and social network association data, master the algorithm operation logic involving feature weights and model iteration strategies, and control cross-border transmission paths, such as transmitting user data to overseas servers for joint modeling. Therefore, these platforms have substantial control over data risks [15].

According to the risk society theory, the risks arising in modern society mainly come from technological expansion and system operation. Ulrich Beck believes that when industrial society transforms into a risk society, technical decision-makers create organized irresponsibility in the process of creating wealth, and risk distribution often evades the traditional liability attribution model [16]. While AI financial platforms use algorithmic technology to generate data value, they also create new personal information risks, including unfair credit granting caused by algorithmic discrimination, insufficient right to know caused by model black boxes, the dilemma of the right to be forgotten caused by data aggregation, and sovereign regulatory conflicts arising from cross-border transmission [17]. These risks are characterized by man-made uncertainty. Individual users cannot fully bear all responsibilities due to information asymmetry and differences in negotiation status, and ex post judicial remedies are difficult to implement due to complex causal relationships and delayed damage. As the main shapers of risks, platforms should bear corresponding governance responsibilities, including risk prevention in advance, transparent explanation during the process and damage remedy afterwards [18].

According to the data controller theory, platforms have the power to process and distribute data, so their assumption of liability is justified. The EU *General Data Protection Regulation (GDPR)* defines a controller as a natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data, and imposes a series of responsibilities on it, such as adopting compliance measures, conducting data protection impact assessments and responding to data subjects' rights requests [19]. AI financial platforms not only decide what to

DOI: 10.54254/2753-7048/2026.35129

process and why to process, such as assessing credit risks by building user profiles, but also decide how to process, such as selecting specific feature engineering and model architectures, which fully meets the substantive standard of data controllers [20]. Platforms can exercise exclusive control over algorithmic power throughout the algorithmic decision-making process, including the labeling specifications of training data and the threshold setting in the inference stage, which constitutes a situation where algorithmic power is exercised by private subjects. If power is not matched with corresponding responsibilities, it will easily become a liability-evading technological governance, that is, platforms transfer risks to users or the public through technical black boxes and information advantages [21]. Therefore, identifying platforms as data controllers is an inevitable result of legal logic and a requirement for realizing distributive justice in the digital society [22].

3.2. Functions of platform liability in personal information protection

Platform liability mainly has the function of risk prevention. Platforms can reduce the probability of risks before data exits by classifying and grading data, conducting risk assessments and security reviews. Platforms should formulate differentiated access control and encryption standards according to the sensitivity level of data, such as personal financial information, biometric features and credit behavior trajectories, to prevent unauthorized flow of high-risk data [23]. Risk assessment is an overall review of the scale, scope, purpose of the data to be exited and the data security capability of the recipient, mainly to identify potential secondary sharing or data fusion risks [24]. Security review will conduct real-time monitoring of cross-border transmission channels, including API interfaces and cross-border dedicated lines, and issue alarms for abnormal behaviors. This series of ex ante measures can advance risk control from ex post accountability to source suppression, which is in line with the modern governance logic that prevention is better than remedy [25].

Platform liability also has the function of right protection. Platforms should fulfill their obligations of transparency and explanation, which can protect users' right to know and right to choose. The transparency obligation requires platforms to explain the purpose of data collection, the logic mode of algorithmic decision-making and the recipients of cross-border transmission to users in a clear, concise and dynamic way, so that users can understand how their personal information is processed and where it flows [26]. When platforms make automated decisions such as rejecting credit scores or reducing credit lines that have a significant impact on users, they should provide specific and practical decision-making basis, rather than just outputting abstract risk scores [27]. This obligation is particularly important in the financial field, because users are usually in an asymmetric position of algorithmic power and lack the ability to question the reasons for model rejection. By protecting the right to know and the right to choose, platform liability responds to individuals' demand for control over their own information and forms the main element of algorithmic due process [28].

Platform liability also has the function of maintaining order. Between national supervision and market autonomy, platforms can form an intermediate governance structure to stabilize the digital financial order. National supervision, including the Measures for the Security Assessment of Cross-border Financial Data issued by the central bank and the Measures for the Security Assessment of Data Exits issued by the Cyberspace Administration of China, has structural constraints such as limited law enforcement resources and lagging technical responses, making it difficult to directly penetrate massive algorithmic transactions and real-time cross-border data flows. Without effective coordination methods, market autonomy tends to lead to a race to the bottom, and platforms may ignore high-risk processing activities to reduce compliance costs. Platforms have two functions in

DOI: 10.54254/2753-7048/2026.35129

intermediate governance: on the one hand, they connect upwards with regulatory requirements, including submitting security assessment reports and accepting on-site inspections; on the other hand, they restrict the data processing behaviors of users and third-party partners downwards, such as limiting secondary use through contract terms and technical sandboxes. This meta-governance role makes platforms an irreplaceable stabilizer in the digital financial order. It can not only reduce regulatory pressure, but also prevent market failure, and finally form a multi-level risk prevention and control method of public-private partnership model.

4. Deficiencies of the platform regulation model for personal information infringement in cross-border flow of AI data

4.1. Formalization of the personal consent mechanism

The main method of the personal information protection system is the "notice-and-consent" principle, which has long been regarded as an important tool for balancing the rights and obligations of information controllers and information subjects. However, with the application of artificial intelligence in financial service scenarios, the basis for the application of this principle has encountered structural challenges. When applying for financial products such as credit, insurance and wealth management, users often need to deal with complex technical data logic and also cope with the structure of cross-border data flow. Platforms obtain users' general authorization declarations through lengthy and obscure standard form clauses, multi-layered nested authorization pages and pre-checked default consent methods, making consent gradually become a formal compliance process rather than a legal act that truly reflects users' independent will [29].

In the environment of algorithmic automated decision-making, users' autonomy is weakened. Many financial services rely on real-time and dynamic user profiling and behavior scoring in terms of access, pricing and risk control. Although users refuse authorization for certain non-essential data, the system may automatically mark it as a high-risk or incomplete application, which will result in the inability to obtain services or having to accept unfavorable conditions. The all-or-nothing choice structure actually deprives users of the possibility of differentiated authorization, and consent no longer has the premise of freedom and informed consent.

Large-scale fintech platforms usually have both technological advantages and market dominance. These platforms can covertly expand the scope of data collection by means of algorithmic black boxes and dynamic model adjustment. It is difficult for users to find that data is used beyond reasonable expectations, and they cannot exercise the right to withdraw consent. The law grants users the right to refuse automated decision-making, but due to the lack of operable interfaces and transparent explanation methods, this right usually becomes empty talk in practice. Therefore, the notice-and-consent model has gradually lost its role as the main basis for personal information protection in the AI financial environment, and it is necessary to introduce a new legitimacy basis with situational, dynamic and substantive characteristics [30].

4.2. Difficulty in liability identification caused by algorithmic black boxes

AI algorithms are highly complex and closed, which has caused great obstacles to the operation of algorithmic accountability methods. In financial practice, platforms usually regard algorithmic logic, feature weights and model parameters as trade secrets or proprietary technologies, thus refusing to fully disclose the internal working modes of algorithms to the outside world, including regulatory authorities and users. This "black box" state makes it difficult to timely identify and verify potential

DOI: 10.54254/2753-7048/2026.35129

risks such as algorithmic discrimination, unfair pricing or improper denial of service. For example, some credit scoring models may incorporate proxy variables related to race, region or consumption habits, but due to the lack of explainability, users do not even know why they are denied credit, and regulatory authorities cannot conduct effective compliance reviews [31].

The provisions on algorithmic transparency obligations in current legal norms are mainly principled. For example, Article 24 of the *Personal Information Protection Law* stipulates that when an automated decision-making method is used to make a decision that has a significant impact on personal rights and interests, the individual may require the personal information processor to explain it, but this article does not specify the scope, form, time limit and violation consequences. Although the *Regulations on the Management of Algorithmic Recommendation for Internet Information Services* require informing users in an obvious way and providing convenient options to turn off, it does not clearly explain the algorithmic logic, lacks guidance on the understandability of explanations, and also lacks operable methods for handling users' questions and appeals. This principle-based legislative approach often encounters difficulties in concretization when dealing with the rapid changes of technical forms such as deep learning, integrated models and reinforcement learning, leading to the difficulty in implementing algorithmic transparency liability in practice [32].

Moreover, algorithmic infringement is usually characterized by concealment and indirectness. Unlike traditional infringement behaviors, the damage caused by algorithmic decisions usually does not manifest as one-time or visible external behaviors, but mainly exists in the process of processing massive amounts of data and model calculations, and is manifested in the form of probabilistic outputs. Users may only perceive the unfairness of the final result, such as excessively high loan interest rates or excessively low insurance amounts, but it is difficult to trace back to specific algorithmic links. This infringement structure has visible results but invisible processes, making it difficult for users to meet the proof requirement of causal relationship in the constituent elements of tort liability [33].

Users need to prove that there is an adequate "but-for" causal relationship between the operation of the platform's algorithm and the damage they have suffered. However, when algorithmic parameters are dynamically adjusted, model versions are continuously updated, and multiple data sources interact to cause impacts, users cannot know the decision-making logic of the algorithm at a specific time point, and there is no effective means to exclude the impact of other possible factors on the damage result, such as macroeconomic fluctuations and changes in users' own behaviors. In judicial practice, courts often dismiss users' claims on the grounds of "insufficient evidence" due to the lack of operable algorithmic identification methods and provisions on the distribution of burden of proof, making the actual tort liability borne by platforms much lower than the scale of damage they have caused.

The opacity of algorithms, the ruled-based handling of transparency obligations and the difficulty in proving causal relationships form a trilemma encountered in the governance of algorithmic infringement. To solve this problem, the law should introduce more binding algorithmic impact assessments, expand the algorithmic review power of regulatory authorities, and reasonably invert or reduce the burden of proof in certain cases to restore users and technical platforms to an equal position.

DOI: 10.54254/2753-7048/2026.35129

5. Improvement of platform liability paths for personal information protection in cross-border flow of AI data

5.1. Constructing a hierarchical platform liability system

The formation of the future platform liability model requires abandoning a unified compliance approach and instead establishing a differentiated liability structure according to platform scale, data control capability and risk level. This hierarchical governance approach meets the requirements of the principle of proportionality, can improve the efficiency of regulatory resource allocation, and achieve dynamic matching between liability burden and risk control capability [34].

For large platforms that master a large amount of financial data and have overall impacts, stricter and special obligations should be imposed. In terms of data storage, this paper suggests strengthening the localized management of data and controlling the overseas transmission of sensitive financial data to avoid risks to national security and user privacy caused by cross-border access. Secondly, in terms of algorithmic governance, periodic and substantive algorithmic review methods should be introduced, including filing of algorithmic logic, assessment of discriminatory impacts and traceable records of model updates. Furthermore, large platforms also need to conduct more complete cross-border risk assessments in cross-border businesses, including the security guarantee level of data recipients, the stability of the legal environment in third countries and the remedy nature after data exits. This high-intensity liability configuration is mainly because large platforms have obvious advantages in data scale, market influence and technological innovation capability, and these platforms have the ability and should bear higher duty of care and compliance costs [35].

Small and medium-sized fintech start-ups are general technical service platforms or third-party service providers that only provide auxiliary data processing functions, and their main work is to complete basic compliance obligations. These obligations include fulfilling basic notification obligations, ensuring the effective acquisition of user consent, establishing preliminary data security protection measures and responding to users' rights requests. In terms of algorithmic transparency, the mandatory disclosure requirements for proprietary algorithmic logic can be appropriately relaxed, and instead, result-based explainability or ex post appeal mechanisms can be used as alternative compliance standards. Adopting this "focus on the major issues and let go of the minor ones" hierarchical governance approach can reduce the compliance burden and innovation threshold of small and medium-sized enterprises, and also help regulatory authorities concentrate limited resources on the highest-risk areas, thereby improving the overall effect of data governance and algorithmic governance [36].

The differentiated liability structure should also have a dynamic adjustment mechanism. The risk level of a platform will not remain unchanged. When the user scale expands, the sensitivity of data types increases or the business scope extends to cross-border scenarios, the platform needs to apply higher liability standards in a step-by-step manner. If large platforms can effectively reduce the risk level of specific businesses after technological improvement or obtaining third-party certification, they can also apply for relatively simplified compliance procedures in accordance with the law. The dynamic and scenario-based liability stratification reflects the governance philosophy of matching liability with capability, and helps prevent excessive deterrence or regulatory arbitrage [37].

DOI: 10.54254/2753-7048/2026.35129

5.2. Strengthening algorithmic transparency and explainability obligations

Platforms should establish an algorithmic filing and review system and appropriately disclose automated decision-making logic. The main purpose of this system is to solve the information asymmetry problem caused by algorithmic black boxes. Regulatory authorities require platforms to submit basic information such as algorithm design objectives, main characteristic variables, decision-making logic modes and update records, which can realize the traceability and supervision of algorithmic operation logic without substantially disclosing trade secrets. Especially for algorithms used for important financial decisions such as loan approval, insurance pricing and credit rating, since these algorithms are directly related to users' property rights, credit opportunities and risk burdens, it is necessary for the law to further introduce an independent third-party review method. Third-party review institutions can be certified by regulatory authorities, have composite professional capabilities in technology, law and finance, regularly conduct discriminatory impact assessments, fairness tests and model robustness tests on high-risk algorithms, and issue publicly available review reports. This external checks and balances method can solve the problems of insufficient internal compliance motivation and limited regulatory professional resources [38].

The law should clearly grant users the right to refuse purely automated decision-making and allow users to require platforms to provide human review. "Purely automated decision-making" refers to a decision that directly affects users' legal or major interests completely relying on algorithmic output results without any human intervention with substantive discretion. In specific scenarios such as credit approval, premium verification and anti-fraud monitoring, if users have different opinions on the automated output results, they can require the platform to conduct a human review procedure. Reviewers need to be independent of the algorithm development team, have the ability to re-evaluate the facts and evidence of the case, and can revise or overturn the algorithmic conclusion when necessary. This model is not only an extension of procedural justice in the algorithmic era, but also a concrete implementation of the right to algorithmic explanation and the right to oppose automated decision-making in current laws [39].

Algorithms must have explainability, which is the technical condition on which the aforementioned institutional arrangements rely. The explainability obligation requires platforms to use clear, easy-to-understand and non-technical language when explaining the logic, expected consequences and main influencing factors of automated decision-making to users, and shall not use standard form clauses or technical terms for formal explanations. For models that are difficult to explain directly such as deep learning, platforms can use alternative methods such as counterfactual explanation and feature importance ranking to allow users to understand why the decision was made and master how to change inputs to get different results. Research results show that practical explainability will improve users' trust in financial services and promote platforms to actively discover discriminatory features during design, thereby reducing the risk of algorithmic discrimination and unfair decision-making at the source.

The intensity of the explainability obligation should be positively correlated with the importance of the decision and the impact consequences. For low-risk and auxiliary recommendation algorithms, the explanation can be simplified. For the above-mentioned major financial decisions, the highest explainability standard should be applied, and complete explanation records should be kept for subsequent regulatory review and judicial review. Only by integrating algorithmic filing, independent review, refusal of automated decision-making, human review and hierarchical explainability obligations as a whole can a closed loop of algorithmic governance covering the whole process of ex ante, in-process and ex post be formed [40].

DOI: 10.54254/2753-7048/2026.35129

6. Conclusion

The cross-border flow of AI financial data is an obvious trend in the era of digital economy. It promotes financial innovation and improves the efficiency of resource allocation, but also brings new personal information risks. Platforms occupy a dominant position in data collection, algorithm operation and cross-border transmission, and have gradually become the main participants in data governance. At this stage, China's platform liability model still has problems such as insufficient algorithmic governance, imperfect cross-border regulatory collaboration and weak user remedy methods.

In the future, on the premise of ensuring national data security and financial security, China needs to form a hierarchical, transparent and collaborative platform liability model, and promote the establishment of a digital governance approach that takes both security and development into account through the improvement of algorithm management, cross-border cooperation and right remedy methods. Only through effective cooperation between platform liability and national supervision can the overall risks faced by personal information protection in the AI financial era be addressed.

References

[1] Gao, F. P. (2018). Personal Information Protection: From Individual Control to Social Control. Chinese Journal of Law, (3), 84.
[2] Cheng, X. (2022). Understanding and Application of the Personal Information Protection Law. China Legal Publishing House, 112-115.
[3] Zhang, X. B. (2021). Principles of the Personal Information Protection Law. Renmin University of China Press, 36.
[4] Ding, X. D. (2021). The Consent Dilemma in Personal Information Protection and Its Solutions. Journal of Comparative Law, (6), 27.
[5] Zuboff, S. (2019). The Age of Surveillance Capitalism. Public Affairs, 198-205.
[6] Yin, S., & Shi, D. (2024). Algorithm for User Profile Construction on New Media Platforms Driven by Artificial Intelligence. 2024 International Conference on Power, Electrical Engineering, Electronics and Control (PEEEC), 586–591.
[7] Ding, X. D. (2026). Legal Regulation of Digital Power. Journal of Comparative Law, (1), 112.
[8] Gao, F. P. (2021). Personal Information Protection in a Data Society. Law Press, 174.
[9] Xiong, B. W., & Li, Y. Q. (2024). On the Multi-point Parallel Forensics Rules for the Virtual World. Rule of Law Society, (1), 56.
[10] Barocas, S., & Selbst, A. (2016). Big data's disparate impact. California Law Review, 104, 671-732.
[11] Wang, L. M., & Bian, Q. (2025). The Era Expansion of the Personality Right System. Contemporary Law Review, (4).
[12] Zou, C., & Zhang, F. (2022). Algorithm Interpretation Right—The First Step to Algorithmic Governance. Beijing Law Review, 13(02), 227–246.
[13] Civil Code of the People's Republic of China, arts. 1194-1197.
[14] Schrepel, T. (2021). Algorithmic finance and the limits of platform responsibility. Journal of Financial Regulation, 7(2), 211-238.
[15] Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677-739.
[16] Beck, U. (2018). Risk Society: Towards a New Modernity (Trans. He, B. W.). Yilin Press, 45-50.
[17] Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1-33.
[18] Zhang, L. H. (2022). New Trends in Platform Liability: From Safe Harbor to Ex Ante Prevention. Chinese Journal of Law, (3), 105-122.
[19] General Data Protection Regulation, Regulation (EU) 2016/679, arts. 4(7), 24, 32, 35, 22.
[20] Google Spain SL v. Agencia Española de Protección de Datos & Mario Costeja González, Case C-131/12 (EU Court of Justice May 13, 2014).

DOI: 10.54254/2753-7048/2026.35129

[21] Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information (Trans. Zhao, Y. N.). CITIC Press, 178-185.
[22] Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the General Data Protection Regulation. International Data Privacy Law, 7(4), 243-265.
[23] Personal Information Protection Law of the People's Republic of China, art. 51.
[24] European Data Protection Board. (2020). Recommendations 01/2020 on measures that supplement transfer tools.
[25] Data Security Law of the People's Republic of China, arts. 21, 24.
[26] Personal Information Protection Law of the People's Republic of China, art. 17.
[27] Bygrave, L. A. (2020). Automated decision-making and the right to an explanation. International Data Privacy Law, 10(1), 1-4.
[28] Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 141-145.
[29] Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880-1903.
[30] Xu, K. (2021). Algorithmic Governance in the Era of Artificial Intelligence — Paradigm Shift from "Notice-and-Consent" to "Situation-Dynamics". China Law Review, (4), 112-115.
[31] Zheng, Z. H. (2020). Judicial Review of Algorithmic Discrimination — With Reference to the Practice in the U.S. Fintech Field. Chinese Journal of Law, (6), 88-91.
[32] Zhou, H. H. (2021). The Right to Algorithmic Explanation and Personal Information Protection — An Interpretive Theory Centered on Article 24 of the Personal Information Protection Law. Peking University Law Journal, (5), 1172-1175.
[33] Chen, J. H. (2022). Governance by Algorithms: Another Possibility of the Rule of Law. Law and Social Development, (4), 52-54.
[34] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 14 September 2022 on a single market for digital services (Digital Services Act), arts. 31-33.
[35] Wang, Y. (2023). Institutional Logic and Local Construction of Algorithmic Audit. Modern Law Science, (4), 101-104.
[36] Financial Stability Board. (2019). FinTech and market structure in financial services: Market developments and potential financial stability implications (pp. 28-30).
[37] Zhou, H. (2021). Algorithmic Power and Its Regulation. China Social Sciences Press, 215-218.
[38] Personal Information Protection Law of the People's Republic of China, art. 55(1).
[39] Wachter, S. (2020). The right to a human decision. In The Cambridge Handbook of the Law of Algorithms (pp. 312-315). Cambridge University Press.
[40] Ding, X. D. (2026). Challenges and Responses of the Personal Information Protection System in the Context of Artificial Intelligence. Political Science and Law, (1).