

Criminal-Law Regulation of Illegally Obtaining Token Data for Volume-Boosting and Comment-Manipulation

Jiahui Li*

School of Law, Shandong University of Traditional Chinese Medicine, Jinan, Shandong, China

**Corresponding author: Jiahui Li.*

Abstract

With the prevalence of online traffic, cases involving the illegal acquisition of Token data have kept emerging. Nevertheless, multiple judicial dilemmas persist for such cybercrimes: inconsistent criteria for determining the legal nature of Tokens; widespread conviction by default under the crime of illegally obtaining computer information system data; and judicial practices that penalize only the front-end act of stealing Tokens while overlooking subsequent harms caused by volume-boosting and comment-manipulation. For such cases, special judicial interpretations targeting cyberspace should be promulgated to clarify the legal attributes of Token data and unify adjudication standards. Consideration should be given to adding a new crime of impairing online-traffic order to specifically regulate criminal acts of stealing Tokens for bulk account login to conduct volume-boosting and comment-manipulation, so as to safeguard fair competition in platform traffic. Meanwhile, adjudicative mindsets ought to be adjusted: the entire black-and-grey industry chain shall be evaluated as a whole, and conviction shall be based on the core perpetrating acts of the crimes.

Keywords

token data, derivative personal information, algorithm-based identification, volume-boosting and comment-manipulation

1. Introduction

In cyberspace, a Token is an identity token issued by platforms. It represents the identity of a logged-in user and serves as a temporary identity credential that enables login without entering account passwords. After stealing Tokens, perpetrators can simulate bulk user logins and manipulate accounts to perform mass operations such as liking and commenting. Amid the boom of the online-traffic economy, stealing and exploiting Tokens for volume-boosting and comment-manipulation has evolved into a mature, complete industrial chain. According to publicly available data from the “Clean-the-Net” special campaign of the Ministry of Public Security, within merely one year, public-security organs nationwide investigated over 900 cases involving online water-army groups and apprehended more than 5,000 criminal suspects. Some criminal gangs can generate tens of billions of false interactions in bulk, with high case-related amounts and severe social harms.

Stealing Token data to conduct volume-boosting and comment-manipulation undermines fair platform-based economy competition. In addition, illegal access to Token data may inversely locate users and trigger leaks of users’ derivative personal information. Existing studies mainly focus on the legal nature of Tokens

and the characterization of volume-boosting behaviors, while lacking a holistic evaluation of the black-and-grey industrial chain related to Tokens. This paper is divided into three parts. The first part defines the behavioral pattern of Token-based volume boosting. The second part analyzes relevant judicial disputes. The third part puts forward corresponding improvement approaches.

2. Basic Definition and Behavioral Patterns of Acts of Illegally Obtaining Token Data

2.1 Defining the Data Attributes of Token Identity Credentials

A Token is a temporary login credential issued by platforms to streamline repeated user login procedures. While it contains no explicit identity information itself, background algorithms can match it with the identity of specific individuals. For instance, after a user logs into a short-video platform, the server generates a Token and sends it to the user's device. The Token does not directly record explicit identifiers such as natural persons' real names or ID numbers; instead, it is uniquely bound to a user ID in a one-to-one correspondence. Once stolen by wrongdoers, the Token can be used to log into others' accounts. After the platform verifies the Token's validity, it can pinpoint the bound user ID. By retrieving corresponding user IDs from background databases based on the Token and leveraging platform algorithms, perpetrators can access registered account information, avatars, nicknames, historical interaction records and other data, and ultimately identify the specific natural person behind the account. Without acquiring account-password credentials, offenders can submit stolen Tokens to platform interfaces and manipulate large batches of accounts for volume-boosting and comment-manipulation in this manner.

Two sets of standards prevail in judicial adjudication. The first represents a conservative adjudicative logic under which only data containing explicit identity information qualifies as personal information—a reasoning previously seen in rulings on Cookie-related cases. The second draws on existing academic research on algorithm-driven identity recognition [1]: whether data constitutes personal information hinges not on whether it explicitly records identity content, but on whether algorithms can indirectly identify a specific natural person through such data. Text analyses of privacy policies from one hundred mobile applications conducted by Liao Bingyi and other scholars show that platforms commonly associate and identify users through device identifiers such as Cookies. As a comparable identity credential, Tokens follow the same identification logic. Synthesizing the characteristics of Token data alongside prevailing judicial criteria, Tokens possess the legal feature of indirectly identifying natural persons, and bear dual attributes as both computer-system data and derivative personal information.

2.2 The Complete Behavioral Chain of Illegally Obtaining Tokens for Volume-Boosting and Comment-Manipulation

A full-fledged industrial chain for Token-enabled traffic fraud has taken shape, comprising closely integrated upstream, midstream and downstream links. In the upstream segment, perpetrators steal user Tokens in bulk via Trojan horse programs, malicious plug-ins or crawler technologies. For example, Trojan horses can be implanted into users' computers or mobile phones to surreptitiously capture Tokens stored in browsers or applications when users log in normally. Malicious plug-ins may also be disguised as practical utilities: once installed by tricked users, they monitor websites and intercept Tokens upon their issuance by platforms. In the Shanghai Li Mou case, the defendants repackaged applications to induce user installation, and surreptitiously stole users' Token data to boost live-stream viewership for profit [2].

In the midstream, automated script programs are developed, into which upstream-obtained Tokens are imported to realize mass log-ins to accounts across major internet platforms. Judgments from Fengxian District People's Court illustrate that perpetrators operating automated scripts can simultaneously control hundreds or thousands of accounts, furnishing technical support for subsequent volume-boosting and comment-manipulation.

Downstream actors exploit these mass-controlled accounts to post false comments, inflate viewership for live-streams, raise the popularity of goods and live-stream rooms, mislead consumers and drive sales for illicit gains.

Token theft is merely a means to achieve traffic fraud, whereas manipulating traffic and comments constitutes the core objective; the two are inextricably linked. Purely stealing Tokens cannot directly generate economic profits—perpetrators cannot profit without leveraging stolen Tokens for subsequent volume-boosting and comment-manipulation. Conversely, implementing volume-boosting and comment-manipulation requires large quantities of accounts as tools, rendering the theft of login-enabling Tokens an indispensable prerequisite. These acts serve as mutual preconditions for one another. Nevertheless, some grassroots courts adopt conservative adjudicative reasoning, assessing only upstream Token-theft while disregarding perpetrating acts of volume-boosting and comment-manipulation in midstream and downstream segments.

3. Judicial Controversies Concerning Acts of Illegally Obtaining Token Data

3.1 Judicial Divides over the Legal-Nature Determination of Token Data

Current judicial interpretations lay down general definitions for computer-system data and personal information, yet contain no special provisions for specially-featured data such as Tokens. The 2011 interpretation on crimes endangering computer-information-system security enumerates account numbers, passwords and digital certificates within identity-authentication information, while the 2017 interpretation on personal-information crimes defines citizens' personal information as information that can, alone or in combination with other information, identify a specific natural person. Significant divergences exist in trial practice. Some courts classify Tokens purely as computer-system data on the grounds that they carry no explicit identity markers and apply the crime of illegally obtaining computer information system data [2]. In the Shanghai Li Mou case, for example, the court held that since Tokens contained no plain-text personal identifiers such as names or ID numbers, defendants were convicted under that crime. Other courts adopt the algorithm-identification standard, qualify Tokens as personal information, and apply the crime of infringing upon citizens' personal information [3]. Guiding Case No. 195 released by the Supreme People's Court involving Luo Mou and Qu Mou, who profited by selling mobile-phone verification codes [4], exemplifies this approach: the court ruled that verification codes may qualify as citizens' personal information under criminal-law provisions under given conditions and convicted the defendants of infringing upon citizens' personal information.

Scholars including Peng Chengxin and Xu Wei argue that algorithm-driven identification represents the essential characteristic of personal information [5]. The "identifiability" stipulated in traditional legal provisions is not the quintessence of personal information; identifying specific natural persons via platform algorithms lies at the heart of identifying individuals from online data. This theory supports the proposition that Tokens constitute derivative personal information, and refutes conventional adjudicative logic. It also exposes regulatory gaps in current judicial interpretations when distinguishing ordinary computer data from special data capable of identifying natural persons, which has given rise to conflicting rulings in materially similar cases. Some scholars warn that adopting the algorithm-identification standard might expand the scope of personal information to engulf ordinary online data. Still, algorithm-based identification does not automatically label data as personal information merely because background systems can associate it with users [6]; certainty of identification and direct relevance must also be satisfied.

3.2 Absence of Specialized Crimes for New-Type Criminal Conduct

When the existing criminal-law system was constructed, criminal acts revolving around Token-type data were not anticipated, leading to deficiencies in evaluating Token-theft conduct. In current judicial practice, most cases involving Token-driven volume-boosting and comment-manipulation resort to the crime of illegally obtaining computer information system data as a fall-back conviction. No specialized crime targets disruptions to online-traffic competition order. Such fall-back convictions under this crime cannot fully capture core harms inflicted by backend traffic manipulation.

In the case of Li Mou, Rong Mouwei and three accomplices, the defendants repackaged applications embedded with malicious code, tricked users into installing them, stole users' Token data without consent, logged into accounts in bulk to boost live-stream popularity and post false comments. Forensic appraisal identified 47,219 sets of Token information and 1,421 sets of Cookie data stored on defendant-controlled servers, meaning digital keys for at least 48,000 accounts were illegally obtained. The court convicted the five

defendants of illegally obtaining computer information system data and meted out fixed-term imprisonment ranging from one year to three years and two months, together with fines from RMB 8,000 to RMB 20,000. Following conservative adjudicative logic, the court only evaluated defendants' conduct of obtaining Tokens by implanting malicious code in repackaged applications and inducing installations. It failed to adjudicate subsequent volume-boosting and comment-manipulation targeting live-streams and merchandise. Consequently, rulings cannot regulate acts that generate fake traffic to disrupt market order and harm consumers. In an era defined by online traffic, adjudicative and legislative rationales inherited from traditional sectoral law prove ill-suited. Scholarly discussions on the independent development of cyber-criminal law further attest to the need to fill gaps in cyber-related legislation.

3.3 Incomplete Criminal-Law Evaluation of Composite Criminal Conduct

Existing criminal charges only enable fragmented evaluation of acts of stealing Tokens for volume-boosting and comment-manipulation. Gaps in regulating backend exploitation of data crimes in current judicial practice narrow the scope and intensity of criminal-law crackdowns [7]. Traditional criminal-law evaluation models built around single harmful acts struggle to accommodate composite behavioral structures characterized by upstream-downstream linkages within cyber black-and-grey industries. Traffic fraud harms not only personal-information and data security but also fair internet-competition order and fuels vertically integrated black-and-grey industrial chains. Hence greater attention must be paid to backend core perpetrating acts and underlying criminal purposes behind Token-theft-enabled crimes.

Existing criminal charges including the crime of false advertising, the crime of illegal business operations, and the crime of sabotaging production and business operations all suffer from limits in application and fail to fit the behavioral patterns and legal-interest infringements of online-traffic black-and-grey industries. First, the crime of false advertising governs direct false promotion concerning goods or services. Token-theft-enabled bulk volume-boosting and comment-manipulation merely fabricates artificial popularity and public-opinion atmospheres without directly advertising goods or services. Such conduct therefore falls outside the scope of false-advertising offenses.

Regarding the crime of illegal business operations, judicial precedents have convicted organizers of paid volume-boosting services for click-farming under this crime pursuant to Article 7 of the 2013 Judicial Interpretation on Issues Concerning the Application of Law in Handling Criminal Cases Involving the Use of Information Networks to Commit Libel and Other Offenses. Yet three limitations constrain its application. First, its regulatory scope is narrow: it covers only organizers providing paid services. It cannot capture upstream Token-thieves nor evaluate downstream scenarios where perpetrators steal Tokens for self-use in volume-boosting. Second, convictions rely on the catch-all clause under Item (4), Article 225 of the Criminal Code, which should be construed narrowly. Randomly subsuming diverse online violations under this crime risks over-criminalization. Third, this crime protects primarily market-access and business order. It cannot fully evaluate infringed legal interests such as data security and derivative personal information stemming from Token-theft.

As for the crime of sabotaging production and business operations, traditional adjudication requires perpetration via destroying machinery and equipment, injuring or slaughtering draught animals, or other means of sabotaging production and business. Although the 2015 reverse click-farming case heard by Yuhuatai District People's Court of Nanjing brought malicious online click-farming within the purview of this crime, its application to Token-theft-driven volume-boosting and comment-manipulation remains controversial. Such conduct mostly inflates commodity prices and account popularity rather than inflicting physical damage on platform servers or equipment, making it hard to subsume under this offense.

4. Pathways to Improve Criminal-Law Regulation of Acts of Illegally Obtaining Token Data

4.1 Judicial Improvement: Establish Conviction-Distinguishing Criteria Centered on Core Perpetrating Acts

To regulate the Token-related volume-boosting-and-comment-manipulation black-and-grey industry within the current judicial framework, criteria for identifying core perpetrating acts must first be clarified. A core perpetrating act directly brings about principal legal-interest infringements and constitutes the pivotal link

generating harmful consequences across criminal chains. Core perpetrating acts within behavioral chains may be identified by examining two dimensions: sources of illicit gains, and harmful consequences, i.e., which conduct directly undermines fair platform-competition order [8].

Under substantive law, for the black-and-grey industry of stealing Tokens for volume-boosting and comment-manipulation, Token-theft constitutes a means-act while volume-boosting and comment-manipulation represent purpose-acts. The full behavioral chain ought to be evaluated integrally. Token-theft and subsequent volume-boosting and comment-manipulation exhibit a means-to-end implicated relationship, but the application of implicated offenses requires that both the means act and purpose act independently constitute crimes. Two scenarios should be distinguished. Where actors organize paid volume-boosting services, the purpose act constitutes the crime of illegal business operations, while the means act of stealing Tokens may establish the crime of illegally obtaining computer information system data or the crime of infringing upon citizens' personal information. In such cases, the implicated offense rule applies and the heavier penalty shall be imposed. In contrast, if actors steal Tokens merely for self-use volume-boosting and comment-manipulation, the purpose act cannot be criminalized under current law. The prerequisites for implicated offenses are therefore unfulfilled, leaving only the crime of illegally obtaining computer information system data to be applied, which results in fragmented evaluation. This normative gap motivates the proposal of a new offense in the subsequent section. Take the Shanghai Li Mou case: stealing Tokens served merely as a means; profiting by leveraging Tokens to log into accounts in bulk and boost live-stream popularity constituted the ultimate purpose. Adjudication should assess the complete behavioral chain.

As for purpose-acts of volume-boosting and comment-manipulation, organizing paid volume-boosting services may be evaluated as the crime of illegal business operations under Article 7 of the 2013 Judicial Interpretation on Cyber Libel Cases. The means-act of stealing Tokens may trigger convictions for illegally obtaining computer information system data. Where Tokens are deemed derivative personal information, the crime of infringing upon citizens' personal information may apply. Judicial organs should select and impose the heavier penalty among the crime of illegal business operations, the crime of illegally obtaining computer information system data, and the crime of infringing upon citizens' personal information. Current judicial practice should revise adjudicative mindsets, abandon the traditional approach of dissecting composite conduct, evaluate core perpetrating acts within entire black-and-grey industrial chains, distinguish Token-related means-acts from core purpose-acts of traffic manipulation, and ground convictions on core acts inflicting the gravest harm to legal interests. Reasoning for rulings on analogous composite cybercrimes shall be standardized.

4.2 Interpretive Improvement: Promulgate Judicial Interpretations to Clarify Rules for Ascertaining Token-Type Derivative Personal Information

Special judicial interpretations targeting data crimes ought to be promulgated to define independently the legal attributes of Token-type identity credentials. Credentials that enable reverse identification of natural persons via background algorithms shall be categorized as derivative personal information. Identification rules for identity data shall be refined in light of the theory that algorithm-driven identification constitutes the essential feature of personal information. Given the technical trait that a single Token enables actors to repeatedly operate one account and generate hundreds of false interactions, specific thresholds for incrimination based on quantity and circumstances should be formulated.

Pursuant to the 2011 Judicial Interpretation on Criminal Cases Endangering Computer-Information-System Security, illegally obtaining 500 or more sets of identity-authentication information satisfies incrimination thresholds. Yet this standard misaligns with behavioral features of Token-involved cases. Each Token corresponds to identity credentials for one online account. Acquiring one set of Token credentials allows perpetrators to repeatedly operate one account and generate hundreds of false interactions. Retaining the 500-set threshold would require offenders to steal credentials for 500 accounts to satisfy criminal-filing requirements, hampering effective regulation of Token-enabled traffic fraud.

Evaluation rationales for Token-type crimes should therefore shift. Incrimination thresholds should be premised instead on the number of controlled accounts or volumes of false interaction data. A baseline for incrimination could be set at controlling 20 or more accounts or generating over 500 cumulative false-interaction entries. While substantially lower than the 500-set identity-authentication threshold in the 2011

judicial interpretation, this adjustment fits technical characteristics of Token-driven traffic fraud rather than unduly expanding criminal sanction scope. First, the 500-false-interaction threshold draws on existing judicial interpretations: circulating more than 500 reposts of defamatory information qualifies as “serious circumstances”. This reference borrows only its quantitative logic instead of directly adopting the constitutive elements of cyber defamation, as the two provisions protect different legal interests. False comments and traffic interactions follow the same logic as online reposts, so adopting the 500-entry baseline maintains consistency within quantitative frameworks for cyber-information crimes. Second, the 2019 judicial interpretation for the crime of aiding cyber-criminal activities rendering assistance to three or more targets as constituting “serious circumstances”. This confirms that quantitative thresholds for judging cyber black-and-grey industries characterized by limited data yet extensive harms may sit well below 500. Third, the thresholds of controlling 20 or more accounts and generating over 500 cumulative false-interaction entries represent theoretically proposed reference values subject to further verification and adjustment through future judicial practice. These parameters serve as transitional adjudicative rules for closing regulatory gaps under current law and shall later be absorbed as constituent elements of a new specialized crime upon its enactment.

4.3 Legislative Improvement: Enact an Independent Crime of Impairing Online-Traffic Order

Basic positions governing application of criminal-law charges in the digital era shall be clarified [9]. New criminal charges ought to be added prudently. Nevertheless, given that existing crimes cannot fully evaluate conduct of stealing Tokens for volume-boosting and comment-manipulation, introducing a new crime becomes necessary to safeguard platform-related order. Conviction criteria shall be differentiated for upstream, midstream and downstream conduct within black-and-grey industrial chains, with distinct application rules for acts including merely providing technologies to steal Token data, reselling Token identity credentials, and fabricating traffic and evaluations in downstream segments [10].

A new crime of impairing online-traffic order may be added to the Criminal Code. It could be placed either within the section on computer crimes under Chapter VI (Crimes against Social-Administration Order), or within the section on disrupting market-order crimes under Chapter III (Crimes against the Socialist Market-Economic Order). Since this crime primarily infringes upon internet-platform traffic order and online market-competition order, which essentially represent disruptions to market-competition order, locating it within Chapter III on disrupting market-order crimes is preferable.

Regarding statutory penalties, incrimination thresholds shall be established, discarding the prior 500-set identity-authentication threshold. Criminal liability attains where a perpetrator controls 20 or more accounts or generates over 500 false-interaction entries. Whoever, in violation of state provisions, illegally obtains online-identity credentials, manipulates online accounts in bulk, fabricates false interactive data including likes, comments, page-views and transactions, creates fake traffic and online evaluations, and seriously disrupts fair online-market competition and traffic-evaluation order shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and may concurrently or independently be imposed a fine. Where circumstances are especially serious, the perpetrator shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years, together with a fine.

Provisions shall regulate the full industrial chain of traffic fraud across upstream, midstream and downstream segments. Upstream actors who steal credentials and personally engage in volume-boosting shall be subject to joinder-of-offense rules: where this crime coincides with data-related crimes or personal-information-infringement crimes, the heavier penalty shall apply [11]. Upstream actors who only steal and resell credentials shall be convicted of data-related or personal-information-infringement crimes; where perpetrators know full well that stolen credentials will be used for volume-boosting, they may simultaneously constitute accessories to this new crime. Midstream actors who purchase and resell credentials and supply account-controlling tools, knowing that such tools will be deployed for volume-boosting and comment-manipulation, shall be deemed accessories to this new crime. Downstream actors who manipulate accounts to conduct volume-boosting and comment-manipulation are principal offenders of this crime.

Some scholars argue that existing provisions under the *Anti-Unfair-Competition Law* governing false advertising suffice, and administrative penalties render new criminal-law charges unnecessary. However, the *Anti-Unfair-Competition Law* primarily regulates false-promotion acts committed by business operators

themselves. It cannot adapt to independent black-and-grey industrial chains built around stealing Token data for bulk volume-boosting and comment-manipulation. Moreover, traffic-fraud black-and-grey industries exhibit prominent industrialized traits, huge case-related sums and broad victim groups. Administrative penalties remain relatively light, generate limited deterrent effects, and leave perpetrators prone to re-offending. As scholar Jia Yinsheng observes in research on traffic-fraud crimes, such offenses have evolved into complete industrial chains with clear divisions of labor across upstream and downstream links [12]. Specialized criminal provisions are therefore needed to regulate black-and-grey conduct including stealing Tokens and other data, manipulating accounts in bulk to generate false comments, inflate traffic and conduct online comment-manipulation. This fills legislative gaps in criminal-law protection for platform-traffic-competition order and curtails over-reliance on catch-all application of traditional criminal charges.

5. Conclusion

To summarize, judicial dilemmas confronting criminal-law governance over acts of illegally obtaining Token data are threefold: inconsistent determinations of Tokens' legal attributes, resort to traditional charges as fall-backs for new-type crimes, and incomplete evaluation of front-end and back-end conduct. These problems stem from the lag of existing laws, regulations and traditional unitary adjudicative models behind developments in online-traffic economies and the expansion of digital black-and-grey industrial chains. This paper proposes improvement pathways from three dimensions: optimizing judicial adjudication, refining judicial interpretations, and enacting new independent criminal charges. These proposals aim to better regulate criminal conduct within Token-enabled traffic-fraud black-and-grey industries.

As typical identity credentials on online platforms, Tokens epitomize regulatory challenges shared by diverse identity-related data in the digital age, such as Cookies and device fingerprints. The algorithm-identification reasoning advanced herein may be extended to such comparable scenarios. Cyber black-and-grey industries continuously evolve alongside iterative platform risk-control technologies, with traffic-fraud behavioral patterns growing more covert and more industrialized. Hence criminal-law institutions must keep pace with digital-technological developments, continuously update judicial interpretations governing cyber-data crimes, make timely legislative adjustments when appropriate, precisely crack down on online-traffic black-and-grey industries, and safeguard fair and orderly competition within digital markets.

References

- [1] Peng Chengxin. Reinterpreting the Essential Feature of Personal Information: Algorithmic Identifiability. *Journal of Shanghai Normal University (Philosophy & Social Sciences Edition)*, 2023, 52(3).
- [2] Higher People's Court of Shanghai. Typical Cases of Shanghai Courts Cracking down on New-Type Cybercrimes. (2026-05-28). <https://mp.weixin.qq.com/s/B4WcHxqjdvzWHI7yDyeLA>.
- [3] Criminal Judgment (2021) Hu 0120 Xing Chu No. 828, Fengxian District People's Court of Shanghai Municipality.
- [4] Criminal Judgment (2021) Xiang 0212 Xing Chu No. 149, Lukou District People's Court of Zhuzhou City, Hunan Province.
- [5] Xu Wei. On the Algorithmic-Identification Feature of Personal Information and Its Normative Significance. *Legal Forum*, 2025, 40(6).
- [6] Sun Daocui. Knowledge-Advancement and Theoretical Construction for the Independence of Chinese Cyber-Criminal-Law. *Journal of People's Public Security University of China (Social Sciences Edition)*, 2026, 42(4).
- [7] Liu Xianquan. Research on Improving Criminal-Law Regulation of Data Crimes. *Chinese Criminal Science*, 2022(5): 23.
- [8] Sun Daocui. Judicial Reflections and Legislative Responses to Crimes of Online Unfair Competition. *Journal of South China Normal University (Social Sciences Edition)*, 2019(5).

- [9] Yu Haisong. Basic Positions for Applying the System of Criminal-Law Charges in the Cyber-Era. Legal Forum, 2025, 40(5).
- [10] Owusu-Mensah K, Ansong E D, Adu-Manu K S, et al. A Systematic Review of Frameworks for the Detection and Prevention of Card-Not-Present (CNP) Fraud. Journal of Cyber Security, 2026, 8(1): 33.
- [11] Zhang Mingkai. How to Dealing with Specific Method Mistake. The Fundamental Issues upon Criminal Law Theories. Singapore: Springer Nature Singapore, 2025: 219-247.
- [12] Jia Yinsheng. Research on Core Issues in Criminal-Law Regulation of Traffic-Fraud Crimes. Contemporary Law Review, 2023(2): 88.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights

Copyright for this article is retained by the author (s), with first publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).