Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 9, No. 1, 2026
www.scholink.org/ojs/index.php/elp

Original Paper

Research Review on Criminal Law Interpretation Path Dilemma and System Construction of Data Monopoly

Xiang Wang[1*], Longchang Geng[1] & Mingfang Wang[1]

[1] College of Public Administration, Xinjiang Agricultural University, Urumqi, Xinjiang Uygur Autonomous Region, 830052, China

[*] Corresponding author, Xiang Wang

Received: February 27, 2026 Accepted: April 4, 2026 Online Published: April 8, 2026

doi:10.22158/elp.v9n1p287 URL: http://dx.doi.org/10.22158/elp.v9n1p287

Abstract

The review takes "The Criminal Law Interpretation Path Dilemma and System Construction of Data Monopoly" as the research topic, and sorts out the challenges brought by platform data monopoly to traditional criminal law regulation in the context of the digital economy. The aim of the study is to clarify how criminal law should interpret and apply existing norms to deal with the risk of data monopoly. Through various analytical approaches, this review summarizes the current research status at home and abroad in terms of the definition of data monopoly, the theoretical basis of criminal law protection, and the choice of interpretation paths. The results show that the current research has significant difficulties in areas such as the boundaries of penalability, the tendency of "pocketing" of computer system crimes, and the mechanism of connection between criminal law and punishment, and the criminal law interpretation system is characterized by fragmentation. The review suggests that in the future, a criminal law regulation system centered on the "three rights separation of data" theory and linked to the anti-monopoly law should be constructed to provide a systematic solution for achieving the balance between data security and circulation value by clarifying the differentiated protection paths of data resource ownership rights, processing and usage rights, and product operation rights.

Keywords

Data monopoly, Criminal Law Interpretation, System Construction, Dilemma

1. Introduction

In the global wave of the digital economy, data has become a production factor as important as land, labor, capital and technology, profoundly influencing the way the world economy develops, the way society lives and the way nations compete. The new economic "giants" represented by Internet platform companies, due to their characteristics of "network externalities", "economies of scale", "big data processing", especially their advantages in the possession of huge data resources, data analysis capabilities and the utilization of results, have led to the objective existence of the new economic power of "data monopoly".

In general, the causes of data monopolies are a combination of factors such as technology, economy and system. In terms of technology, platform enterprises can "absorb" large amounts of data and have the ability to control data due to technologies such as algorithms, computing power, and data collection and processing, while restricting "data interoperability" (such as restricting platforms from opening API interfaces) in order to create technical barriers. Economically, the non-competition, scale and network effect of data determine that data is naturally concentrated, and the giants take advantage of the iterative development mechanism of "data - traffic – data" accumulated by a large number of users to "naturally" monopolize data and strengthen themselves. In terms of laws and institutions, data property rights are not clear, anti-monopoly laws do not adapt to the changes in the business models of new data-driven enterprises, and the law has incomplete coordination of departmental supervision, making room for data monopolies. In addition, during the literature search, a major mechanism of building a platform ecosystem data monopoly using data elements, algorithms and technologies was discovered. Although this literature does not provide criminal law explanations for it, it still has high academic value, as shown in Figure 1 below.

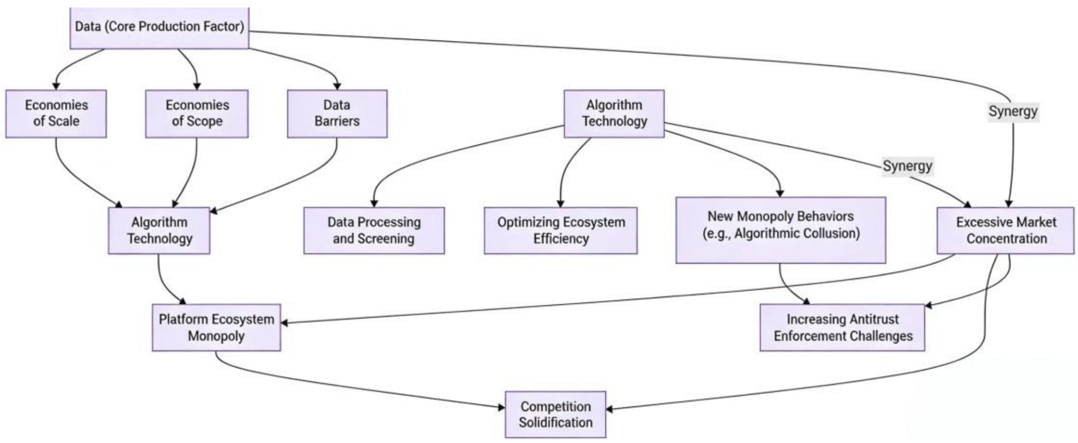

Figure 1. Data and Algorithm Synergy Driving Platform Monopoly Mechanism Diagram

Essentially, this is an inevitable manifestation of capital's pursuit of monopoly profits in the digital age, and behind it, it shows many problems. First of all, this new monopoly shows many characteristics of cross-border, multilateral, data and algorithmic competition, and thus is different from market competition, which may also lead to more serious anti-competitive effects; Secondly, dominant platforms, through the accumulation of data, engage in algorithmic collusion, data dumping, self-favoring, price discrimination, and other serious distortions of the market, harm of consumer interests, and affect innovation; In addition, platform companies engage in covert competition through algorithmic “black boxes”, restrictions on data intercommunication, traffic hijacking, etc., which may not only distort the market competition order, harm consumer welfare, challenge fairness and justice, but also endanger national security and public interests. Therefore, it is particularly important for criminal law to intervene. To better demonstrate the necessity of criminal law intervention, the review has produced the following figure.

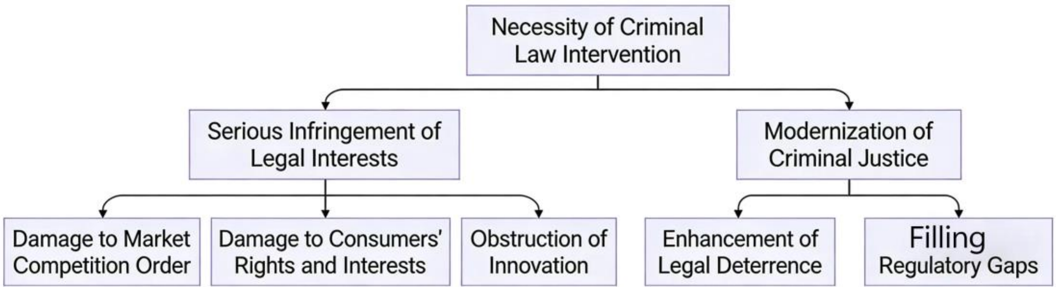

Figure 2. Manifestation of the Necessity of Criminal Law Intervention in Data Monopoly

Since criminal law intervention is so necessary, how to interpret criminal law has also become a major problem for us. This review also focuses on this, integrating existing research at home and abroad, and proposes to construct a framework of the “three rights separation of data” criminal law regulation system.

2. Research Background and Significance

2.1 Research Background

Entering the digital economy era, data, as a new factor of production, has given rise to a new phenomenon of market power - data monopoly. It is the result of the combined effect of multiple factors such as technology, economy and system: platform enterprises use technologies such as algorithms and data processing to obtain the active accumulation of data resources, while the lack of competitiveness, scale benefits and networking of data leads to the natural aggregation of data resources towards leading enterprises, eventually resulting in the phenomenon of “data siphoning”; The lack of clear definition of data rights and the lag of anti-monopoly rules and systems also provide fertile ground for the existence and development of data monopolies.

At present, in the face of this problem, China’s laws and regulations such as the “Data Security Law” and the “Personal Information Protection Law” have made specific and relatively comprehensive provisions for data monopoly behaviors, but there are difficulties in criminal regulation. The characteristics of data monopoly, such as secrecy and technicality, are in conflict with the thinking of infringement of legal interests in traditional criminal law, and it is difficult to determine the boundaries of criminal penalties for data monopoly. In addition, the lack of specific charges in judicial practice reflects the limited ability of criminal law to deal with new types of data monopoly behaviors by “pocketing” the charges of computer system crimes. The connection between anti-monopoly administrative law enforcement and criminal justice is also difficult to handle many cases that seriously infringe upon public interests.

This regulatory dilemma highlights the urgency of innovating the path of criminal law interpretation. It is necessary to explore criminal law interpretation theories that adapt to the characteristics of data monopoly while adhering to the principle of legality of crimes and punishments, balance data security and innovative development, and build a scientific criminal law regulation system to provide a solid legal guarantee for the development of the digital economy.

2.2 Research Significance

2.2.1 Theoretical Significance

The review of the criminal law interpretation of data monopoly in this study is of great significance for enriching and expanding the basic theory of criminal law and promoting the modernization transformation of the development of law.

On the one hand, it expands the territory of criminal law hermeneutics and forces hermeneutic methods to adapt to the data age; The traditional methods of criminal law interpretation focus on the subjective literal meaning of the legislative intent, while the development of data technology makes facts in the data age likely to change dramatically, and the static interpretation methods in law cannot cope with the emerging problems; The objective interpretation attitude holds that the law should be regarded as rational text in the current context, and that the gaps in the legal provisions can be filled through the interpretation of the purpose and system of the legal provisions, which can choose a more flexible conceptual framework for the judgment of the penability of data monopolies.

On the other hand, this review promotes interdisciplinary integration, grafting and fusing monopoly theory in economics, data technology in data science, and legal principles to help people gain a deeper understanding of the truth of data monopoly. For example, the introduction of the concept of data stratification supplements and develops the concept of legal interest in criminal law, explains the divergence between formal protection and substantive protection, and brings new insights to the rapid formation of a dynamic protection system for information protection that balances data security and sharing in China.

2.2.2 Practical Significance

This review is highly instructive for judicial practice, legislative policy and society.

First of all, it guides judicial practice and helps judges, prosecutors and other judges to correctly grasp the interpretation context when reviewing cases involving monopolistic data. For example, when determining that a platform monopolizes through algorithmic black boxes or data blockades, the objective interpretive thinking in this review can guide judges to look beyond the technical surface, discover the actual harm, prevent the “pocket” understanding of computer system crimes, promote fairness and uniformity in adjudication, and enhance judicial credibility.

Secondly, it helps the legislature to revise and improve criminal regulations for punishing monopolistic data. By reflecting the drawbacks of the connection between anti-monopoly law and criminal law, it suggests more detailed charges, clear standards for the connection between criminal and administrative sanctions, and a more long-term and operational approach to criminal sanctions, providing a reference point for the supporting provisions of the Data Security Law of the People’s Republic of China.

Finally, it helps the management to correct the flawed data governance ecosystem and effectively promote the prosperity of the data market. By balancing regulation of data monopolies with technological innovation, it warns enterprises to avoid abuse while ensuring a fair environment for data circulation, thereby promoting the prosperity of the digital economy, safeguarding consumer rights and public interests, and providing a solid legal guarantee for the construction of Digital China.

3. Domestic Research Trends: From Data Monopoly to Integrated Logical Framework in Criminal Law Interpretation

3.1 Conceptual Definition and Controversies of Data Monopoly

3.1.1 Theoretical Controversy on Data Non-exclusivity and Monopoly Possibility

There are different opinions in the academic community regarding the theoretical controversy over data non-exclusivity and monopoly. Hu Jiye (2021) argues that although data is non-exclusive and enterprises cannot exclusively possess data at the physical level, large platforms can monopolize data sources through forms such as “choose one of the two”, forming a de facto monopoly (Hu, J. Y., 2021, pp. 88-91) of data. Cheng et al. (2023) further proposed that by virtue of network externalities and technological monopoly exclusivity, the aggregation of databases is inevitable, and this kind of monopoly is of the technological type, transcending the exclusivity (Cheng, E. F., & Yu, X. S., 2023, pp. 76-83) of property rights. Li Yongjian (2021) proposed the stratification theory of data, suggesting that data monopoly has two levels: data volume monopoly and data accommodation data monopoly. The lack of encryption and sharing enables the platform to overcome the non-exclusivity of data, monopolize the volume (Li, Y. J., 2021, pp. 56-66) of data, and data exists in both static and dynamic stages. Cheng Na et al. (2025), from the perspective of capital logic, pointed out that the increasing returns on the scale of data elements generate networked mutually reinforcing data characteristics, and the data accumulation of technology-advantage-dominant companies changes the market competition pattern, which is also a monopoly imposed on data and has dynamic characteristics (Cheng, N., & Yang, J. Y., 2025, pp. 14-24). The opposing view is reflected in the article “Political Economy Analysis of Data Monopoly and Anti-Monopoly”, which holds that the non-exclusivity of data determines that data cannot be monopolized by one entity, acknowledges that the technical means of data may give rise to monopolies at certain stages, and it is up to the government to achieve social equilibrium (Lin, D., & Li, J. J., 2022, pp. 29-38) of data. Mei et al. (2021) hold a compromise view that the controversy over data monopoly is actually formed by the traditional anti-monopoly theory not adapting to the nature of data, and advocate adjusting the standards of welfare measurement to cope with the changes (Mei, X. Y., & Wang, J., 2021, pp. 94-103) in the nature of the data economy. Song et al. (2023) used Marxist monopoly theory to explain that data monopoly is the product of the profit-seeking nature of capital itself, and that the emergence of data monopoly has dual realistic conditions (Song, D. L., & Tian, G. H., 2023, pp. 104-114) of technology and market structure.

3.1.2 Path Analysis of Data Monopoly through Technical Means

How does technology achieve data monopoly? Li et al. (2021), taking the restriction of data interoperability as an example, pointed out that the exclusive monopolistic behaviors of market leaders, such as blocking API interfaces and prohibiting compatibility of data formats, aim to technically block data, not only blocking data but also depriding the market of new innovation momentum (Li, F. T., He, Y. J., & Guo, D. Y., 2021, pp. 43-49). Xu et al. (2022) explore from the perspective of the attention economy how platforms use algorithms to control users' attention, converting users' personal attention costs into digital lock costs. The technical path of traffic monopoly has the "undetectable" covert characteristics and is difficult for users to recognize the technical content and harm (Xu, X. Y., & Yang, D., 2022, pp. 20-31) fulness. Meng Xiaofeng (2020) pointed out that the aggregative nature of data-intensive technologies themselves leads to models such as machine learning requiring large-scale data input when applied to obtain reasonable results, and the aggregative nature promotes the aggregation of data towards enterprises (Meng, X. F., 2020, pp. 58-61) with data technology advantages. Zhan Fujing (2020) also took the EU Amazon case and others as examples to examine how technology-advantaging enterprises can turn the data they hold into a dominant position in the market, which is manifested as typical characteristics (Zhan, F. J., 2020, pp. 138-152) of the technical path of data monopoly such as data collection concealment and data analysis concealment. Ma Pingchuan (2025) proposed that platform enterprises use technology to build "digital cages", making data monopoly not only an economic issue, but also a structural problem that platforms bind to digital social governance (Ma, P. C., 2025, pp. 46-56).

3.1.3 Data Monopoly Stratification Theory

Regarding the research on the stratification theory of data monopoly, Sun Fangjiang (2021) further evolved the stratification theory into a three-level stratification theory. Besides the monopoly of data elements, there are also monopolies of data channels and data value, which reflect that platforms monopolize data sources and market prices, forming a theoretical framework (Sun, F. J., 2021, pp. 28-38) for the monopoly of the entire data process. For the analysis of the applicability of the stratification theory, Chen et al. (2024) explained from the perspectives of fair competition and equal use that data volume monopoly mainly undermines the efficiency of market competition, while data-based monopoly directly infringes upon the fair distribution (Chen, B., & Zhang, T. R., 2024, pp. 51-66) of data; Han Shipeng (2024), from the perspective of "three rights separation", believes that data volume monopoly is essentially the abuse of data resource holding rights, while data-based monopoly is reflected in the abuse of data processing and usage rights and the alienation of data product operation rights, and different legal regulatory countermeasures (Han, S. P., 2024, pp. 150-159) need to be adopted. An empirical analysis by Tang et al. (2025) shows that the prohibition of data business imitation in the EU's Digital Markets Act reflects the level of monopoly based on data, demonstrating the legislative guidance (Tang, Y. J., & Yu, J. Y., & Tang, C. H., 2025, pp. 5-22) of the stratification theory. Ren Chao (2020), however, from the perspective of the intervention level of anti-monopoly law, shows that monopolies of data volume apply structuralist regulatory means, and monopolies based on data are appropriate behaviorist regulatory means. The contractionary approach is a methodological revelation (Ren, C., 2020, pp. 123-132) of the implementation level of the stratification theory.

3.2 Theoretical Foundations of Criminal Law Protection for Data Monopoly

3.2.1 Criminal Legal Positioning of Data Security Interests

Regarding the criminal law positioning of data security interests, Wang Yinghui et al. (2025) focused on the risk classification and grading system in Articles 21 and 22 of the aforementioned "Data Security Law of the People's Republic of China", and proposed to construct a criminalization and conviction model oriented towards preventing data risks, using security issues as a transitional node (Wang, Y. H., & Xu, X. M., 2025, pp. 162-169) connecting "risk society" and "criminal law". Li Huaisheng (2023) proposed from the perspective of the entire life cycle of data that criminal law should establish a protective position in the value balance of data sharing and security, ensuring both static data security and dynamic security risks (Li, H. S., 2023, pp. 74-85) in the process of data flow. Zhang Ting (2022) pointed out that data security already has the realistic basis for the legal interest of criminal law, but there is a significant gap between the current dual protection model and the generational shift of data crime, and a three-dimensional protection system (Zhang, T., 2022, pp. 121-128) that spans the physical layer, network layer, and application layer needs to be reconstructed. Regarding the divergence between formal and substantive protection of data, Lin Yujia (2024) reveals that this divergence is the root cause of the difficulty in identifying data crimes and advocates for legislative adjustment to construct a "one main line and multiple sub-lines" crime name system. The main line reflects the contemporary demand for data sharing and flow, while the sub-lines radiate the protection space for the multiple attributes of data (Lin, Y. J., 2024, pp. 15-28). Liu Shuangyang (2025) suggested that criminal law should shift from bulk criminalization to individual criminalization for unfair competition in commercial data, and add crimes of infringing upon commercial data to make up for the insufficiency of qualitative legislation in criminal law in the current digital age (Liu, S. Y., 2025, pp. 78-91). Qin Xuenna (2023) reflects on the choice of legal sources and suggests that legislation on cyber data crimes should no longer follow a single codification path, but should gradually move towards interactive and diverse legal sources to adapt to the judicial reality of specialized crimes (Qin, X. N., 2024, pp. 140-147).

3.2.2 Disputes between Data Form Protection and Substantive Protection

As for the dispute between the formal protection of data and the substantive protection of data, Liu Xianquan (2022) found when discussing computer system crimes that the formal protection of data in criminal law is also inappropriate. The "pocket-like" classification of "data crimes" into the crime of destroying computer information systems neglects the independent protection demand (Liu, X. Q., 2022, pp. 67-78) for the substantive value of data. The article "Comparative Investigation and System Construction of Criminal Protection of Data" presents the experience of Germany's dual protection approach, that is, the differentiated protection approach of personality rights protection for personal data and property rights protection for non-personal data can be used (Wang, H. W., 2021, pp. 135-151) to reconcile the differences between formal protection and substantive protection of data. Cheng et al. (2022) analyzed from the perspective of platform governance that formal protection of data cannot counter the substantive monopoly of data by platforms in the form of algorithmic black boxes. To penetrate and interfere in the flow of data, it is necessary to see the power of data behind the data (Cheng, X. J., & Hou, S. Q., 2023, pp. 2-18). The data sharing approach proposed by Sun et al. (2023) is an operational method to reduce the divergence between the two, arguing that data form protection provides the technical dimension for data sharing and data substance protection provides the legal interest dimension for data sharing, and the two constitute the dimensions for governing data monopolies (Sun, H. T., & Zhou, Q. Q., 2023, pp. 131-139). Yang Yuxiao (2023) warns from the perspective of algorithmic governance: "Overemphasizing the true protection of data is a mismatch between criminal law and technological development. The relationship between true protection and technological innovation should be adjusted through criminal compliance in criminal law" (Yang, Y. X., 2023, pp. 86-94). Zheng Linghan (Zheng, L. H., & Hao, M. L., 2023, pp. 77-86) et al. (2023) put forward the concept of data sovereignty, arguing that formal protection points to the technical sovereignty of data and substantive protection points to the value sovereignty of data, and the divergence between the two needs to be addressed in the context of China's data security.

3.2.3 Criminal Law Responses to Data Lifecycle Security Risks

Regarding the criminal response to security risks throughout the data lifecycle, Li Huaisheng (2023) constructed the theory of dynamic protection throughout the data lifecycle, arguing that criminal protection of data should not remain at the static protection stage, but rather incorporate different risks throughout the entire lifecycle of data collection, storage, use, transmission, destruction, etc., into criminal protection. Particular attention should be paid to determining the protection stance (Li, H. S., 2023, pp. 74-85) in the process of balancing data sharing and security. This view is further developed in "Disagreements and Solutions on the Path of Data Criminal Law Protection", where Lin Yujia (2024) points out that there are significant differences between formal protection and substantive protection requirements at different stages of the data lifecycle, and legislation needs to achieve precise responses (Lin, Y. J., 2024, pp. 15-28) through the design of a "one main line and multiple sub-lines" charge system. Wang et al. (2025) proposed from the perspective of risk prevention that a stepwise criminal law regulation intensity (Wang, Y. H., & Xu, X. M., 2025, pp. 162-169) matching the risk level of the data life cycle should be constructed based on the classification and grading system established by the Data Security Law of the People's Republic of China. At the technical implementation level, Liu Shuangyang (2025) focuses on the commercial data circulation link and advocates filling the criminal law protection gap in the data transaction process by adding specific charges to provide institutional guarantee for the dynamic security of data (Liu, S. Y., 2025, pp. 78-91). In terms of governance framework, "Research on the Problem of Data Monopoly in Internet Platform Enterprises" advocates for an agile and collaborative governance model for responding to security risks throughout the data lifecycle, and for coordinating governments at all levels, industries and enterprises to achieve full-process prevention and control of data risks (Zhang, F., & Zhu, T. Y., 2022, pp. 69-79).

3.3 Position Selection in Criminal Law Interpretation Approaches

3.3.1 The Standoff between Subjective Interpretation and Objective Interpretation

Regarding the position dispute between subjective interpretation and objective interpretation, Lu Yimin (2022) discussed the direction of criminal law interpretation in the Internet age. Objectively speaking, these two interpretation positions cannot be directly used as "interpretation methods", but rather determine the goals and directions of interpretation. Among them, subjective interpretation emphasizes seeking the original intention of the legislator, while objective interpretation focuses on the reasonable implications of the current legal context. Objectively speaking, it is one interpretation, and the other interpretation is the meta-theoretical framework of subjective interpretation, such as the interpretation (Lu, Y. M., 2022, pp. 101-120) of subjective intent. The article "Comparative Investigation and System Construction of Criminal Law Protection of Data" reveals through the comparison of German experience that subjective interpretation has the advantage of historical continuity in the field of personal data protection, while objective interpretation is more suitable for the regulatory requirements of non-personal data circulation. This binary position choice model provides a comparative law reference (Wang, H. W., 2021, pp. 135-151) for criminal law regulation of data monopolies. Li Huaisheng (2023) approaches from the perspective of the entire life cycle of data, arguing that subjective interpretation is difficult to cover the dynamic security risks of data and advocating the use of an objective interpretation position to construct an open regulatory framework in response to the balancing needs (Li, H. S., 2023, pp. 74-85) of data sharing and security protection. Lin Yujia (2024) pointed out that there are differences in interpretive positions behind the dispute between formal protection and substantive protection of data: "Formal protection is more dependent on subjective literal interpretation, while substantive protection is more dependent on objective purpose interpretation. The correct combination of formal protection and substantive protection requires legislation and cannot be achieved by interpretive techniques" (Lin, Y. J., 2024, pp. 15-28).

3.3.2 Application Logic of Objective Interpretation of Criminal Law in the Network Era

In the logic of the application of objective interpretation of criminal law in the Internet age, Lu Yimin (2022) systematically expounds the logic of the application of the theory of objective interpretation of criminal law in the Internet age (data crime age), arguing that it is to abandon subjective literal interpretation and move towards the starting point of objective literal interpretation, and to understand and rationally interpret legal concepts in the context of current technological conditions. This conforms to the need (Lu, Y. M., 2022, pp. 101-120) for "normative application issues" in the context of rapidly developing data elements. Yuan Hao (2020) pointed out that the function of criminal law in the digital economy era should shift from "punishment law" to "regulation law", and the change from the function of criminal law requires a dynamic and objective logic for the implementation of criminal law interpretation to meet the new social risks (Yuan, H., 2020, pp. 81-91) caused by data monopoly. Dai Qiuyan (2023), Anti-monopoly Research on the abuse of user Agreement behavior, also presupsets the necessity of objective interpretation logic for the problem of platform data monopoly in practice, that is, to view the “imbalance (Dai, Q. Y., 2023, pp. 89-101) of rights” behind “apparent equality” through substantive interpretation.

3.4 Practical Dilemmas in Criminal Regulation of Data Monopoly

3.4.1 Concealed Characteristics of Platform Data Monopoly Behavior

Regarding the concealment of platform data monopoly behavior, Zhong Ying (2025) argues that digital platforms build “digital prisons” through technology, hiding monopolies in the daily process of data interaction, making it difficult for anti-monopoly “toothknives” to be used for identification and evidence (Zhong, Y., 2025, pp. 1-17) collection. Zhang Yong et al. (2025) pointed out three hidden points of platform data monopolies: weakening users’ awareness through default checks and other means in the data collection stage, masking data rights through various agreements in the data property stage, and concealing the authenticity of monopolies through opaque technologies in the data utilization stage (Zhang, Y., & Li, Z. Y., 2025, pp. 50-60). Wang Qun (2023) adds from the perspective of the attention economy that the platform precisely manipulates the distribution of users’ attention through algorithms, concealing monopolistic behavior under the guise of personalized services and creating a “boiling frog in warm water” type of gradual (Wang, Q., 2023, pp. 36-45) monopoly effect. Ma Tianyi (2025) particularly emphasizes the “two-sided” nature of platform monopolistic behavior. Its positive externalities (such (Ma, T. Y., 2025, pp. 169-180) as reducing transaction costs) often mask the negative externalities of data monopolies, which pose a special challenge to criminal regulation under the guise of legality.

3.4.2 Regulatory Gaps in the Alignment between Antitrust Law and Criminal Law

Regarding the “blank gap” in the connection between anti-monopoly law and criminal law, Li Qi et al. (2023) started with the behavior of data processors using user agreements and found that the anti-monopoly law’s criteria for determining the dominant market position of data platforms and the criminal law’s evaluation criteria for “serious social harm” are “sinkholes”, Platform data monopoly behavior is generally difficult to prove that the platform abuse is malicious and thus escape punishment (Li, Q., & Su, Z. L., 2023, pp. 108-118). Su Sangni et al. (2025) argued that the “separation” of data resource ownership rights, processing and usage rights, and product operation rights led to the error of the protected objects of anti-monopoly law and criminal law. Anti-monopoly law emphasizes protection in terms of market competition order, while criminal law should address it as “damage to specific rights”. The difference in the protection purposes of the two led to a gap in legal connection (Su, S. N., & Shi, J. H., 2025, pp. 71-80). From the perspective of commercial data, He Qun (2024) found that the anti-unfair competition Law and the Criminal Law have differences in the determination of the illegality of commercial data-related acts such as data capture. The Anti-unfair Competition Law emphasizes the disruption of the market competition order, while the Criminal law requires proof of actual damage results. This difference in proof results creates a “gap” in the legal connection (He, Q., & Lin, J. T., 2024, pp. 70-78). Nie et al. (2021) also pointed out through their research on restricting data interoperability behavior that the anti-monopoly law categorization of abuse of dominant market position does not (Nie, H. T., & Han, X. Y., 2021, pp. 93-100) correspond one-to-one with provisions such as "illegal business operations" in the criminal law, and a large number of criminalized data monopoly behaviors can only be subject to administrative penalties. Ma Pingchuan (2022) believes (Ma, P. C., 2023, pp. 98-110) that the bilateral market nature of platform data monopolies causes the relevant market determination methods in anti-monopoly law to deviate from the temporal and spatial scope determination of infringement of legal interests in criminal law, and this technical error brings difficulties in the connection of departmental laws.

4. International Research Trends

The current international academic research on data monopoly is showing a multi-dimensional deepening trend. European and American scholars generally focus on the disruptive impact of data monopolies on the market competition pattern. Research shows that platform enterprises form "data barriers" by controlling user data, significantly raising the market entry threshold. For example, Hiyi Z et al. pointed out through empirical analysis that the information spillover effect would intensify the degree of monopoly in the product market, and data controllers could achieve implicit monopoly coordination (Hiyi, Z., 2024) through algorithmic collusion. This form of monopoly not only distorts the price mechanism but also harms consumer welfare through personalized pricing strategies, as shown in Figure 3, the concentrated situation in the search engine market is a concrete manifestation of this data monopoly power.

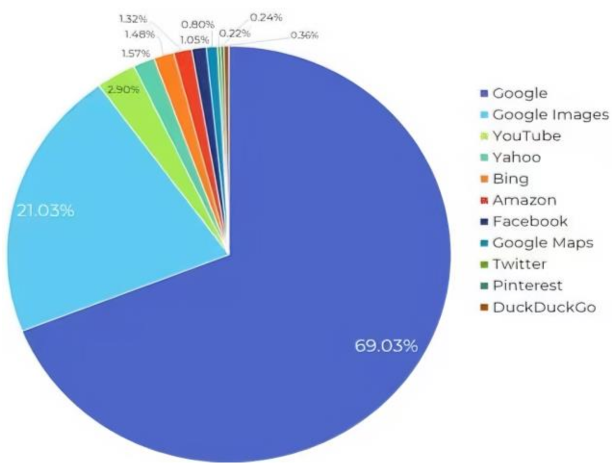

Figure 3. Market Share Distribution of Foreign Search Engines (Hiyi, Z., 2024)

In terms of the overall regulatory path, scholars such as Lu J have focused on the issue of industrial monopoly, recognizing that the control of data infrastructure such as submarine cables can be elevated to a new form of monopoly. Through the analysis of the degree of industrial monopoly, they have concluded the quantitative differences between data monopoly and traditional monopoly, which is a new standard (Lu, J., 2022) for anti-monopoly law enforcement. Foreign scholars pay particular attention to the importance of establishing a sharing mechanism and achieving data sharing, and believe that an industrial data sharing ecosystem as shown in Figure 4 should be established to break the monopoly of industrial enterprise data, make industrial data shared and open, and be conveniently controllable through interfaces. There is no relevant research on the intervention and interpretation of criminal law, which can serve as an inspiration and, depending on the circumstances, combine these relevant foreign viewpoints for research.

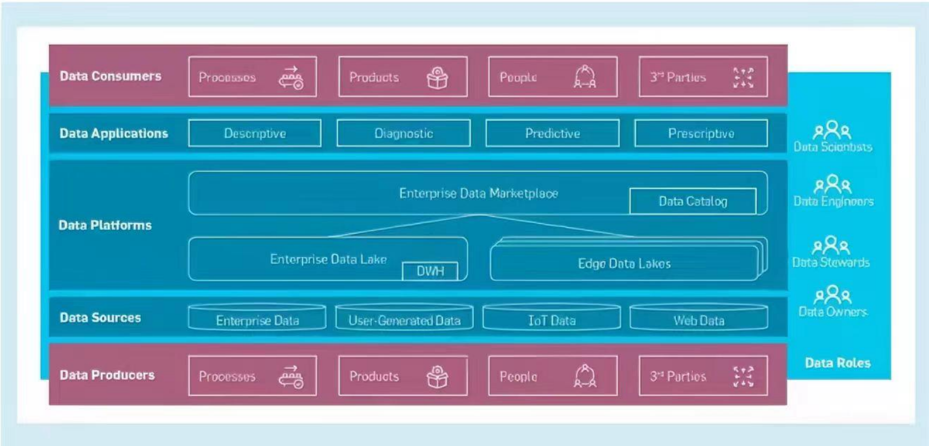

Figure 4. Schematic Diagram of Data Sharing Ecosystem Established By Foreign Industrial Enterprises to Address Data Monopolies (Hiyi, Z., 2024)

5. Review of Domestic and International Research Status

5.1 Theoretical Controversial Focus: No Consensus Has Been Reached On the Penalty Boundaries for Data Monopolies

There have been significant advancements in the interpretation paths of data monopolies in criminal law: theoretically, there are theories such as the stratification of data and the protection of the entire life cycle; technically, there are new monopoly formation paths such as the black box of algorithms and traffic; at the regulatory level, there are theories on the application of subjective and objective "interpretive positions", and the main disputes are centered on the boundary of penability: Whether the penalability of data monopolies is aimed at disrupting the market competition order, or bounded by generating specific consequences that harm legal interests, or by another independent standard similar to risk prevention, the debate has not yet formed a convincing opinion. The fundamental differences have led to three research deficiencies: The first is the inadequate demonstration of the compatibility between the various monopolistic forms (algorithmic collusion, etc.) strongly expressed by current technology and the natural elements of criminal law, and the simple application of technical content to constitute a judgment of criminal facts is a mechanical approach; The second is the ambiguity of the boundary between criminal and administrative law enforcement, especially after the amendment of the Anti-Monopoly Law of the

People's Republic of China introduced a special chapter on digital markets, which could not be well connected with criminal law, and the "gatekeeper" obligation or competition obligation of the platform did not explicitly lead to criminal measures. The third is the confusion of methodological approaches from various disciplines, the lack of effective application of data rights technology methods from the computer discipline, network effect theory from the economics discipline, and legal interpretation methods, and the lack of quantitative support for measuring the social harm of data monopolies. What's more serious is that the criminal law challenge raised by the "three rights separation" reform of data property rights has not been well addressed, nor can it explain the different calculation weights of the right to hold data resources, the right to process and use, and the right to operate data products at the level of criminal law illegality, which will restrict the progress of research on the criminal law protection of the data element market.

5.2 Methodological Limitations: Existing Studies Predominantly Remain At the Normative Analysis Level, Lacking Empirical Support

The current research shows a clear structural imbalance at the methodological level of criminal law interpretation for data monopoly: normative analysis takes an absolute dominant position, while empirical research is severely lacking. Although scholars have designed stratified theories and life-cycle protection theories based on self-deduction, they talk about both subjective and objective positions in the criminal interpretation of data monopoly. But these analyses are largely based on the accumulation of literature and logical thinking, lacking evidence such as statistical data of various judicial decisions and analyses of platform behavior. The research with the characteristics of "emphasizing norms over empirical evidence" reveals three problems: First, the understanding of the invisibility of data monopolies is still limited to the conceptual stage in the literature, and the causes and actual harms of various platform monopolies are not examined through technical methods (such as algorithm auditing, data traffic analysis, etc.); Second, there is a lack of empirical research on the "pocket-like" nature of the judiciary of computer system crimes, and it is not clear how effective the expansion of explanations is for "data crimes". Third, the "gap" in the connection between China's anti-monopoly law and criminal law is only demonstrated through the analysis of the provisions in the literature, without considering the current situation of departmental law conflicts in specific case studies and their manifestations in judicial practice. In particular, existing research rarely uses econometric methods to measure the market distortion effects of data monopolies, nor does it establish a causal model between criminal acts and damage results, resulting in a lack of objective standards for criminal illegality judgments. This weak empirical basis directly restricts the practical transformation of theoretical results - when legislators attempt to translate the data stratification theory into specific criminal norms, it is often difficult to determine a reasonable penalty gradient due to the lack of quantifiable indicators of harmfulness. Future research urgently needs empirical methods such as experimental jurisprudence and judicial big data analysis to provide more persuasive empirical evidence for criminal law interpretation paths by building databases of data monopoly behaviors and conducting in-depth analysis of platform monopoly cases.

5.3 Lack of Systematization: Ineffective Integration between Criminal Law Interpretation Approaches and Antitrust Regulatory Frameworks

At present, there is a significant lack of systematic research on the criminal law regulation of data monopoly in the relevant research results. For instance, the “interpretation space” of criminal law and the penalties of anti-monopoly law lack systematization. Although the research has considerable room for improvement on fundamental issues such as data stratification and technological monopolies, it lacks solutions to value conflicts and “technological barriers” among departmental laws: First, antitrust law emphasizes the efficiency advantage of overall market competition, and the corresponding criminal law’s protection of data security interests lacks a relatively clear hierarchy. As a result, the analysis of the “administrative violation” and “criminal illegality” of the same data monopoly behavior is broken; Second, the relevant market concepts, monopoly position judgments and other technical contents in the anti-monopoly analysis are difficult to be transformed into practical behavioral forms that can be used in the “criminal law interpretation”, leaving the problem of “criminal law regulating data monopoly intervention in the market” and “inability to remedy monopolistic means” unsolved. This lack of systematization specifically gives rise to three problems: First, in the reform of the “three rights separation” of data property rights, the anti-monopoly law focuses on the abuse of the right to hold data resources and the infringement of the right to process and use data protected by criminal law, and there is no set of interconnected evaluation system for the infringement of legal interests; Second, in a series of new antitrust law regulatory tools such as platform gatekeeper obligations, there are no criminal regulatory means of successor law; Third, the economic analysis method in antitrust enforcement and the normative judgment method in criminal law interpretation have not been transformed into mutual communication between each other, especially the data economy characteristics such as network effects and increasing returns to scale have not been effectively absorbed into the judgment method of criminal illegality. The fragmentation of departmental laws weakens the collective performance of governing data monopoly operations and may also lead to a bias in criminal regulation towards the goals and values of market-oriented reforms of data elements.

5.4 Interpretation Path: Constructing the Regulatory Framework of Criminal Law for “Separation of Data Rights, Powers, and Interests”

At present, there is a significant lack of systematic research on the criminal law regulation of data monopoly in the relevant research results. For instance, the “interpretation space” of criminal law and the penalties of anti-monopoly law lack systematization. Although the research has considerable room for improvement on fundamental issues such as data stratification and technological monopolies, it lacks solutions to value conflicts and “technological barriers” among departmental laws: First, antitrust law emphasizes the efficiency advantage of overall market competition, and the corresponding criminal law’s protection of data security interests lacks a relatively clear hierarchy. As a result, the analysis of the “administrative violation” and “criminal illegality” of the same data monopoly behavior is broken; Second, the relevant market concepts, monopoly position judgments and other technical contents in the

anti-monopoly analysis are difficult to be transformed into practical behavioral forms that can be used in the "criminal law interpretation", leaving the problem of "criminal law regulating data monopoly intervention in the market" and "inability to remedy monopolistic means" unsolved. This lack of systematization specifically gives rise to three problems: First, in the reform of the "three rights separation" of data property rights, the anti-monopoly law focuses on the abuse of the right to hold data resources and the infringement of the right to process and use data protected by criminal law, and there is no set of interconnected evaluation system for the infringement of legal interests; Second, in a series of new antitrust law regulatory tools such as platform gatekeeper obligations, there are no criminal regulatory means of successor law; Third, the economic analysis method in antitrust enforcement and the normative judgment method in criminal law interpretation have not been transformed into mutual communication between each other, especially the data economy characteristics such as network effects and increasing returns to scale have not been effectively absorbed into the judgment method of criminal illegality. The fragmentation of departmental laws weakens the collective performance of governing data monopoly operations and may also lead to a bias in criminal regulation towards the goals and values of market-oriented reforms of data elements.

The correct system for the review of this is as follows: Starting from the overall vision of the market-oriented reform of data elements, based on the accurate determination of legal interests, centered on the reasonable construction of constitutive elements, and guaranteed by maintaining the smooth and orderly connection between administrative and criminal law. First, at least at the criminal legislative level, recognize the independent status of the legal interests of the right to hold data resources, the right to process and use data, and the right to operate data products, corresponding respectively to different levels of legal interest objects such as national data security, market competition order, and property interests, to provide a higher-level normative basis for criminal regulation. Second, the constitutive elements of criminal law should take into account the reality of the difficulty in adjudication caused by the change of rights, and adopt a method similar to "substantive interpretation", focusing regulation on the nature and harm of specific rights acts that have not yet become rigid. For example, for the compound monopolistic behavior of platforms controlling both data possession and processing, a comprehensive assessment should be made to determine whether it substantially excludes market competition and hinders technological innovation, rather than mechanically splitting the evaluation of various rights. Finally, the system must be coordinated with pre-laws such as the anti-monopoly law and the data security law. The key lies in establishing a quantifiable set of criteria for assessing social harmfulness, implementing economic implications such as the definition of relevant markets and the determination of market dominance in relevant markets in anti-monopoly analysis as standards for "serious social harmfulness" in criminal law provisions, and also having a tiered legal liability that clearly defines the boundaries between administrative penalties and criminal liability. In particular, some of the principles of the property rights system in the "Twenty Data Articles" should be implemented specifically and transformed into a grid of penalties. Only a dynamic and coordinated framework can help the "three rights separation of data" theory, as a tool of rights theory analysis, truly become a set of specific justifications for limiting data monopolies and handling data security and the value of traffic in criminal rule of law.

6. Conclusion

This review systematically examines potential approaches to interpreting criminal law regarding data monopolies, concluding that as a technological monopoly, data monopolies exhibit characteristics of secrecy, dynamism, and technical complexity that exceed the regulatory scope of traditional criminal law. This necessitates a new interpretive framework for addressing data monopolies. While current research on criminal law for data monopolies has explored foundational theories such as data stratification and lifecycle protection, and acknowledged the importance of objective interpretation to meet digital-era regulatory needs, fundamental limitations remain: First, the legal basis for penalizing data monopolies remains unclear, obscuring their criminal illegality. Second, research methodologies overly emphasize normative analysis without empirical data to quantify the scale of monopolistic harm. Third, a significant disconnect exists between criminal law and antitrust legislation, resulting in administrative-criminal disconnection that hinders coordinated regulation. The review critically evaluates Han Shipeng's proposed differentiated regulatory system approach and proposes a "data tripartite rights separation" framework for criminal law regulation.

References

Chen, B., & Zhang, T. R. (2024). From Clarifying the Prerequisites of Data Monopoly Regulation to Formulating Regulatory Schemes: Fair Competition or Equal Access. *Academic Exchange*, *2024*(02), 51-66.

Cheng, E. F., & Yu, X. S. (2023). Path Analysis of Data Monopoly and Exploitation in the Digital Economy Era. *Theory Monthly*, *2023*(09), 76-83.

Cheng, N., & Yang, J. Y. (2025). Capital Logic and Technological Power in Data Monopoly: Formation Mechanisms and Governance Innovation. *Industrial Technology Economics*, *44*(04), 14-24.

Cheng, X. J., & Hou, S. Q. (2023). Regulatory Dilemmas and Governance Mechanisms of Data Monopoly in Internet Platforms. *E-Government*, *2023*(03), 2-18.

Dai, Q. Y. (2023). Antitrust regulatory measures against data processors' abuse of user agreements. *Law and Business Research*, *40*(06), 89-101.

Han, S. P. (2024). Regulation and Relief of Platform Data Monopoly: An Analysis Based on the Perspective of Separation of Three Powers. *China Science and Technology Forum*, *2024*(03), 150-159.

He, Q., & Lin, J. T. (2024). Criminal Legal Regulation of Data Monopoly Behavior on Online Platforms. *Journal of Nanjing University of Aeronautics and Astronautics (Social Sciences Edition)*, *26*(03), 70-78.

Hiyi, Z. (2024). *Big Data and Anti Monopoly Law Research on Data Monopoly and Market Competition Issues*.

Hu, J. Y. (2021). Antitrust Dilemma of Data Production Factors and Countermeasures. *People's Tribune*, *2021*(19), 88-91.

Li, F. T., He, Y. J., & Guo, D. Y. (2021). Formation Mechanism of Monopoly in the Big Data Field and Antitrust Regulation. *China Certified Public Accountant*, *2021*(08), 43-49.

Li, H. S. (2023). Data lifecycle security risks and their criminal law response pathways. *Journal of Soochow University (Philosophy and Social Sciences Edition)*, *44*(03), 74-85.

Li, Q., & Su, Z. L. (2023). Weapons of digital refugees: Criminal legal regulation of platform digital monopoly. *Changbai Journal*, *2023*(02), 108-118.

Li, Y. J. (2021). Data Monopoly in Internet Platforms: Theoretical Disputes, Governance Practices, and Policy Recommendations. *People's Tribune Academic Frontiers*, *2021*(21), 56-66.

Lin, D., & Li, J. J. (2022). Political Economics Analysis of Data Monopoly and Antitrust. *Fujian Forum (Humanities and Social Sciences Edition)*, *2022*(09), 29-38.

Lin, Y. J. (2024). Disputes and Solutions on Data Criminal Law Protection Paths. *Journal of Shanghai University (Social Sciences Edition)*, *41*(02), 15-28.

Liu, S. Y. (2025). Pathways and Boundaries of Criminal Law Regulation on Unfair Competition Behaviors in Commercial Data during the Digital Economy Era. *Law Forum*, *40*(01), 78-91.

Liu, X. Q. (2022). Reconstruction of Criminal Law Regulation for Computer System Crimes in the "Internet 3.0" Era. *Journal of East China University of Political Science and Law*, *25*(05), 67-78.

Lu, J. (2022). The Copyright Dilemma and Solution for "Data-Driven Creation". *Academic Journal of Humanities & Social Sciences*, *5*(18). https://doi.org/10.25236/AJHSS.2022.051819

Lu, Y. M. (2022). Objective Interpretation Approaches of Criminal Law in the Internet Era. *Journal of National Prosecutors College*, *30*(02), 101-120.

Ma, P. C. (2023). Operational Logic and Legal Regulation of Platform Data Power. *Legal Science (Journal of Northwest University of Political Science and Law)*, *41*(02), 98-110.

Ma, P. C. (2025). Legal Regulation of Platform Data Monopoly. *Zhejiang Social Sciences*, *2025*(03), 46-56.

Ma, T. Y. (2025). Criminal Law Regulation of Algorithmic Risks in the Digital Economy Era. *Journal of Xi'an Jiaotong University (Social Sciences Edition)*, *45*(04), 169-180.

Mei, X. Y., & Wang, J. (2021). Theoretical Response to the Controversy Over the Validity of the "Data Monopoly" Proposition. *Law Forum*, *36*(05), 94-103.

Meng, X. F. (2020). Research on Several Governance Models for Breaking Data Monopoly. *People's Tribune*, *2020*(27), 58-61.

Nie, H. T., & Han, X. Y. (2021). Legal Regulation Dilemmas and Solutions for Data Monopoly in Internet Platforms. *Changbai Journal*, *2021*(04), 93-100.

Qin, X. N. (2024). Three Major Issues in Legislation on Cyber Data Crimes. *Journal of Beijing Institute of Technology (Social Sciences Edition)*, *26*(01), 140-147.

Ren, C. (2020). Theoretical Justification and Path Selection for Big Data Antitrust Law Intervention. *Modern Economic Research*, *2020*(04), 123-132.

Song, D. L., & Tian, G. H. (2023). The Roots, Mechanisms and Governance Strategies of Data Monopoly in Platform Economy. *Journal of Soochow University (Philosophy and Social Sciences Edition)*, *44*(01), 104-114.

Su, S. N., & Shi, J. H. (2025). On the Position, Foundation, and Limits of Criminal Law Regulation on Monopolistic Behavior. *Henan Social Sciences*, *33*(05), 71-80.

Sun, F. J. (2021). Research on Symbiotic Development of Financial Industry and Internet Platforms from the Perspective of Data Monopoly. *Southwest Finance*, *2021*(03), 28-38.

Sun, H. T., & Zhou, Q. Q. (2023). Regulatory Dilemmas and Sharing Mechanisms in Platform Data Monopoly. *Jiangsu Social Sciences*, *2023*(03), 131-139.

Tang, Y. J., & Yu, J. Y., & Tang, C. H. (2025). Innovative Impact of Commercial Imitation Self-Preferential Policies and Antitrust Policies. *Industrial Economics Review*, *16*(04), 5-22.

Wang, H. W. (2021). Comparative Study and System Construction of Data Criminal Law Protection. *Comparative Law Studies*, *2021*(05), 135-151.

Wang, Q. (2023). Criminal Law's Intervention in Internet Platform Monopoly Behavior and Its Boundaries: A Discussion on the Legitimacy of Criminal Liability Provisions in the New Anti-Monopoly Law. *Finance and Economics*, *2023*(05), 36-45.

Wang, Y. H., & Xu, X. M. (2025). On the Construction of a Data Criminal Law Regulatory System: A Case Study of the Provisions in the Data Security Law. *Social Scientist*, *2025*(04), 162-169.

Xu, X. Y., & Yang, D. (2022). Theoretical Framework and Regulatory Approaches for Flow Monopoly. *Economic Theory and Economic Management*, *42*(12), 20-31.

Yang, Y. X. (2023). Research on Criminal Regulatory Approaches to Algorithmic Discrimination in Artificial Intelligence. *Legal Application*, *2023*(04), 86-94.

Yuan, H. (2020). Legal Regulation of Data Monopoly on Internet Platforms from the Perspective of Emerging Rights. *Journal of Northwest Minzu University (Philosophy and Social Sciences Edition)*, *2020*(05), 81-91.

Zhan, F. J. (2020). Antitrust Regulation against Abuse of Dominant Market Position in the Big Data Sector: A Logical Development Based on Path Analysis. *Journal of Shanghai University of Finance and Economics*, *22*(04), 138-152.

Zhang, F., & Zhu, T. Y. (2022). Research on Data Monopoly Issues in Internet Platform Enterprises. *International Economic Cooperation*, *2022*(05), 69-79.

Zhang, T. (2022). Risk Challenges and Conceptual Updates of Data Crimes in the Digital Economy Era: A Case Study of Data-Threat-Based Cyber Black and Gray Industries. *Law Forum*, *37*(05), 121-128.

Zhang, Y., & Li, Z. Y. (2025). Criminal Law Regulation of Algorithmic Monopoly Behavior. *Journal of Nanjing University of Posts and Telecommunications (Social Sciences Edition)*, *27*(01), 50-60.

Zheng, L. H., & Hao, M. L. (2023). Conceptual System and Modeling Research on Data Sovereignty in China. *Library and Information Science*, *2023*(02), 77-86.

Zhong, Y. (2025). Antitrust Regulation of Public Data Authorized Operation. *Comparative Law Studies*, *2025*(06), 1-17.