International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 6, Nov-Dec 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Research on Single Fault Liability in AI Logistics Platforms

Hu Liting, Zhang Jiaxue, Zhang Yi, Xu Xuebing, Meiherinuer·Aierken

Law School, Beijing Wuzi University, Beijing, China

ABSTRACT

The deep embedding of AI logistics platform algorithms into physical operations, autonomous decision-making, and black box characteristics pose structural obstacles to traditional fault liability determination. The core dilemma lies in the legislative gaps in the recognition criteria, which result in inconsistent judgment scales. The blurred boundary between platform and third-party liability leads to the generalization of joint and several liability. The algorithmic black box blocks causal proof, making it difficult for victims to provide evidence. The lack of algorithmic security obligations leads to the absence of fault judgment. The single fault of the platform can be classified as dereliction of duty in intelligent scheduling and control, lack of operation and maintenance in end delivery, data management negligence, and illegal online activities. In this regard, unified recognition standards should be established within the existing framework of infringement law, responsibility boundaries should be divided based on technical control, phased evidence relief should be set up, mandatory obligations for algorithm security should be added, and the situation of liability reduction should be clarified to balance victim relief and industry innovation.

KEYWORDS: *AI logistics platform; Single fault liability; Algorithmic black box; Causal inference; Algorithm Security Obligations.*

How to cite this paper: Hu Liting | Zhang Jiaxue | Zhang Yi | Xu Xuebing | Meiherinuer·Aierken "Research on Single Fault Liability in AI Logistics Platforms" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-6, December 2026, pp.42-48, URL: www.ijtsrd.com/papers/ijtsrd142283.pdf

IJTSRD142283

Copyright © 2026 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

I. INTRODUCTION

The AI logistics platform focuses on intelligent scheduling, unmanned warehousing, and autonomous driving delivery, with algorithms running through warehousing, transportation, and delivery to make real-time decisions, and the normalization of human-machine mixed operation; However, algorithmic autonomy, black box, and data dependence make it difficult to identify platform faults, and traditional fault liability is difficult to adapt to algorithmic autonomous decision-making[1]. The expansion of algorithmic power also blurs the boundaries of duty of care. AI logistics directly dominates the physical space of people and things, with risks that are realistic, fluid, and involve multiple parties. It has a high frequency of damage, a long causal chain, and strong platform control, and cannot simply copy the rules of e-commerce or content platforms; Existing research mostly focuses on autonomous driving accidents and the responsibility of e-commerce platforms[2], with insufficient attention paid to the independent fault of AI logistics platforms. Our research aims to clarify the boundary between platform single fault and third-party technical fault, provide operational standards for the judiciary, prevent improper joint liability, and balance relief and innovation. Based on fault liability, this study employs normative analysis, case analysis, and comparative methods to analyze the objectification and typification of faults, compare foreign experiences, and propose institutional and judicial countermeasures. The innovation lies in attributing individual faults on platforms independently, constructing a multi-scenario fault type system, and proposing phased burden of proof mitigation and presumption of causality.

II. Basic theory of single fault liability for AI logistics platforms

A. Core Concept Definition

1. AI Logistics Platform Definition: AI logistics platforms belong to digital operation carriers, relying on artificial intelligence algorithms to complete logistics scheduling, business control, and supply chain management. In technical operation, the platform first collects various logistics information, and then uses algorithm models to obtain decision instructions, which are implemented in real logistics operations [3]. The current AI technology has been

applied in warehouse scheduling, end of pipe distribution, supply chain data management and other aspects, changing the traditional logistics operation mode [4]. Unlike ordinary online intermediary platforms that only provide information dissemination, AI logistics platforms are not simply channels for information display. In corresponding business scenarios, algorithm generated scheduling and delivery decisions can directly affect offline physical logistics activities.

2. The connotation of single fault liability mentioned in this article refers to a type of infringement situation where the damage consequences can be attributed to the AI logistics platform's own fault behavior, and other parties generally do not have attributable faults, and the platform alone bears all the infringement consequences. This situation needs to be distinguished from joint liability and mixed fault of multiple parties: joint liability occurs in joint infringement, where multiple actors jointly cause damage, and the victim can demand full compensation from any party; Multi party mixed fault refers to the behavior of multiple parties separately causing damage, and each party sharing compensation according to their own fault size. In a single fault, the fault mainly comes from the AI logistics platform itself.

B. The legal basis for the platform to bear sole fault liability

The theory of hazard control proposes that the entity that initiates and can effectively control risks is usually responsible for the damage caused by the risk. The AI logistics platform controls the operation permissions of the algorithm system, can manage intelligent scheduling, unmanned delivery and other systems, and generally has the ability to avoid damage caused by algorithm errors. This theory can be used as the theoretical basis for the platform to bear single fault infringement liability [5]. In addition, according to the principle of consistency between income and risk in civil law, operators who obtain income from business activities should bear the risk consequences of such activities. AI logistics platforms rely on artificial intelligence algorithms to compress costs, obtain profits, and enjoy the dividends of technological innovation. Generally, they should bear responsibility for the damage risks associated with algorithm operation.

C. Industry specificity of applying single fault liability in logistics scenarios

The algorithmic activities of short video and social networking platforms are primarily confined to online virtual spaces, whereas AI logistics platforms possess dual attributes of algorithmic computation and offline physical operations[6]. The harm caused by algorithms on ordinary internet platforms is mostly limited to information rights and interests. The instructions generated by AI logistics will drive the operation of unmanned distribution and warehousing equipment, potentially causing personal or property damage. Furthermore, the logistics business chain is long, and platform operations, algorithm development, and equipment maintenance are often carried out by different entities. Coupled with the objective existence of algorithmic black boxes, it is practically difficult to identify the faulty entity in practice. Therefore, it is necessary to conduct a special discussion on the sole fault liability of AI logistics platforms.

III. The legal basis for the platform to bear sole fault liability

The algorithmic activities of short video and social networking platforms are primarily confined to online virtual spaces, whereas AI logistics platforms possess dual attributes of algorithmic computation and offline physical operations. The harm caused by algorithms on ordinary internet platforms is mostly limited to information rights and interests. The instructions generated by AI logistics will drive the operation of unmanned distribution and warehousing equipment, potentially causing personal or property damage. Furthermore, the logistics business chain is long, and platform operations, algorithm development, and equipment maintenance are often carried out by different entities. Coupled with the objective existence of algorithmic black boxes, it is practically difficult to identify the faulty entity in practice. Therefore, it is necessary to conduct a special discussion on the sole fault liability of AI logistics platforms.

A. There is a legislative gap in the standard for determining sole fault, and the standards for judgment are not uniform

The current Civil Code's tort liability section does not set specific standards for determining sole fault liability for AI logistics platforms. In cases of damage caused by the same type of intelligent scheduling errors, different courts may reach diametrically opposite conclusions due to different understandings of "reasonable duty of care". Some courts impose heavy penalties by referring to the standards of traditional logistics enterprises, while others believe that AI has exploratory characteristics and should be allowed to make mistakes. Legislative gaps directly lead to serious inconsistency in judicial judgment standards, undermining the predictability of legal application.

B. The boundary of responsibility between the platform and third-party algorithm development entities is blurred, and a single fault is easily mistakenly identified as joint and several fault

The AI system of logistics platforms is usually built with the deep participation of third-party entities such as algorithm developers, cloud service providers, and data providers. When damage occurs, the platform may argue that it stems from a third-party algorithm defect, and the third party may argue that the development task has been completed according to the platform's requirements. When facing multiple defendants, the court often tends to apply the joint infringement provision of Article 1168 of the Civil Code, recognizing the platform and third parties as joint and several liability[7]. However, the prerequisite for the application of joint liability is that all parties involved have joint intent or joint negligence, and the relationship between the platform and the third party is usually only a contractual relationship, and there may not be any intention of joint negligence. More importantly, there is ambiguity in the current law regarding the nature of the legal relationship between platforms and third parties. If the third-party algorithm developer is positioned as a "staff member" as stipulated in Article 1191 of the Civil Code, the platform shall bear alternative liability; If it is positioned as the "contractor" as stipulated in Article 1193, the contractor shall bear its own responsibility [8]. However, in the practice of AI logistics, the degree to which third-party algorithm developers are controlled by the platform is between the two, and the current binary model is difficult to directly apply. The legal qualitative gap further exacerbates the risk of a single fault being wrongly identified as joint liability[9].

C. The black box of algorithms hinders the proof of causality, making it difficult for victims to provide evidence

The principle of fault liability requires the victim to provide evidence to prove the causal relationship between the faulty behavior and the damage consequences. However, the black box nature of AI algorithms makes this proof extremely difficult in the logistics platform scenario [10]. The black box of the algorithm makes it difficult to trace the causal chain, the autonomous iteration of the algorithm weakens the time anchor of causal judgment, and the algorithm decision breaks the empirical correlation between "behavior-result". In the logistics scenario, the supply chain is long and the time span is large, and there are often many intermediate variables between the algorithm fault and the final damage.

D. There is no dedicated algorithm security obligation set for AI logistics, and the lack of basis for fault determination

The core of fault determination lies in determining whether the perpetrator has violated the due diligence obligation. However, current legislation does not establish specific algorithmic security management obligations for AI logistics platforms. The existing regulations such as the Electronic Commerce Law mainly target information intermediary platforms, and their security management obligations focus on protecting user information and maintaining transaction order, without extending to algorithm design, testing, deployment, and operation. The logistics industry also lacks unified algorithm security technology standards, and there are no clear regulations on testing and verification requirements before algorithm launch, monitoring and auditing frequency during operation, and emergency intervention mechanisms for abnormal decisions. In summary, the current infringement liability system is designed with human behavior as the normative object, and its tools for fault identification, causal proof, and liability division have encountered a holistic mismatch in their applicability when facing AI logistics systems with autonomous decision-making capabilities and multi-party collaboration characteristics.

IV. Analysis of Specific Types of Single Faults on AI Logistics Platforms

The dilemma of identifying a single fault in AI logistics platforms can only be solved through typological analysis of specific behavior types. Based on the functional module division of logistics business, a single fault mainly presents in the following five forms.

A. Intelligent scheduling algorithm control negligence fault

The intelligent scheduling algorithm for controlling dereliction of duty is the most typical and frequent type of fault on the platform. In June 2026, the AI dispatch system Movement Planner deployed by BNSF Railway Company in the United States bypassed safety restrictions and discharged a 146 carriage train carrying hazardous substances into the track occupied by road maintenance workers. The disaster was avoided only by the immediate intervention of human dispatchers. The union later wrote to the Federal Railway Administration stating that the accident could have constituted a public disaster[11]. This technical inaction completely shifts the real-time intervention obligation that should have been borne by the system to human dispatchers. If it were not for the latter's immediate intervention, it

would have almost led to a public disaster. Therefore, it can be concluded that the negligence of intelligent scheduling algorithms in controlling this event constitutes a single fault - the passive failure of the algorithm in the security verification stage alone is sufficient to independently trigger the complete failure of the security defense system, without the need for other fault factors to be added.

B. Operational and maintenance oversight in the unmanned delivery algorithm at the end

The fault of the lack of operation and maintenance of the unmanned delivery algorithm at the end is manifested as the platform's failure to properly maintain the perception and decision-making algorithm for delivery vehicles. The unmanned express delivery vehicle in Hohhot did not recognize the fence and traffic cone in the construction area. After multiple unsuccessful attempts to stop, the staff used a reflective cone to smash the vehicle and make it stop. The operator admitted that sensor contamination may cause recognition failure[12]. The existence of blind spots in the perception system, inadequate response of decision-making algorithms to complex road conditions, and lack of emergency redundancy all point to the lack of platform operation and maintenance obligations. Wang Liming once pointed out that negative inaction and positive action that violate security obligations are equivalent in terms of fault composition[13]. The platform charges service fees and collects real-time data, but has not established a daily inspection and remote upgrade mechanism that matches public road risks. There is a significant causal relationship between its inaction and avoidable identification errors, which constitutes a single fault presented in the form of inaction.

C. Omissions and errors in supply chain data and logistics data management

The negligence in the management of supply chain and logistics data is based on the platform's inadequate control over data quality. From July 2025 to January 2026, 21 frozen meat trucks that received orders through the Yunmanman platform collectively deviated from the original southern route and diverted to Biyang, Henan, where they were seized. The freight involved was about 30% lower than the market price, and the total value of the seized frozen goods exceeded 3 million yuan. The platform has launched the "fresh goods tracking" function in January 2024, promising to rely on big data to warn and intervene in abnormal locations. However, none of the 21 deviation incidents received active warnings or customer service follow-up from the platform [14]. Throughout the entire process, there was no second factor involved or superimposed. Based on this, it can be concluded that the negligence in the management of supply chain and logistics data is the single root cause of the incident-the platform should have conducted real-time verification and cross comparison of abnormal driving trajectories, significant deviations in freight rates, and other data, but failed to fulfill its basic data monitoring and warning obligations, and subsequent chain risks could have been avoided. The single fault of this data-driven approach lies in the platform's failure to effectively filter and verify the accuracy of input data, which directly leads to subsequent chain losses.

D. Subjective fault of the platform for launching an AI system in violation of regulations

The subjective fault of a platform for illegally launching an AI system refers to the act of the platform putting the algorithm system into commercial operation despite knowing or should have known that it has significant security flaws or fails to meet the statutory access conditions. The "Guidelines for Safe Service of Autonomous Vehicles in Transportation (Trial)" issued by the Ministry of Transport clearly stipulates that the use of autonomous vehicles for cargo transportation operations should be accompanied by corresponding safety management systems and emergency response plans, and can only be put into operation after passing the test and verification[15]. If a platform operates on public roads without sufficient road testing of the system or obtaining legal access qualifications, the act of launching itself constitutes an independent type of subjective fault, without the need for additional proof of specific errors in the algorithm's operation.

E. The distinction between single fault in logistics scenarios and AI faults in other industries

The core difference between single fault in logistics scenarios and general AI fault lies in the long chain and multivariate characteristics of logistics systems. Medical AI errors usually manifest as diagnostic or prescription errors at a single diagnosis and treatment node, and there is an immediate and direct correspondence between damage and error. The faults of financial AI are concentrated in the decision-making bias of credit evaluation or transaction execution, and the causal chain is relatively clear. The logistics platform operates in a constantly changing physical environment, and a large number of intermediate variables, such as transport duration, road condition change, weather impact, are involved between scheduling decisions and damage results. A single fault often functions in a cumulative manner, which determines that its causal relationship cannot be determined simply by applying traditional rules.

V. Summary of Independent Research on Causation

Determination under Single Fault of AI Logistics Platforms Causation is an essential element for the establishment of tort liability and also a judicial difficulty in AI logistics infringement. Traditional causation determination relies on traceable human behavior chains for factual presumption, with mature judicial logic. However, after algorithms are involved in logistics scheduling, route planning, and distribution operations, traditional rules struggle to cope with new types of technological disputes. This section focuses on single fault of AI logistics platforms, excluding the interference of mixed faults involving multiple subjects, analyzes the dilemma of causation determination between algorithm flaws and damage results, and improves the judicial system for intelligent logistics infringement liability [16].

A. The dilemma of traditional causality identification rules in the context of algorithmic black boxes

1. The presumption logic of traditional causality identification

The traditional causal relationship is based on the conditional theory and the equivalent causal relationship theory, and through the "if there is none, then not" ehavioral context. In conventional logistics infringement, transportation, warehoutest, infers the relationship between behavior and damage based on objective facts and bsing[17].And other behaviors can be observed, and monitoring and operation records can restore the complete chain of behavior, and causal relationships can be verified.

2. Algorithm black box blocks factual inference

AI logistics is autonomously decided by backend algorithms, and the operational logic, data weights, and risk thresholds are not publicly disclosed, forming an algorithm black box. After the accident, the outside world cannot distinguish whether the damage is caused by program vulnerabilities, data deviations, or normal algorithm operation. Algorithmic decision-making has irretrievability, and even if the code is retrieved, it is difficult to reconstruct the inference process at the moment of the accident. The traditional presumption model cannot break through technological barriers, resulting in difficulties in verifying causal facts and creating obstacles to legal application [18].

B. It is difficult to distinguish the cause of a single mistake in logistics dynamic and multivariate scenarios

1. Multiple interference factors in the logistics environment affect logistics operations, including weather, road conditions, warehousing, and manual operations. Even if the unilateral fault of the platform is confirmed, external risks will still intertwine with algorithm defects, jointly inducing damage results.

2. In a complex logistics environment where there is a lack of power of reasons leading to differences in judgment, the degree of harm caused by algorithm errors cannot be quantified. It is difficult for the judiciary to distinguish whether algorithmic flaws are the direct cause, main cause, or conditional factor of damage. The lack of unified discretion standards has resulted in inconsistent judgment scales and vague division of responsibilities in similar cases, which is particularly prominent in long chain businesses such as multimodal transportation[19].

C. The legal obstacle of the inability of victims to provide causal evidence in reality

1. The basic allocation of burden of proof in civil litigation follows the principle of "whoever asserts, bears the burden of proof". The victim needs to prove the infringement, the consequences of the damage, and the causal relationship between the two. This rule is reasonable in ordinary infringement, but it is not suitable for the special scenario of AI logistics.

2. The evidence is biased towards the dual dilemma of technical barriers. Core evidence such as algorithm parameters and scheduling logs are controlled by the platform, and victims lack the technology and channels to obtain data, resulting in serious information asymmetry between the two parties. Victims have difficulty obtaining evidence on their own, and applying for judicial investigation also faces practical obstacles such as high appraisal costs and scarce professional institutions, which makes it difficult for victims to complete causal evidence and hinder their rights protection[20].

D. Feasibility of Applying Causal Inference Rules to AI Logistics with Single Fault

1. The application logic and value of the causal inference rule are aimed at the problem of closed algorithms and biased evidence. Causal inference can be applied to single fault cases on the platform [21]. On the premise of preliminary confirmation of unilateral fault on the platform, it is presumed that there is a causal relationship between the fault and the damage. The platform shall provide evidence to prove that the algorithm is compliant, the damage is unrelated to its own behavior, or there are intervening factors that cut off the causal chain, in order to reduce the burden of proof for the victim and correct the imbalance of evidence status.

2. The system space and boundary causality presumption applicable to the rules can be applied within the current civil law framework, and can refer

to the reversal of evidence rules for environmental pollution and medical damage in the tort liability section of the Civil Code[22]. This rule makes up for the shortcomings of traditional infringement rules, relying on the platform's counter evidence to balance the platform's business interests and victim relief. At the same time, it should strictly adhere to the application boundary and only apply to situations where the platform's single fault has been preliminarily proven, avoiding excessive increase in platform responsibility and hindering technological innovation. Algorithm black box, multivariate interference, and imbalanced evidence are the three major practical challenges in causal identification. Causal presumption provides a judicial path by adjusting the burden of proof, refining the criteria for determining causality in single fault scenarios, and filling the gaps of traditional infringement theory in the field of intelligent logistics, providing theoretical support for the construction of an AI logistics infringement liability identification system.

VI. Institutional measures to improve the definition of single fault liability for AI logistics platforms

A. Unify the criteria for determining single fault on the platform, which means that the platform violates its algorithm security management obligations and fails to take reasonable measures for foreseeable damages. The management obligation covers four aspects: algorithm design, data training, operation monitoring, and emergency response. It is based on the industry's technical level at the time of the damage to avoid reverse inference of results.

B. The clear division of responsibilities between the platform and third-party technology entities should be judged based on technical control and risk activation. The platform has substantial control over the operation of the algorithm, or the algorithm operates for the benefit of the platform, and the platform bears a single fault; If a third party provides universal technology and the platform has fulfilled its obligations, the third party shall be solely responsible[23]. It is prohibited to impose joint liability solely on the grounds of platform benefits or scene provision, in order to prevent the generalization of liability and suppress the application of technology.

C. Optimize the allocation rules for evidence and set up phased evidence mitigation rules: If the victim initially proves that the damage occurred during the operation of the platform and there were abnormalities, the court may require the platform to submit algorithm operation logs, sensor data, scheduling decision records, and impact assessments. If the platform refuses to submit without justifiable reasons or cannot provide a reasonable explanation, it can be presumed that there is a causal relationship and fault. The scope and amount of compensation for damages shall still be borne by the victim to avoid excessive reversal of the burden of proof [24].

D. Establish mandatory obligations for algorithm security operations, based on existing artificial intelligence standards, and add specialized obligations for logistics scenarios: algorithm impact assessment covers path security and human-machine mixing risks; The retention of operation logs covers scheduling decisions, environmental awareness, and manual takeover records; Establish an automatic circuit breaker and manual intervention mechanism for situations such as abnormal weather, equipment failures, and network interruptions.Risk warning is integrated with traffic management and warehousing systems, and data control covers complex roads and extreme working conditions; Algorithm filing and interpretable explanation meet the minimum retrospective requirements for accident investigation [25].

E. Clarify the circumstances of liability reduction and stipulate the statutory reasons for liability reduction: the victim's intentional or gross negligence may reduce or exempt liability; Force majeure or unexpected events, and the platform has fulfilled reasonable emergency obligations, may be exempted from liability; If the algorithm is maliciously attacked or tampered with by a third party, and the platform has taken reasonable network security measures and dealt with them in a timely manner, the responsibility can be reduced; Rare perceptual blind spot risks that comply with mandatory national technical standards and cannot be avoided through regular testing can be used as grounds for liability reduction. The platform bears the burden of proof for the reasons for exemption, in order to prevent the abuse of terms [26].

VII. Conclusion

The AI logistics platform is deeply embedded in physical operations, and the autonomous decision-making of algorithms makes it difficult to adapt to traditional fault liability. The identification of single fault faces four major institutional obstacles: legislative gaps, blurred boundaries between platform and third-party responsibilities, algorithmic black boxes blocking causal proof, and lack of algorithm security obligations. Causal identification is entangled in the dilemma of burden of proof due to the interweaving of algorithmic black boxes and dynamic variables. The presumption rule of causality can balance the interests of both parties. It is necessary to unify the standards for fault identification, divide platform and third-party responsibilities based on

technological control, set up a phased burden of proof mitigation, add mandatory obligations for algorithm security operations, and clarify exemption and reduction scenarios, providing an operable framework for judicial judgment.

REFERENCES

[1] Zheng Ge. The Law of Algorithms and the Algorithms of Law [J]. China Legal Review, 2018(2): 66-85.

[2] Zhang Xinbao, Ren Hongyan. Tort Liability on the Internet: An Interpretation of Article 36 of the Tort Liability Law [J]. Journal of Renmin University of China, 2010,24(4): 17-25.

[3] Zhai Ling. Research on Optimization of Logistics System Based on Artificial Intelligence [J]. Journal of Shanxi University of Finance and Economics, 2024, 46(S2): 77-79

[4] Liang Zhen. Analysis of the Application Practice of AI-Empowered Smart Logistics [J]. China Logistics and Procurement, 2026(04): 119-120.

[5] Yao Beilin. On the Allocation of Data Security Responsibilities in Cloud Environment - From the Perspective of Hazard Control Theory [J]. Network Security Technology and Application, 2024(10):58-60.

[6] Liang Zhen. Analysis of the Application Practice of AI-Enabled Smart Logistics [J]. China Logistics and Procurement, 2026(04):119-120

[7] Yin Fei. Systematic Thoughts on the Application of Tort Liability of the Party Receiving Labor Services [J]. Journal of the National Procurators College, 2023, 31(5): 138-156.

[8] Cao Xianfeng. The Dual Model of Employer Liability and Contractor Liability in the Civil Code [J]. Jurist, 2023, (1): 90-99+193-194. DOI: 10.16094/j.cnki.1005-0221.2023.01.003.

[9] Liu Li. Responsibility Identification and Form of Majority Tort in the Context of Artificial Intelligence [C] // Collection of "Smart Law" 2025, Volume 2 - Collection of Digital Legal Research. 2026: 20-32. DOI: 10.26914/c.cnkihy.2026.000168.

[10] Zhu Xiaofeng. Responsibility Identification when the Causal Relationship of Personal Information Infringement by Generative Artificial Intelligence is Unclear [J]. Forum of Politics and Law, 2025, 43(6): 18-33

[11] http://www.bnsf.com/

[12] https://mp.weixin.qq.com/s?__biz=MjM5OTM5NDI2Mg==&mid=2650233509&idx=1&sn=3c4ca4189f81614fc445dbc77cbc3c14&chksm=be4dfa2fd3db8beafd36eea1a3e507e3723571edf05b4505b25ec2a73ef9ec8d642a669e0581&scene=27

[13] Wang Liming. Research on Tort Liability Law: Second Edition [M]. China Renmin University Press: 2016

[14] https://www.ctdsb.net/c1716_202606/2772793.html

[15] Ministry of Transport of the People's Republic of China https://www.mot.gov.cn/gongkai/zcjd/202512/t20251226_4191175.html

[16] Wang Liming. Research on Tort Liability Law [M]. Beijing: China Renmin University Press, 2020.

[17] Cheng Xiao. An Explanation of the Tort Liability Part of the Civil Code [M]. Beijing: Law Press, 2021.

[18] Zhang Xinbao. Legislative Research on Tort Liability Caused by Artificial Intelligence [J]. China Legal Science, 2022.

[19] Yang Lixin. Improvement of Rules for Traffic Accident Liability of Autonomous Vehicles [J]. Science of Law, 2023.

[20] Zhang Xinbao. Legislative Research on Tort Liability for Damage Caused by Artificial Intelligence [J]. China Legal Studies, 2022.

[21] Wang Liming. Research on Tort Liability Law [M]. Beijing: China Renmin University Press, 2020.

[22] Yang Lixin. Improvement of Rules for Traffic Accident Liability of Autonomous Vehicles [J]. Science of Law, 2023.

[23] Civil Code of the People's Republic of China.

[24] Shen Weiwei. The Myth of Algorithmic Transparency Principle [J]. Global Legal Review, 2019, 41(6): 20-35.

[25] Cyberspace Administration of China, et al. Regulations on the Management of Algorithm Recommendations for Internet Information Services [Z]. 2022.

[26] Yao Beilin. On the Allocation of Data Security Responsibilities in Cloud Environments: From the Perspective of Hazard Control Theory [J]. Network Security Technology and Application, 2024(10):58-60.