ISSN: 2688-8653

The Construction and Pathway Concept of Data Legal Benefit Protection System

Kangyuan Li[1, *]

[1]School of Law, Xinjiang University, Urumqi, Xinjiang, 830000, China

[*]Corresponding author: likangyuan@foxmail.com

Abstract

The conventional theories surrounding data legal benefits, whether dependent or independent, exhibit several shortcomings in addressing the complexities of ownership definitions that stem from the intangible and fluid nature of data. This inadequacy may inadvertently result in the inappropriate broadening of criminalization standards. Data legal benefits ought to be recognized as a unique category of legal benefit, characterized by a dualistic nature, where a dynamic interplay exists between intrinsic legal benefits and functional legal benefits. Any infringement upon the core of data could pose a direct threat to the legal benefits tied to the real-world implications of that data. In light of this understanding, I propose a "dual-layer data legal benefit protection framework," which categorizes data legal benefits and establishes tiered protection along with differentiated regulation for personal data, corporate data, and public data.

Keywords

Data crime; Data legal benefits; Criminal law protection.

1. Introduction

In the age of big data, an immense volume of information is perpetually generated, gathered, stored, structured, and leveraged across the internet[1]. Data is emerging as a pivotal production factor, and the centralized storage and analytical application of data not only amplifies its economic and strategic significance but also introduces new challenges in data security. The manifestations of data-related offenses have become increasingly varied, encompassing both unstructured data and violations arising from diverse endpoints. Criminal law was conceived in an era devoid of the internet, and the evolution of contemporary criminal legislation and theories transpired in a pre-digital milieu, complicating the applicability of specific legal concepts to cybercrime. The criminal law, which is designed to safeguard legal interests, cannot afford to overlook the novel forms of cybercrime but must proactively address them[2]. The legal interest in data is progressively evolving into a new category of cybersecurity interest, rendering the safeguarding of network data security a paramount concern for criminal law[3]. As a result, the digital transformation has engendered an urgent necessity for criminal law to protect data-related legal interests, making it imperative to navigate the digital frontiers effectively. Achieving a balance between promoting innovation and upholding regulatory order is not only a critical challenge in the modernization of criminal governance at this juncture but also a vital avenue for refining the legal system with Chinese characteristics.

ISSN: 2688-8653

2. Differentiation Between Data Legal Interests and Traditional Legal Interests

(1) The Doctrine of Dependency of Data Legal Interests

The doctrine of dependency asserts that data legal interests do not constitute an autonomous category of legal interest; rather, they are contingent upon established traditional legal interests, such as personal rights and property rights. The theory surrounding data information legal interests exemplifies this doctrine, positing that data security is fundamentally synonymous with personal information security. This viewpoint is rooted in the philosophical understanding of data information, which posits that "everything can be digitized or informationalized[4]." It suggests that there is no fundamental distinction between data and information. However, this perspective presents significant limitations. Firstly, it reduces data security to merely personal information security, potentially constraining the protective scope for data legal interests and neglecting the safeguarding requirements of non-personal information data, such as operational data from computer systems and corporate data. Secondly, it tends to minimize the significance of protecting broader legal interests. If data security is solely equated with personal information security, the safeguarding of non-personal information data may be overlooked, thereby jeopardizing the integrity of the overall societal information security framework. Lastly, if data security is exclusively interpreted as the protection of personal information content, it becomes increasingly difficult to justify the necessity of establishing specific criminal offenses for other categories of data-related crimes.

The fundamental premise of the theory of data property rights posits that data should be treated as a form of property deserving protection under property security legislation. This viewpoint underscores the economic significance of data, contending that it transcends mere information or code; rather, it represents a product that encapsulates the labor and intellect of its creators and organizers, thereby possessing unique property characteristics. Nevertheless, the implementation of the data property rights theory encounters several obstacles. Firstly, the intrinsic properties of data—its ease of replication, distribution, and alteration—complicate the classification of data as a property object. Legally, this is reflected in the challenges associated with defining "ownership" of data, as the act of copying and sharing can swiftly dilute control, complicating traceability and management. Secondly, this theory risks fostering an excessive criminalization of data access and processing, where any unauthorized interaction with data may be interpreted as a violation of property rights. Finally, the specification of data rights necessitates further elucidation. For data to be fully recognized as property, it is crucial to distinctly outline the allocation of various rights, encompassing ownership, usage, access, and control.

The theory of data order benefits asserts that the core of data security transcends the mere protection of individual information from unauthorized access or destruction; it fundamentally pertains to the preservation of a management order essential for the secure functioning of computer system data and the governance of network security. Nevertheless, the abstract and dynamic characteristics of the theory of data order benefits introduce several challenges. Firstly, the abstract nature of order benefits hampers this theoretical framework's ability to offer precise guidance for the criminalization of specific unlawful acts. The definitions and scope of order benefits lack a cohesive standard, resulting in considerable discrepancies in interpretation and application within academic discourse. Secondly, the theory of data order benefits may lead to the unwarranted broadening of criminalization criteria for data-related offenses. For example, certain online activities that do not directly pertain to data state security, such as the volume of shares or comments, could be interpreted as actions jeopardizing data order, thus constituting a criminal offense. This broadening poses a risk of imposing unnecessary legal constraints on legitimate online activities, increasing the legal risks

ISSN: 2688-8653

encountered by individuals in their routine internet usage, and potentially igniting societal concerns regarding excessive data regulation.

The ongoing academic dialogue regarding the theoretical examination of data legal interests predominantly centers on three key dimensions: dependency, property, and order. Each of these theoretical frameworks presents distinct advantages, yet they also reveal specific shortcomings. The dependency theory reduces data to mere personal information, complicating the comprehensive safeguarding of diverse data security types. Conversely, the property legal interest theory highlights the economic significance of data but encounters various obstacles in defining rights and enforcing them effectively. Meanwhile, the order legal interest theory, while demonstrating a commitment to overarching data security, risks inappropriate extensions of criminal standards due to its abstract nature. In light of this analysis, I assert that, within the digital era, the safeguarding of data legal interests necessitates a multifaceted and integrative strategy. Firstly, it is imperative to recognize that data encompasses multiple attributes, including personal information, economic value, and social order. Secondly, a well-structured protection framework should be developed, utilizing differentiated protection strategies tailored to the unique characteristics of various data types. Lastly, in both legislative and judicial contexts, it is vital to uphold the principle of restraint to prevent the excessive broadening of criminal regulation. By adhering to these principles, we can effectively ensure data security without unduly hindering social progress and technological advancement.

(2) The Doctrine of the Independence of Data Legal Interests

The doctrine of the independence of data legal interests should be recognized as a unique category of legal interest, defined by its specific characteristics and framework. This encompasses both the theory of pluralistic data legal interests and the theory of independent novel data legal interests. The broader theory of pluralistic data legal interests asserts that data legal interests maintain an autonomous position within the criminal law framework; however, their fundamental nature is a synthesis of traditional multiple legal interests, including economic order, property rights protection, personal rights protection, and public order. Conversely, the narrower interpretation of pluralistic data legal interests merges only "personal rights + property rights," indicating that data embodies a dual rights characteristic. Nonetheless, the pluralistic data legal interests theory is not without its limitations. Firstly, it presents a scenario of perceived competition; when data-related offenses simultaneously violate multiple legal interests, the application of criminal law may face challenges in determining which interest to prioritize. For example, if some offenses are linked to lower statutory penalties, existing regulations may be seldom enforced in practice, resulting in the occurrence of "zombie clauses." Secondly, the extensive and varied nature of the content associated with data legal interests—spanning economic order to various dimensions of personal rights—creates ambiguity in the delineation between different legal interests. The practical difficulty of precisely defining and reconciling these pluralistic legal interests remains an area for further investigation. Lastly, this theory does not adequately emphasize the independent status of data legal interests within the realm of criminal law; its core remains a fusion of traditional legal interests, lacking substantial significance.

The theory of independent new data interests asserts that the autonomy of data interests is not merely dictated by their terminology or the varied content they encompass, but is fundamentally shaped by their distinct attributes. The "three security dimensions of data"—confidentiality, integrity, and availability of digital information and systems—constitute a groundbreaking category of legal interest[5]. Nevertheless, in both practical implementation and theoretical delineation, the theory of independent new data interests exhibits certain deficiencies. Firstly, the notion of the "three security dimensions of data" risks misclassifying conventional information security categories, such as personal data protection, national

ISSN: 2688-8653

security, and trade secrets, as matters related to data status security. Secondly, the theory reveals considerable inadequacies in its approach to cybercrime. The existing legal framework finds it challenging to effectively integrate cybercrime—especially offenses that do not directly violate the three security dimensions of data—into the "three security dimensions of data" paradigm, thereby neglecting the inherent connection between cybercrime and data security. Finally, incorporating the security of the content of information entities into the realm of data interests, particularly regarding data that does not disrupt essential system operations, such as publicly accessible information, may incite unwarranted legal intervention, contravening the principle of restraint.

The preceding analysis indicates that both the pluralistic data interest theory and the independent new data interest theory strive to establish a theoretical framework for data protection, yet each encounters unique challenges. The pluralistic data interest theory aims to enhance data security by amalgamating traditional interests; however, this approach may result in ambiguity and inefficiency in legal application. Conversely, the "data triadic security" concept introduced by the independent new data interest theory, despite its innovative nature, still faces significant limitations regarding conceptual clarity and practical execution. I contend that the formulation of a data interest protection system should embrace a more pragmatic methodology.

To begin with, it is of paramount importance to clearly articulate the unique characteristics of data interests, acknowledging their departure from conventional interests while simultaneously recognizing the intricate relationships that exist among them. Moreover, at the legislative level, it is essential to establish a well-defined hierarchy of interest protection to prevent any inappropriate expansion or overlap in the scope of such protections. In addition, within the realm of judicial practice, it is critical to formulate adaptable and effective adjudication standards that ensure robust data security while minimizing unnecessary interference.

Looking forward. the evolution of data interest theory should emphasize the preservation of theoretical independence while also aligning with the pressing demands of the contemporary world. This necessitates moving beyond the limitations imposed by traditional interest theory and thoroughly exploring the complexities inherent in the digital age, thereby creating a data interest protection framework that reflects both theoretical rigor and practical relevance. Furthermore, there is a need for deeper exploration into how to reconcile the interplay between data interests and other competing interests, which would ultimately lead to a more scientifically informed and rational approach to the regulation of data-related offenses.

3. The Judgment and Expansion of Data Legal Benefits

(1) The Duality of Data Legal Benefits

Data does not exist in a vacuum within computer systems; its importance stems from its interconnectedness with real-world interests[6]. The inherent legal advantages of data primarily pertain to its confidentiality, integrity, and availability—qualities that safeguard data from unauthorized access, illicit alterations, or destruction throughout its entire lifecycle. The practical legal advantages of data associate its value with specific legal interests in the real world, thus enhancing its relevance beyond mere numerical collections and linking it to tangible legal rights, such as the right to personal information, property rights, and trade secret protections.

To effectively comprehend the interplay between the intrinsic legal value of data and its functional legal value, it is imperative to acknowledge that infringing actions primarily affect the intrinsic legal value of data, which may subsequently influence its functional legal value. Logically, an infringement on the intrinsic legal value of data indicates that the corresponding

ISSN: 2688-8653

functional legal value could also be jeopardized. Therefore, maintaining the integrity of the intrinsic legal value of data is a critical prerequisite for safeguarding its functional legal value. Any assault on the intrinsic characteristics of data—whether through deletion, modification, or unauthorized access—can pose a direct threat to the real-world legal interests tied to that data. When analyzing and addressing legal challenges related to data, it is essential to consider both the intrinsic and functional legal values to ensure a holistic protection strategy that encompasses not only its technical features but also its associated legal rights. Moreover, the significance of the intrinsic legal interest in data is dependent on the functional legal interests it embodies. If data is devoid of any linkage to real-world legal interests, it possesses minimal legal protective value. Consequently, when evaluating the illegality and detrimental nature of a data infringement, it is inadequate to focus solely on the infringement of the intrinsic value; the repercussions of the action on the functional legal value must also be considered. For example, unauthorized access to national security data, even if it pertains to a minimal amount of information, represents a substantial infringement of legal interests due to its associated functional legal value of "national security."

(2) An Exploration of the Dual-Pathway for the Protection of Data Interests

Some researchers have proposed that our nation's criminal law framework concerning data should embrace a multifaceted strategy, incorporating a parallel crime group model that facilitates the co-regulation of various crime factions Nevertheless, this model does not adequately address the full spectrum of data crimes that violate tangible interests[7]. I argue that the development of a data interest protection framework should prioritize both intrinsic and functional interests, as each possesses distinct characteristics and complexities, thereby establishing a "dual-layer data interest protection framework." It is crucial to examine the interplay between intrinsic and functional offenses within data crimes. The category of intrinsic offenses is primarily focused on safeguarding the security of computer information systems and maintaining the original state and integrity of data, which includes crimes such as unauthorized access, system intrusion, and data destruction. In contrast, the category of functional offenses centers on the protection of traditional rights articulated through data as a medium, encompassing property rights, intellectual property rights, and personal privacy. The substantive damage resulting from data criminal activities constitutes a violation of real-world interests. Unlike the parallel crime group model, which often appears in legal texts as a static categorization, this parallel model inadequately highlights the dynamic interactions and legal conflicts among offenses. The design of the "dual-layer data interest protection framework" transcends mere rigid classifications of offenses; it aims to explore the legal interconnections and dynamic interactions among various offenses. In the adjudication of cases, it facilitates a more holistic evaluation of the multiple offenses that an individual's data actions may concurrently invoke, as well as the legal relationships and conflicts that exist among these offenses.

The "dual-layer data protection framework" is not a static entity; instead, it exhibits a certain level of openness, which arises from its responsiveness to technological innovations and societal transformations. Firstly, as technology advances, the functional relevance of data continually evolves and broadens, resulting in a rise in offenses associated with data functionality. Secondly, the methods of data violations are intricately tied to technological progress, with the iterative nature of technology propelling the persistent growth of functional crimes. In this swiftly evolving technological environment, forecasting new forms of data-related or illicit activities that may emerge through novel technological avenues becomes exceedingly difficult. For example, environmental pollution data offenses, which involve the manipulation or falsification of pollutant emission records, exemplify a type of crime that conventional data crime frameworks struggle to anticipate. Within the context of parallel crime classifications, this emerging category of crime may not be adequately categorized or addressed.

ISSN: 2688-8653

In this regard, the "dual-layer data protection framework" is equipped to swiftly respond to and integrate these new criminal manifestations, showcasing foresight and adaptability in safeguarding data interests against future crime trends.

In summary, when constructing a robust data protection framework, it is essential to simultaneously consider both the intrinsic legal advantages associated with data and the operational legal benefits that arise from its use. This dual focus is crucial for achieving a seamless integration of these elements. A holistic approach necessitates that we not only protect the technical attributes of the data itself but also place significant emphasis on the concrete legal advantages that data can provide. Given the rise of new data-related offenses fueled by rapid technological advancements, the legal protection framework must demonstrate sufficient inclusivity and foresight to effectively address emerging challenges as they develop. Furthermore, in the analysis of specific cases, it is imperative to conduct a thorough assessment of the interplay between intrinsic and operational legal benefits, accurately evaluate the severity of criminal behavior, and ensure that the enforcement of the law is both scientific and rational.

4. The Construction of Criminal Law Protection Paths for Data Legal Interests

(1) The Feasibility of Classifying Data Legal Interests

The ambiguity that often accompanies the concept of data has persistently posed a considerable challenge within various fields. The often indistinct boundary between data and information further complicates the accurate conceptual differentiation of data, particularly in legal frameworks. In light of the inherent characteristics of data, Article 21 of the Data Security Law of the People's Republic of China establishes a comprehensive framework aimed at the classification and tiered protection of data. Within this framework, conducting research on classification can serve as a valuable tool in addressing the categorization of legal interests that are intricately associated with data.

Data, serving as a crucial vessel for information, holds significant legal implications in the context of the information it conveys. For instance, the data extracted from a user's purchasing behaviors on an e-commerce platform can be regarded as a component of personal privacy. However, when this data is aggregated and analyzed by the e-commerce platform, it transforms into a form of commercial intelligence that has the potential to predict consumer behavior, thereby shifting its value to that of a trade secret. The legal attributes of data are not static; they fluctuate based on the specific applications and processing methodologies employed. Furthermore, by systematically categorizing and re-categorizing offenses related to data, we can achieve a more precise assessment of the damage inflicted on legal interests and accurately characterize the nature of crimes based on the particular applications and consequences of the data involved. For example, while both data theft and data misuse involve the unlawful manipulation of data, they differ fundamentally in terms of the severity and nature of the harm they inflict on individual or corporate legal interests. Data theft may directly infringe upon a company's trade secrets and property rights, whereas data misuse may encroach upon an individual's privacy rights and data security.

Typological research acts as a supplementary approach to conventional conceptual classification methods. It differentiates between standard instances of a type and contentious edge cases, with a seamless transition linking one type to another[8]. Through the meticulous application of normative value judgments and legal interpretations, there has not only been a reclassification of data-related criminal activities, but a clearer demarcation of the scope and categories of data crimes has also gradually emerged, elucidating the distinctions between empirical types and normative types. Legal norms, by re-typologizing empirical types, classify

ISSN: 2688-8653

behaviors into specific criminal categories, thereby achieving a more substantive and nuanced protection of data-related legal interests.

(2) Specific Concept of Criminal Law Protection for Data Interests

1. Protection of Personal Data Interests

The Criminal Law of the People's Republic of China delineates the components that constitute the offense of infringing upon citizens' personal information. This encompasses the illicit sale or provision of personal data, the unauthorized transfer or sale of acquired personal information to third parties, as well as the theft or acquisition of personal information through other unlawful means. In examining the legal interests implicated in offenses against personal data, the primary emphasis is placed on the right to personal information self-determination, which entails the capacity for autonomous governance over personal data, fundamentally rooted in informed consent. The right to personal information self-determination comprises three principal dimensions: the prevention of improper collection, disclosure, and misuse of personal information. This framework not only justifies the establishment and amendment of related offenses but also shapes the interpretation of the elements of these crimes and the extent of penalties. The Civil Code of the People's Republic of China and the Personal Information Protection Law mandate that publicly accessible personal information undergo "reasonable processing," signifying that such processing must align with the original intent of information disclosure and must not alter its usage or infringe upon the significant interests of the information subject. The act of rendering personal information public does not equate to a total relinquishment of control over that information. The Criminal Law must ensure the "reasonable processing" of publicly available information to avert its misuse. In instances where personal information is voluntarily disclosed, it suggests that the information subject has, to a certain degree, consented to the processing of their data; however, this does not confer unrestricted rights upon the information processor to utilize that data. In practice, the specific criteria for "reasonable processing" should be assessed across three dimensions: the purpose, method, and outcome of the processing activities. Should the processing exceed this framework or fail to secure renewed authorization and consent from the information subject, it may constitute an infringement of personal information autonomy, thereby contravening relevant legal provisions. Therefore, the regulation of personal data crimes under criminal law not only focuses on preventing the improper acquisition and use of data but also extends to how to balance individual rights with the freedom of information in the processing of publicly available data, ensuring that the legal interests of personal data receive comprehensive and meticulous protection in the information age.

2. Safeguarding Corporate Data Rights

Corporate data transcends a mere collection of raw information; it is a meticulously organized and applicable asset that embodies substantial property characteristics, carefully curated by corporate personnel. In examining the safeguarding of corporate data rights and the violations of data property rights, the emphasis is placed on the property rights linked to corporate data, which encompass data control rights, data development rights, data licensing rights, and data transfer rights. Once corporate data is legally acknowledged as a right, it concurrently acquires the protection of legal enforcement and the recognition of the societal framework, thus offering a sense of security and reasonable anticipation. The establishment of data property rights represents a return on the efforts expended by enterprises in data aggregation and the creation of data products. Disparities in labor investment result in notable variations in the application and property valuation of data products and collections. Through careful selection and integration, raw data is converted into structured and organized derivative data, thereby augmenting its inherent value. The legal framework should align the distribution of rights with the property value of data. For high-value data products, such as derivative data—which is considered a product of human intellectual endeavor—protection should be classified under

ISSN: 2688-8653

intellectual property. The fundamental value of derivative data resides not only in the electromagnetic records or computer code that constitute its medium but also in the informational content it embodies, which can be safeguarded through the establishment of specialized rights such as data exclusivity rights. This innovative category of data property rights can be positioned alongside traditional intellectual property rights, including copyright, patent rights, trademark rights, and trade secret rights.

3. Protection of the Benefits of Public Data Law

The safeguarding of public data interests within the realm of criminal law requires a precise definition of the security management framework for public data.[10] Public data security encompasses both static and dynamic protective measures, which include confidentiality, integrity, availability, controllability, and legitimacy; these components collectively represent the fundamental essence of data security. It is crucial to not only avert external unlawful intrusions, such as data breaches or destruction, but also to guarantee the legality and compliance of data processing practices, thereby preventing misuse or illicit dissemination of data. The criminal implications related to public data have increasingly diverged from conventional computer information system security offenses. The "Data Security Law of the People's Republic of China" and the "Regulations on the Security Management of Network Data (Draft for Comments)" advocate for a security management framework that spans the entire data lifecycle, requiring public management entities to enforce rigorous security protocols at every phase of data collection, storage, and utilization to ensure the efficacy of data security management. In this context, it is essential to establish independent criminal offenses for actions that violate public data, differentiating them from traditional crimes associated with the damage of computer information systems. Drawing from the legislative precedents of the "German Penal Code" and the laws of Taiwan, it is advisable to consider the inclusion of offenses pertaining to the destruction of public data, as well as the unlawful acquisition, provision, and utilization of public data within our criminal law system, thereby creating a comprehensive criminal protection framework. Furthermore, the implementation of a tiered data security protection regulation is recommended, which would delineate varying criminal liabilities based on the security classification and societal impact of public data, thus clarifying the standards for handling data of differing security levels in judicial interpretations, ensuring that legal applications effectively safeguard data interests.

In light of the preceding analysis, the establishment of a criminal protection framework for data interests must be grounded in a precise comprehension of the distinct characteristics associated with personal, corporate, and public data. The safeguarding of personal data interests is fundamentally anchored in the principle of informational self-determination, which underscores the necessity of defining the reasonable use of publicly accessible information. Conversely, the protection of corporate data interests accentuates its proprietary nature, thereby necessitating innovative rights frameworks to ensure adequate safeguarding. Simultaneously, the protection of public data interests is primarily concerned with the maintenance of security management protocols, which calls for the development of an autonomous criminal regulatory system. I contend that enhancing the criminal protection framework for data interests should adhere to the following guiding principles: First, the principle of differentiated protection and treatment must be upheld. A customized protection mechanism should be devised, taking into account the unique characteristics of various data types, thereby ensuring comprehensive protection while preventing redundancy or conflict in the protective scope. Second, a focus on dynamic equilibrium is essential. In the pursuit of data security, it is equally important to consider the efficiency of data circulation and utilization, striking a balance among the interests of all stakeholders to foster the sustainable growth of the digital economy. Third, the legal framework must be strengthened. Through legislative enhancements and judicial clarifications, it is imperative to further delineate the constitutive

ISSN: 2688-8653

elements of pertinent offenses and to elucidate sentencing standards, thereby providing clear directives for judicial application.

5. Conclusion

The typological thinking approach is characterized by a systematic classification analysis that emphasizes the fundamental attributes of various entities. In this context, the diverse categories of legal attributes associated with data necessitate the implementation of corresponding protective measures to uphold data rights effectively. The protection of personal data should be prioritized to ensure the safeguarding of individual rights, while the information security of corporate data must concentrate on the preservation of economic interests. Furthermore, the governance of public data should underscore the significance of maintaining social order and adhering to public ethics. Consequently, the refinement of criminal law standards should be firmly rooted in a comprehensive understanding of the essential elements of data rights. This foundation will provide a normative framework for addressing a wide array of unlawful activities related to data through clear and explicit judicial interpretations. This strategic approach aims to translate the principles of the rule of law into tangible governance outcomes. By establishing a coherent and rational regulatory framework and integrating insights derived from judicial practice, we can progressively enhance the effectiveness of data governance. Ultimately, this will facilitate the modernization of the criminal governance framework concerning data.

References

[1] Liu Feng, Lin D.d: "The Cybersecurity System of the United States," Science Press, 2015, p. 243.

[2] Zhang Mingkai. "Criminal Legislation in the Age of the Internet," China Prosecutor, 2017, (13): 80.

[3] Sun Daochui. "Examination and Prospects of Criminal Law Protection of Big Data Legal Interests," Journal of Central South University (Social Science Edition), 2017, 23(01): 58-64.

[4] Zhang Guihong. "On the Nature of Data and Its Relationship with Information," Philosophical Analysis, 2018, 9(02): 119-132 + 198-199.

[5] Ulrich Beck: "Global Risk Society and Criminal Law in the Information Society," translated by Zhou Zunyou, Jiang Su, et al., China Legal Publishing House, 2012, p. 308.

[6] Zhuang Jing. "Constructing an Open Chinese Data Criminal Law System: Based on the Distinction between Ontological Legal Interests and Functional Legal Interests," Chinese Journal of Criminal Law, 2023, (02): 37-53.

[7] Zhuang Jing. "Constructing an Open Chinese Data Criminal Law System: Based on the Distinction between Ontological Legal Interests and Functional Legal Interests," Chinese Journal of Criminal Law, 2023, (02): 37-53.

[8] Zhang Guihong. "On the Nature of Data and Its Relationship with Information," Philosophical Analysis, 2018, 9(02): 119-132 + 198-199.

[9] See Lin Li: "Legal Methodology and Dworkin," China University of Political Science and Law Press, 2002, p. 127.

[10] See Peng Cheng.X: "Research on Modern Rights Theory: An Analysis Based on 'Will Theory' and 'Interest Theory'," Law Press, 2017, p. 323.