WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 10, Number 4, Year 2026
DOI: https://doi.org/10.62051/ijsspa.v10n4.04
Journal homepage: https://ijsspa.org

Abuse of Algorithmic Rights: The Boundary of Criminal Liability for AI Manipulation in the Securities Market

Yuhan Zhang*

School of Vocational Education, Xi'an Eurasia University, Xi'an, 710065, China
*d61132070@gmail.com

ABSTRACT

With the deepening application of AI in securities markets, the issue of abuse of power in algorithmic trading has become prominent, posing a threat to market fairness and investor rights. This paper focuses on the challenges in identifying criminal liability for algorithmic market manipulation and explores the scope of liability for AI decision-making entities under the current legal framework. Existing research primarily revolves around algorithmic transparency, determination of subjective intent, and assessment of market impact, but a consensus has not yet been formed regarding liability attribution for autonomous algorithmic decision-making. The "black box" nature of intelligent algorithms challenges the determination of traditional criminal law subjective elements, while novel manipulation methods expose regulatory lags. Significant differences in management across jurisdictions reflect conflicts between technological ethics and legal values. Current research lacks targeted liability theories, suffers from insufficient interdisciplinary integration, and has a scarcity of empirical samples. The future requires the construction of a criminal liability framework adapted to the characteristics of algorithms, improving diversified regulatory models, providing legal theoretical support for balancing technological innovation and market order, and contributing to the improvement of China's securities market regulatory system.

KEYWORDS

Algorithm Rights; Securities Market; AI Manipulation; Criminal Responsibility; Boundary.

1. INTRODUCTION

With the deep integration of artificial intelligence technology and the securities market, the characteristics of algorithmic trading have given rise to new types of market manipulation behaviors, from high-frequency spoofing to AI collaboration, posing challenges to the traditional criminal liability identification system. How to penetrate technology, clarify the liability boundaries among algorithm developers, users, and regulators, and balance technological innovation with market order security has become a core proposition urgently to be solved in the field of financial rule of law.

2. TECHNICAL MEANS OF AI MANIPULATION IN THE SECURITIES MARKET

Algorithms have now become key foundational tools in various industries. However, these algorithms might cooperate with each other, hoard profits, and even crowd out normal human trading[1]. Such technology-enabled manipulation methods not only undermine market fairness but also pose a severe test to the existing legal regulatory system[2]. Current securities regulatory rules lack clear definitions for such new manipulation methods, resulting in certain regulatory blind spots. Coupled with

insufficient cross-border regulatory cooperation, differences in identification standards among different jurisdictions provide room for evading cross-border violations.

Traditional market manipulation mainly involves artificially inflating stock prices by agreeing on transaction times and prices with others in advance, conducting a large number of false transactions between accounts under one's actual control, or providing false investment advice to misleading other participants into investing before conducting reverse transactions. It can be traced through traces such as trading volume fluctuations and account correlations, with a limited scope of impact. Moreover, subjective intent can be corroborated by objective facts such as transaction motives, capital flows, and account correlations, and the overall regulatory approach mainly relies on price and trading volume indicator monitoring and post-event investigation and handling.

In contrast to traditional market manipulation, new types of market manipulation are mainly manifested in behaviors such as high-frequency trading and algorithmic collaboration. High-frequency trading is characterized by high speed, automation, and low-latency information transmission. It obtains market quotes in advance and completes a large number of order placements and cancellations within milliseconds to create false market signals[3]. Spoofing is a typical high-frequency trading method, whose core is a three-step cycle of "false placement - cancellation - reverse operation" to create the illusion of supply and demand, lure other market participants into misjudgment and follow-up operations to drive prices, cancel all false orders before they are executed, and then conduct real transactions in the opposite direction. Algorithmic collaboration relies on distributed networks to achieve cross-subject and cross-market transaction linkage, forming a hidden manipulative force. These behaviors collectively rely on the "black box" characteristics of algorithms-opaque decision-making processes, autonomous learning, rapid execution, complex transaction logic, and strong disguise-making it difficult to determine "human intent"[4].

3. APPLICATION DILEMMAS AND CHALLENGES OF THE CURRENT CRIMINAL LIABILITY FRAMEWORK

3.1. Substantive Law Dilemmas

(1) Rigid Identification of Liability Subjects: Current laws are difficult to adapt to AI autonomous decision-making scenarios and cannot determine the independent liability subject status of highly autonomous AI. In addition to the emergence of AI as a new liability subject, human crimes and humans themselves should also appear in a new form[5].

(2) Obstacles to Proving Subjective Intent: The difficulty in tracing the algorithmic decision-making process invalidates the identification standards of traditional criminal law that rely on corroboration of human subjective intent. Especially for manipulation behaviors generated by AI autonomous learning, it is impossible to define "human intent," making it difficult to apply existing provisions.

(3)Insufficient Coverage of Behavior Types: Provisions such as Article 182 of the Criminal Law are designed based on traditional manipulation models and do not cover new manipulation behaviors spawned by AI, and the application of catch-all clauses is also uncertain[6].

(4) Lack of Adaptability in Imputation Standards: A differentiated imputation system targeting the degree of AI autonomy (ordinary robots - weak AI - strong AI) has not yet been formed[7]. The existing imputation path cannot respond to the liability division problems brought by algorithmic autonomy, and there is a lack of clear regulatory basis for manipulation behaviors.

3.2. Procedural Law Dilemmas

(1)Imbalanced Distribution of Burden of Proof: Prosecutors are difficult to break through the algorithmic "black box" to obtain core evidence such as subjective intent and causality. There are

regulatory vacuums and regulatory dilemmas of decision lag caused by the learning cycle of algorithms, and the existing burden of proof rules do not take this difference into account[8].

(2)Difficulty in Evidence Acquisition: The high-speed execution, massive data, and easy tampering characteristics of algorithmic trading make it difficult to timely obtain key evidence such as logs and decision data related to manipulation behaviors, and there is a lack of unified evidence collection standards.

(3)Lack of Technical Interpretation: There is a lack of authoritative algorithmic technical identification mechanisms, and algorithm interpretability is insufficient. Paragraph 1(5) of Article 55 of the new Securities Law stipulates deceptive trading manipulation behaviors in information-based manipulation, but the enumeration of their behavior patterns is not comprehensive, failing to provide clear decision-making basis[6].

(4)Obstacles to Cross-border Evidence Collection and Cooperation: AI manipulation behaviors often involve cross-border activities, but there are significant differences in legal provisions and evidence standards among different jurisdictions, and there is a lack of effective cross-border evidence collection cooperation mechanisms, affecting the criminal liability pursuit of cross-border manipulation behaviors [9].

4. COMPARATIVE STUDY OF REGULATORY PATHS IN THE UNITED STATES AND THE EUROPEAN UNION

4.1. U.S. Practice and EU Exploration: "Controller" Liability vs. "Market Abuse"

4.1.1. U.S. "Controller" Liability Practice

Focusing on "control power," it emphasizes "human dominance over algorithms" and denies the independent liability status of AI. In the Coscia case, the court held that the defendant had the design and control rights over the algorithm manipulating the market, and convicted Coscia of all six counts of spoofing and six counts of commodity futures fraud. Even though the algorithm executed transactions automatically, the defendant was still convicted of criminal liability for manipulating the securities market[10]. In the Mina Tadrus case, the defendant profited from an artificial intelligence algorithmic trading model and made false propaganda relying on investors' attention to the new artificial intelligence technology, ultimately being convicted of investment advisor fraud[11]. The above cases clearly show that algorithm-driven high-frequency spoofing transactions can be subject to criminal liability. We can conclude its regulatory characteristics: there is no unified legislation targeting AI manipulation in securities; instead, institutions such as the SEC and CFTC regulate within their respective jurisdictions and respond to new types of manipulation by reinterpreting existing laws[12]. At the same time, it promotes corporate self-supervision, requiring the retention of algorithm logs, providing typical case support for regulatory authorities to investigate AI-related financial fraud, and avoiding evading liability solely on the grounds of "algorithmic black box."

4.1.2. EU Market Abuse Regulation (MAR) Exploration

It includes new manipulation behaviors using AI into the scope of regulation, emphasizing pre-event prevention and in-event supervision. Based on the potential impact of artificial intelligence systems, the bill classifies them into four categories, each applicable to different levels of regulation[13]. In 2025, the EU imposed a total fine of over 157 million euros on three brands: Gucci, Chloé, and Loewe. The three companies restricted the independent pricing power of cooperating third-party retailers and manipulated resale prices to inflate commodity prices, harming consumer interests. This case strengthened the industry's attention to compliance requirements related to independent pricing power[14]. Its regulatory characteristics are coordinated operation with the AI Act, requiring institutions to fulfill obligations such as risk management, and conducting third-party assessments of

algorithm compliance. If MAR is violated and it belongs to high-risk AI applications, the AI Act will be applied cumulatively, with a maximum fine of 7% of global annual turnover[15]. It introduces "presumption of causal link" and "right to evidence acquisition," which were also used in the Coscia case[16].

4.2. Experience Summary and Critical Reference

4.2.1. Experience Summary

(1)The United States clarifies that as long as one has behaviors such as designing and controlling illegal acts, one must bear liability; the EU, in combination with the AI Liability Directive, presumes the fault association of algorithm users. Both break the misunderstanding of "algorithmic black box exemption" and provide key basis for liability tracing.

(2)The U.S. model of "post-event accountability + industry self-regulation" retains room for market innovation and adapts to the rapid iteration characteristics of AI technology; the EU's "pre-event prevention + risk classification" system strictly regulates high-risk AI and moderately relaxes low-risk AI, achieving a precise balance between innovation and risk[17].

(3)U.S. institutions such as the SEC and CFTC are separately responsible for regulation and handle new types of market manipulation by interpreting existing laws; the EU uses multiple regulations in combination, proving the core role of multiple departments and regulations acting together in combating complex AI financial violations.

4.2.2. Critical Reference

Reference Boundaries of the U.S. "Post-event Accountability" Model: We can learn from its flexibility in legal interpretation and case guidance, avoid "one-size-fits-all" in AI financial regulation, gradually delineate the boundaries of algorithm application through typical cases, reserve room for trial and error for technological innovation, avoid the defects of scattered and blank regulation, establish a unified regulatory coordination mechanism to prevent overlapping responsibilities or "passing the buck" among multiple institutions, strengthen pre-event risk prompts, and reduce investor losses.

Reference Boundaries of the EU's "Strict Compliance" Model: We can refer to its framework of "risk classification and full-process control" and set real-time monitoring obligations for high-risk AI; however, we need to be wary of the problem of "excessively high compliance costs." We can reduce the burden on the market by simplifying the compliance process for low-risk AI of small and medium-sized institutions and providing compliance guidelines, balancing regulatory efficiency and market vitality.

5. SYSTEM RECONSTRUCTION AND RULE PATH OF CRIMINAL LIABILITY FOR AI MARKET MANIPULATION

5.1. Basic Principle: Liability Penetration under Technology Neutrality

The core principle of technology neutrality is that we should not restrain technological development to improve the legal system, nor should we increase or exempt legal liability due to its special attributes. The identification of criminal liability needs to penetrate the technological shell. Whether it is algorithm developers, managers, or users, as long as they have control rights, decision-making rights, or supervision obligations over AI market manipulation behaviors, they must bear corresponding criminal liability. This principle not only prevents using AI as an excuse to whitewash and evade criminal liability but also avoids letting "algorithmic black box exemption" go unchecked due to technical complexity.

5.2. Reconstruction at the Substantive Law Level

Manipulation behaviors implemented by developers and producers can be divided into two scenarios:

(1)Developers and producers specially develop and generate artificial intelligence products for criminal purposes, and then use the products to illegally control the securities market and falsely disseminate market information.

(2)Developers and producers initially did not develop and generate artificial intelligence products for criminal purposes, but the products were illegally used by users due to accidents or negligence[18].

(1)Breaking through the limitation of traditional "direct actors" and constructing a "three-tier liability subject system":

Core Layer (Direct Liability): Algorithm developers, producers, and trading strategy formulators who have direct intent to conduct AI manipulation behaviors. The core of imputation is "intentional acts."

Middle Layer (Supervisory Liability): Senior executives and responsible persons of financial institutions who fail to perform the obligations of reviewing and monitoring algorithms, leading to AI autonomously implementing manipulation behaviors or being illegally used by users. The imputation standard is "gross negligence."

Peripheral Layer (Auxiliary Liability): Technology service providers and data providers who provide support knowing or should knowing that their technology and data are used for AI manipulation, and are held liable as accomplices or for separate crimes.

(2)Adjusting the traditional criminal liability imputation logic in combination with AI technical characteristics:

For core layer subjects, adhere to the "intentional liability principle," which requires proving that they knew the algorithm would cause market manipulation and lead to crimes but still promoted and used it.

For middle layer subjects, apply the "fault presumption principle," comprehensively judge and presume based on whether the actually participating subjects have benefited, the size of their benefits, and the degree of control over artificial intelligence[19]. If they can reasonably and compliantly prove that they have not benefited from it or have performed obligations such as compliance review and risk monitoring, negligence is determined.

6. SYSTEMS SHOULD KEEP PACE WITH TECHNOLOGICAL DEVELOPMENT: TOWARDS A TECHNICALLY RATIONAL RULE FRAMEWORK

6.1. Legislative Suggestions: Amendatory Interpretation and Improvement of Criminal Law Provisions

(1)Prior Judicial Interpretation to Clarify the Application Boundaries of Traditional Provisions: Currently, the Criminal Law has included the "crime of manipulating securities and futures markets" in the "crime of disrupting financial management order" under the "crime of disrupting the socialist market economic order" for regulation[20]. In the future, new types of market manipulation behaviors can also be included in the scope of regulation, and special judicial interpretations can be issued to clarify "algorithmic control power" and "technical decision-making participation" as core elements for liability identification.

(2)Supplementary Special Provisions to Respond to AI-specific Risks: At present, since China's current Criminal Law and its judicial interpretations do not stipulate behaviors of manipulating securities and futures markets[18],a new crime of "manipulating financial markets using artificial

intelligence" should be added to the "crime of disrupting financial management order" in the Specific Provisions of the Criminal Law, independently stipulating its constitutive elements including but not limited to "creating false market supply and demand signals through AI technology" and "intentionally allowing autonomous algorithms to implement manipulation behaviors."。

(3)Establishing a Dynamic Legislative Response Mechanism: Relying on the technical monitoring data of financial regulatory authorities and judicial organs, regularly sort out new behavior patterns of AI market manipulation, and timely update the scope of application of provisions through a combination of "legislative interpretation + case guidance" to ensure that criminal law rules keep pace with technological iteration.

6.2. Law Enforcement and Judicial Improvements and Collaborative Governance

(1)Law enforcement departments need to "counter technology with technology" and build an AI algorithm regulatory platform. Conduct pre-event filing and in-event real-time monitoring of algorithms in high-risk areas, identify abnormal behaviors through technical means such as big data analysis and algorithm traceability, and realize early warning and precise crackdown on illegal behaviors. Implement hierarchical law enforcement, apply administrative fines and orders for rectification to minor violations, and promptly transfer suspected criminal behaviors to judicial organs to achieve "matching regulatory intensity with technical risks."

(2)Judicial organs need to break the "technical cognitive barrier" to ensure the professionalism and fairness of judgments. First, absorb professionals in computer technology, financial engineering, etc. as jurors or technical consultants to accurately determine core facts such as algorithm design intent and liability subject fault. Second, optimize evidence rules, clarify the collection of evidence such as "algorithm logs," "transaction data," and "compliance review records," stipulate identification standards, and allow the restoration of the algorithm operation process through technical identification to solve the problem of difficult proof. Third, issue typical case guidance, unify judicial judgment standards by publishing judgment rules for AI market manipulation crimes, realize "similar cases with similar judgments," and demonstrate the certainty and authority of the law.

(3)Governance by a single subject is difficult to cope with the cross-domain and cross-regional characteristics of AI technology, so a multi-dimensional collaborative governance system needs to be built: regulatory authorities and judicial organs establish an information sharing platform to achieve seamless connection between law enforcement data and judicial evidence, improving the efficiency of case handling; financial industry associations formulate AI algorithm compliance guidelines, clarify industry self-regulation standards, and promote self-restraint of industry subjects; encourage technology enterprises to participate in rule-making, build a mechanism for quickly identifying illegal financial market manipulation behaviors, promptly take circuit breaker measures to prevent risk spread, and improve post-event accountability and evaluation mechanisms[21].

7. CONCLUSION

Algorithmic trading has spawned new types of market manipulation behaviors, bringing systematic challenges to traditional criminal liability identification. This article conducts research from four dimensions: technical characteristics, legal dilemmas, comparative reference, and system reconstruction, pointing out that AI manipulation is essentially different from traditional manipulation in terms of efficiency, concealment, and accountability difficulty, exposing the lag of legal regulation.

Currently, substantive law is difficult to adapt to AI autonomous decision-making in terms of identifying liability subjects, subjective intent, and behavior types, while procedural law faces practical obstacles such as difficult proof and evidence acquisition. By comparing the two regulatory models of U.S. "post-event accountability" and EU "pre-event prevention," this article proposes the principle of "liability penetration under technology neutrality," constructs a three-tier liability system

of "core layer - middle layer - peripheral layer," and puts forward improvement paths from both substantive law and procedural law perspectives.

This article accurately grasps the difficulties in liability identification for AI market manipulation, constructs a regulatory framework balancing technological innovation and market order, and has reference value for the construction of financial technology rule of law.

REFERENCES

[1] Lü, T. (2025). Potential risks and prevention paths of algorithmic homogenization in securities trading. Journal of Dalian University of Technology (Social Sciences), 44(2), 120-128.

[2] Jing, Z. (2023). Research on algorithmic regulation of program trading market manipulation behaviors. Securities Law Studies, 10(2), 45-60.

[3] Wang, Y. (2022). Criminal law regulation of technical manipulation behaviors in the securities and futures market. New Economy (Youth Perspective), (11), 136-141.

[4] Feng, X. (2022). Research on regulatory issues of market manipulation behaviors in the intelligent era. Financial Regulation Research, 8(4), 78-92.

[5] Huang, Y. (2021). On criminal liability subjects in the era of artificial intelligence: misunderstandings, positions, and types. Chinese Journal of Law, 43(3), 112-125.

[6] Li, Z., & Xia, Z. (2021). Evaluation of the gains and losses of the revision of market manipulation clauses in the new Securities Law. Securities Market Herald, 30(6), 55-68

[7] Liu, X. (2020). The evolution of criminal liability in the era of artificial intelligence: yesterday, today, tomorrow. China Legal Science, 37(5), 88-102.

[8] Wang, S., & Ma, R. (2022). Construction of an intelligent investment advisor algorithm black box regulatory system under the background of financial data security. Financial Law Review, 15(1), 34-50.

[9] de Koker, L., & Goldbarsht, D. (2022). Financial technologies and financial crime: key developments and areas for future research. In Financial technology and the law: Combating financial crime (pp. 303-320). Cham: Springer International Publishing.

[10] Pantano Jr, P. J., Schachter, M. S., Molesworth, R. M., Gray, E. P., Aguirre, S. A., & Kumar, N. E. (2017). Spoofing Conviction Upheld: Vagueness Challenge Rejected

[11] U.S. Attorney's Office for the Eastern District of New York. (2025). Founder of Purported Artificial Intelligence-Powered Hedge Fund Sentenced to 30 Months. https://www.justice.gov/usao-edny/pr/founder-purported-artificial-intelligence-powered-hedge-fund-sentenced-30-months

[12] Xiao, K. (2017). Judicial determination of spoofing-type high-frequency trading from the Coscia case. Procuratorial View, (4), 28-29.

[13] Liu, X., & Ding, H. (2024). Interpretation of the key points of the EU Artificial Intelligence Act. Zhong Lun Insights. https://www.ctils.com/articles/13737?use_xbridge3=true&loader_name=forest&need_sec_link=1&sec_link_scene=im&theme=light.

[14] Huang, L. (2025). Restricting retailers from price cuts and discounts, three luxury brands fined 157 million euros by the EU. Toutiao. http://m.toutiao.com/group/7562061092206264873/?upstream_biz=doubao&use_xbridge3=true&loader_name=forest&need_sec_link=1&sec_link_scene=im&theme=light

[15] Tian, X., & Li, S. (2025). Regulatory challenges and response thoughts of artificial intelligence technology for the capital market. China Capital Market Research Network. https://www.ccms.org.cn/insights/c/c_20251031_10796649.shtml?use_xbridge3=true&loader_name=forest&need_sec_link=1&sec_link_scene=im&theme=light

[16] Cao, S. (2018). Enlightenment of the EU financial regulatory system on China's front-line transaction supervision (partial content). Securities Times..

[17] Act, E. A. I. (2024). The eu artificial intelligence act. European Union.

[18] Liu, X., & Yu, Y. (2024). Criminal law improvement of securities and futures crimes involving generative artificial intelligence. Journal of Zhejiang Gongshang University, 18(3), 47-57.

[19] Sun, K., & Bao, H. (2023). Algorithmic collusion in the era of artificial intelligence, how to deal with it? China Trial, 2023(18).

[20] Jiao, Z., & Li, M. (2019). Spoofing transactions: typed interpretation and futures market manipulation regulation. Journal of Graduate School of Chinese Academy of Social Sciences, 230(2), 98-103.

[21] Liu, Q., & Bian, H. (2024). Generation, dissemination, and regulation of AIGC false information in China's financial market. New Finance, 2024(8), 32-38.