Enterprise Data Governance in the Digital Intelligence Era: Existing Risks and Legal Responses

Authors: Hao Jiajie

Date: 2025-04-07T00:00:00+00:00

Abstract

Enterprise data governance represents a critical component in unlocking data value; however, it is accompanied by frequent risks related to data security, data compliance, and data monopoly, which highlight deep-seated causes such as outdated legal norms, overly formalistic regulatory frameworks, and unfair competition in data markets. In essence, data security constitutes the foundation of data compliance, while data compliance serves as a bulwark against data monopoly, making it particularly crucial to strike a balance between promoting data circulation and preventing data risks. Accordingly, enterprise data governance must achieve systematic coordination across three levels—formulation, implementation, and guarantee—with each level emphasizing distinct adaptation approaches. At the formulation level, basic principles and requirements for data governance are established through the alignment of legal norms with data standards. At the implementation level, legal norms are refined into actionable operational rules and processes to ensure concrete execution of governance requirements. At the guarantee level, continuous optimization and support for effective rule implementation are provided through multi-stakeholder governance encompassing government oversight, industry self-regulation, and social supervision. The foregoing aims to provide enterprises with systematic, comprehensive, and dynamically adaptable legal responses in the digital-intelligence era and market competition.

Full Text

Existing Risks and Legal Responses to Enterprise Data Governance in the Digital Age

Author: Hao Jiajie, PhD Candidate, Jinan University Law School & Intellectual Property School; Research Fellow, International Digital Trade Law Institute and International Law Research Center (Provincial Level), Foreign-Related

Rule of Law Research Center (National Level), Northwest University of Political Science and Law. Research interests: Digital Law, International Economic Law.

Abstract: Enterprise data governance is the critical link for unlocking data value, yet it is accompanied by frequent risks such as data security, data compliance, and data monopoly, which highlight deeper issues including outdated legal norms, overly formalistic regulatory frameworks, and unfair competition in data markets. Fundamentally, data security forms the foundation for data compliance, which in turn serves as the defense line against data monopoly. Moreover, striking a balance between promoting data circulation and preventing data risks is particularly crucial. To this end, enterprise data governance requires systematic coordination across three levels—formulation, implementation, and guarantee—with distinct adaptation strategies at each level. At the formulation level, linking legal norms with data standards establishes the fundamental principles and requirements for data governance. At the implementation level, legal norms are refined into actionable rules and processes to ensure concrete execution of governance requirements. At the guarantee level, diversified co-governance through government supervision, industry self-discipline, and social oversight provides continuous optimization and support for effective rule implementation. These measures aim to provide enterprises with a systematic, dynamically adaptable legal response framework for navigating the digital intelligence era and market competition.

Keywords: Enterprise Data; Data Governance; Artificial Intelligence; Legal Response

In the digital intelligence era, data has become a key element of enterprise digital transformation, and data governance has ascended to the core of corporate intelligent strategy. Upon closer examination, data gains vitality through circulation, providing crucial support and driving force for enterprises to optimize resource allocation and strengthen market positions. However, as data permeates the entire lifecycle of artificial intelligence operations and becomes universalized through foundational large models, the attendant real-world risks of data security, compliance, and monopoly exhibit dynamic, diffusive, and negative externalities characteristics. Consequently, how to balance promoting data circulation with preventing data risks has become a critical issue for enterprise data governance across nations in the digital intelligence era.

International competition over data governance rules is intensifying, with strategic directions for enterprise data governance already at stake. The EU' s data governance model has shifted from personal data protection marked by the General Data Protection Regulation (GDPR) toward enterprise data governance represented by the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union, the Data Governance Act (DGA), and the Data Act, aiming to curb the development of digital platforms from China and the United States. The United States, based on federal provisions such as the Federal Trade Commission Act (FTC Act) regarding unfair competition methods

and unfair or deceptive acts or practices in commerce, along with the Security Requirements for Restricted Transactions, and state-level data protection bills, has already covered the formulation and implementation of enterprise Privacy Policies while continuously monitoring enterprises engaged in restricted data transactions. China emphasizes the development and utilization of enterprise data resources, market-oriented allocation reforms for data elements, and data circulation and sharing, successively releasing documents including the "Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Data Basic System to Better Leverage Data Elements" (hereinafter "Data Twenty Articles"), the "Three-Year Action Plan for 'Data Elements ×' (2024-2026)", the "Opinions on Promoting the Development and Utilization of Enterprise Data Resources", and the "Implementation Plan for Improving Data Circulation Security Governance to Better Promote the Marketization and Value Enhancement of Data Elements". These initiatives jointly drive the deepening development of enterprise data governance through policy guidance, corporate practice, and technological innovation. By 2023, China's total data production reached 32.85 zettabytes. In essence, whoever controls data gains market advantage. For instance, Huawei Cloud Stack launched the DataArk platform for digital intelligence integration, aiming to provide comprehensive data governance for government and enterprise customers. Alibaba built the DataWorks one-stop intelligent big data development and governance platform, emphasizing full lifecycle Data+AI management for enterprises. Evidently, enterprise data governance has become a necessary and critical practical action.

At the micro level, due to data's unique object structure, enterprises present diverse stakeholder interest relationships during data collection, integration, and analysis, necessitating a rethinking of traditional single-path regulation. In July 2021, "Didi Chuxing" caused serious data security issues due to illegal and irregular information collection. In April 2023, in the case of "Chuangrui Company vs. Weibo Company on Unfair Competition", the court held that Chuangrui Company used improper means to scrape and transport non-original video files and comment content from the Douyin App, harming Weibo Company's competitive interests. In October 2024, in the case of the "Irish Data Protection Commission vs. LinkedIn", LinkedIn was fined for seriously infringing on data subjects' fundamental rights by processing personal data without appropriate legal basis. At the macro level, China has yet to enact specialized laws and regulations for enterprise data, and with numerous data protection-related laws and regulations, enterprise data remains difficult to protect effectively. Combined with factors such as enterprise data management, system equipment vulnerabilities, and technological iteration, this triggers data security risks. Subsequently, enterprises' internal management of data collection, storage, and transmission struggles to meet numerous compliance requirements and security regulations. Once non-compliance reaches a certain level, it may attract regulatory attention and even trigger antitrust investigations. Meanwhile, due to weak regulatory approaches, some enterprises intend to monopolize specific industries, forming

"data silos." Even more concerning, to capture more data, enterprises use artificial intelligence and other technologies to implement precision pricing, personalized services, and "big data price discrimination" to extract excess profits and squeeze out competitors. Clearly, how to promote data circulation while preventing data risks holds both theoretical significance and practical value for driving digital economy development. Although exploration and trial-and-error in enterprise data governance were necessary costs during the initial stages of the digital economy, legal responses should be adhered to in the long run. In view of this, this paper discusses enterprise data governance, analyzes international data governance trends, identifies existing risks in enterprise data processes, explores the underlying causes of these risks, and examines how law should respond to enterprise data governance in the digital intelligence era.

I. Trend Analysis of Enterprise Data Governance in the Digital Intelligence Era

Current international practices in enterprise data governance can be broadly categorized into three models: first, the "strong regulation" model represented by the EU, aiming to promote internal data openness and sharing while cultivating international data markets; second, the "weak regulation" model represented by the United States, emphasizing market rules and autonomous decision-making rights of market entities while advocating cross-border data flow and protecting domestic data; and third, the "security and development equally emphasized" model represented by China, stressing both data localization and multilateralism.

(I) Conceptual Definition of Enterprise Data Governance

In short, enterprise data emphasizes data collections with economic value, expressed in code form, that enterprises collect and integrate in their production and operations. On September 1, 2021, the Data Security Law of the People' s Republic of China (hereinafter "Data Security Law") formally took effect, with Article 3 clarifying: "Data as referred to in this Law means any record of information in electronic or other forms." On November 1, 2021, Article 4 of the Personal Information Protection Law of the People' s Republic of China (hereinafter "Personal Information Protection Law") stipulates that "personal information is various kinds of information related to identified or identifiable natural persons recorded in electronic or other forms, excluding information after anonymization." However, the conceptual connotation of enterprise data remains unclear in the Data Twenty Articles. In practice, data can generate real or potential economic benefits for enterprises in their production and operations, and personal data constitutes an important component of enterprise data. In academia, personal data and personal information carry the same meaning.

Regarding enterprise data governance, it originated in foreign academia in 2004. Hugh J. Watson et al., after studying data warehouse governance practices, ar-

gued that when establishing enterprise data warehouses, multiple stakeholders should jointly participate in the organizational structures and processes for their creation. In June 2014, China first pointed out at the ISO/IEC JTC1/SC40 meeting of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in Sydney that data governance refers to the process by which public institutions such as governments, private institutions such as enterprises, and individuals adopt a series of measures including law, standards, and technology to maximize data value and promote safe, orderly data flow. In summary, enterprise data governance refers to the collection of activities through which enterprises manage and control data, aiming to ensure data quality, security, and compliance while maximizing data asset utilization and value creation.

(II) EU Trends in Enterprise Data Governance

EU data governance policy formulation and practice constitute a gradual process emphasizing the elimination of data flow barriers among member states and characterized by "strong regulation" —namely, unified data legislation with substantial government intervention in digital markets to regulate market behavior, focusing on data sharing and free flow. First, the introduction of GDPR and the Regulation on a Framework for the Free Flow of Non-personal Data emphasized both strong protection of personal data and advocacy for free flow of non-personal data. Subsequently, in 2022, the DGA became a core pillar of Europe' s data strategy, aiming to facilitate easier data sharing among enterprises and citizens in a trusted, secure environment. In 2023, the EU Digital Markets Act (DMA) established a "gatekeeper" system for large IT enterprises to maintain fair trading and competitive market environments. In the same year, the Data Act adopted measures to protect all European enterprises seeking data, especially small and medium-sized enterprises, from unfair contract terms, such as non-negotiable "take-it-or-leave-it" terms imposed by stronger parties regarding data access and use.

(III) US Trends in Enterprise Data Governance

Compared with the restrictive nature of EU enterprise data governance, US enterprise data governance tends toward principle-based approaches, highlighting "weak regulation" and "double standards." On one hand, it insists on market freedom with minimal intervention in data markets to unleash data value. On the other hand, it builds high walls for domestic data protection. In 2018, the US began shifting from an "application-dataset" model to a "data as strategic asset" model through the Foundations for Evidence-Based Policymaking Act (FEBP), the Geospatial Data Act (GDA), and the subsequent Federal Data Strategy. The US Department of Commerce (DOC) then pointed out that developing new technologies and implementing data governance would maximize data value and strengthen competitive advantages for US enterprises and research institutions. Simultaneously, the US enacted stringent data protection

policies such as the Clarifying Lawful Overseas Use of Data Act (Cloud Act) to broaden its jurisdictional boundaries for data access, removing obstacles for US access to overseas data while strengthening protection of domestic data. In 2024, the Center for Strategic and International Studies (CSIS) released the report "Untapping the Full Potential of CLOUD Act Agreements," emphasizing that US service providers should be prohibited from disclosing user information to foreign governments without valid US legal process through "Blocking Statutes."

(IV) China Trends in Enterprise Data Governance

Currently, China' s data security strategic layout has initially established a "three laws and one regulation" system centered on the Cybersecurity Law, Data Security Law, Personal Information Protection Law, and the Critical Information Infrastructure Security Protection Regulations, supplemented by multiple documents including the Data Twenty Articles. Enterprise data governance is developing toward intelligent and automated applications, exploration of data element marketization, and strengthened compliance and supervision, while adhering to an open, inclusive, and cooperative attitude and practicing multilateralism. Specifically, China advocates data security as the prerequisite for developing the digital economy, insists on data localization, and restricts domestic storage and cross-border flow of data through the Cybersecurity Law and Data Security Law. Meanwhile, guided by the "community of shared future" value concept and adhering to multilateralism, enterprises must follow principles of openness, cooperation, equality, and mutual benefit in data acquisition, management, and utilization, jointly participating, consulting, and decision-making with all parties to achieve diversified, standardized, globalized, and sustainable data governance development. Through participation in international documents such as the Global Digital Compact, the Global Initiative on Data Cross-Border Flow Cooperation, and the Belt and Road Digital Economy International Cooperation Beijing Initiative, China fully demonstrates its emphasis on maximizing data value release and promoting international cooperation in data governance.

II. Risk Identification in Enterprise Data Governance in the Digital Intelligence Era

In enterprise data governance, data security risk is the primary concern. As digital technology iterates, enterprises face security risks such as data leakage and privacy infringement during data collection, storage, and processing. If enterprises fail to effectively address data security risks, they may generate compliance risks such as ultra vires data collection and "big data price discrimination" in data governance. When data compliance risks accumulate without proper resolution, combined with data advantages and abundant capital of leading enterprises, they may trigger data monopoly risks. Subsequently, these three risks present complex interactions, intertwining and superimposing upon each other. This chain reaction and superposition effect of risks severely restricts free cir-

culation and efficient sharing of data, preventing data from fully releasing its value in the market.

(I) Data Security Risk

Data in motion contains both economic potential and security risks. To excavate and release data value, enterprises collect data through data acquisition—identifying and selecting data from sources—gathering incidental data in production operations, user personal data, and data on non-natural person subjects, while also obtaining data from other entities through contracts, authorizations, and web crawlers. During this process, constrained by regulatory gaps and lack of standard guidance, massive data capture by enterprises inevitably causes security issues such as data leakage and privacy infringement. Specifically, emerging technologies like artificial intelligence have increasingly become the underlying technical foundation for entire industry chains. Since large language models require massive data during training, this data encompasses core business operations, strategic deployments, and third-party cooperation trade secrets, and may even involve sensitive personal information such as partners' personal privacy, transaction records, and behavioral preferences. In practice, throughout the full lifecycle of data storage, training, and transmission, enterprises often face data leakage when suffering hacker attacks or system vulnerabilities, thereby hindering smooth data transactions. Second, individuals' privacy protection awareness has been rising in recent years, with increasingly stronger demands for controlling their own data, forcing enterprises to invest substantial costs in data management activities. Individuals generally expect to autonomously decide when, where, and how their data is used. Although individuals have diverse needs such as enjoying broader service scopes, more friendly user experiences, and higher cost-performance services, their demands are difficult to realize due to high data migration costs and widespread incompatibility of data formats across major platforms. Therefore, to maintain existing market positions and seek competitive breakthroughs, most enterprises choose to invest heavily in improving data processing speeds, optimizing algorithmic efficiency, and enhancing system analysis capabilities to attract individuals, lock in groups, and bundle data, while potential leakage and abuse risks throughout the data lifecycle are not prioritized.

(II) Data Compliance Risk

Driven by profit, enterprises voluntarily invest enormous costs in collecting, storing, and analyzing data. During this process, enterprises collect data through formalistic compliance methods such as cookies, and can collect privacy information without individuals'knowledge, then extract high-value information through web crawlers. After collecting massive data, enterprises shift their focus from internal activities to external production and operations. Essentially, enterprise data collection resembles an investment. Enterprises intend to "shift from focusing on shareholder equity and corporate discounted cash flow to focusing on

stakeholders and interactions occurring outside the company," with the primary purpose of dominating individual consumption through personalized marketing and precision services. During data analysis, enterprises use artificial intelligence and algorithms to conduct in-depth analysis and profiling of user characteristics, constructing precise user portraits, yet users often remain unaware that their personal information is being deeply analyzed and deconstructed by digital technology. The reason is that while enterprises accept the "notice-consent" framework, they may invest substantial resources in Privacy Policies and other formalistic compliance measures. In practice, Privacy Policy content is lengthy and technical, which ordinary users may lack the time, interest, or capacity to read, so even when signing consent forms they may not understand the specific content. Additionally, much data may have no immediate use when collected but can develop new uses over time, as scenarios change and combine with other factors, making it difficult for enterprises themselves to inform about all data uses. Furthermore, during continuous service provision, enterprises collect data on users' browsing records, purchase histories, and search habits, using algorithmic models to analyze consumption preferences, price sensitivity, and purchasing power, then discriminate between "high-value" and "low-value" users. For instance, showing higher prices or providing inferior services to loyal, high-frequency "high-value" users while offering more favorable prices or better services to new, low-demand "low-value" users constitutes illegal "big data price discrimination." In this regard, neither "high-value" nor "low-value" users can detect they have been "discriminated against" or know their rights have been infringed.

(III) Data Monopoly Risk

After training on massive data, artificial intelligence is applied to search engines, office software, and corporate strategy, with enterprises' data control scale exceeding imagination. On one hand, leading enterprises such as Google, Microsoft, and Facebook hold monopolistic advantages in data control and may play the role of data "gatekeepers," setting high data barriers and thresholds. In practice, Google and Facebook can access data unavailable to other enterprises, while many startups may abandon market entry due to having to pay high "fixed costs" first. Moreover, artificial intelligence in certain professional fields requires high-quality data to improve large model generation accuracy and reduce "disproportion" between original and derived data content. Enterprises possessing such key core data may refuse to open their data to increase user stickiness and strengthen competitive advantages, even blocking data interfaces with other enterprises through technical means, further exacerbating data monopoly risks. On the other hand, enterprises manipulate original data generation results through "data power," reducing individuals' effective control over derived data flow and usage. During personal use of AI large models, whether input questions, interactive content, or behavioral data generated from usage, all are centrally controlled by enterprises. Subsequently, by monopolizing these valuable personal data, enterprises use AI to continuously analyze

patterns, preferences, and needs, thereby expanding market reach and consolidating competitive advantages. Beyond the aforementioned "big data price discrimination," enterprises may also conduct excessive frequency precision marketing toward individuals, frequently pushing information through SMS, phone calls, and emails that is often unrelated to actual needs. Additionally, when individuals request data transfer, enterprises may increase difficulty by using incompatible data formats or complex data export processes, limiting or depriving individuals of the ability to transfer data to third parties.

III. Investigation of Risks in Enterprise Data Governance in the Digital Intelligence Era

The development speed of emerging technologies like artificial intelligence often exceeds law-making speed because legislation requires substantial time for research, demonstration, and formulation, thus legal norms need principled provisions in certain aspects or even deliberate gaps. However, overly principled legal norms may face application difficulties in specific cases, and enterprises struggle to obtain legal protection. Simultaneously, enterprises face difficulties accurately understanding and implementing legal requirements, and may even deliberately circumvent laws for profit, merely satisfying formalistic requirements. Furthermore, enterprises with severe self-interest may use resource and technological advantages to acquire or control data, thereby forming data monopolies in the market.

(I) Legal Norms Need Updating

Alongside technological iteration, information processing activities become increasingly complex, with involved subjects and processing behaviors correspondingly diversifying. In practice, data leakage involves multiple subjects including data providers, data holders, and data users. Currently, China has numerous laws, standards, and documents related to enterprise data governance, but their effectiveness is questionable. For instance, Article 20 of the Personal Information Protection Law clarifies norms for jointly processing personal information, but provisions on "joint processing" are overly principled with few cases, and identification of what constitutes "joint processing" is broad. That is, under the overarching common purpose and method forming a joint processing appearance, the whole constitutes "joint processing." This may require comprehensive judgment in individual cases from aspects such as business cooperation models, subjects' common purposes, and processing method agreements to refine unified identification rules or standards for "joint processing." Alternatively, using the tort liability section of the Civil Code of the People' s Republic of China as an important reference, though some practical views hold that the Civil Code' s multi-person tort liability norm group is unsuitable as a referenced norm. Second, during processing, to prevent data leakage, individuals can freely transfer personal data across different websites and devices based on Article 45(3) of the Personal Information Protection Law regarding the "right to portability,"

requiring enterprises to transmit personal information to designated third parties in secure, convenient ways without worrying about leakage or abuse during transmission. Through the portability right, individuals can more freely determine personal information flow and usage, helping promote free data flow and sharing to address data silos and market monopolies. However, given diversified application scenarios, complex specific methods, and diverse data standards, Article 45(3) of the Personal Information Protection Law is rather principled. The reason is that portability right application scenarios are extensive, involving different industries and fields. For example, in finance, individuals need to transfer personal information from Bank A to Bank B. In social networking, individuals hope to transfer personal information from Platform A to Platform B. Meanwhile, realizing the portability right requires solving technical issues such as data format conversion, transmission security, and integrity verification, with solutions potentially needing to combine enterprises' technical capabilities, business models, and compliance needs. In the future, national cyberspace authorities need to formulate specific guidance or standards based on practical situations.

(II) Rule Framework is Overly Formalistic

Article 13 of the Personal Information Protection Law stipulates various conditions for processing personal information, with obtaining individual consent undoubtedly being a crucial and core condition among them. With absolute advantages in capital and technology, enterprises can easily obtain individual consent for Privacy Policy terms through opt-in mechanisms. Moreover, numerous documents such as rules, guidelines, and standards concerning enterprise data compliance exist. Without extracting and refining core content, the "notice-consent" framework may become formalistic, failing to genuinely reflect individuals' intentions. From the Personal Information Protection Law's system, the duty to inform follows the separate consent clause, and fulfilling the duty to inform is a prerequisite for obtaining consent. Generally, enterprise-formulated Privacy Policies cover notification matters and rights and obligations toward individuals. Some terms may contain vague vocabulary such as "specific products" or "certain functions," and may also include professional terms like SDK and OAID. Even when enterprises use bolding, color changes, and underlining, individuals may struggle to understand due to lack of professional knowledge. In practice, enterprises only focus on whether they have formally fulfilled the duty to inform, not whether individuals genuinely consent. Therefore, individuals cannot fully understand Privacy Policies, let alone truly choose autonomously, meaning that option checks, click confirmations, and other "general consents" obtained by enterprises cannot demonstrate the authenticity or validity of individual consent. Second, after individuals are "forced" to consent, enterprises use personal information for "big data price discrimination." Moreover, individuals' interests and needs are dynamically changing, and information has high timeliness characteristics, so information quickly loses expected value due to inability to update timely and effectively. Taking OpenAI's Privacy Policy

as an example, after individual consent, some data is collected by ChatGPT for service improvement. This "general consent" authorization method, though brief in process, has general provisions and fixed patterns, making it difficult for individuals to assess dynamically changing data risks and impacts of subsequent models, rendering the "notice-consent" framework a mere formality.

(III) Unfair Competition in Data Markets

According to statistics, China investigated and concluded 27 monopoly agreement and abuse of market dominance cases in 2023, with fines totaling 2.163 billion yuan, while reviewing 797 operator concentration cases. This demonstrates that data concentration and monopoly phenomena are increasingly evident in data product and data-as-production-factor markets, while data sharing and reuse have become difficult. Even though Article 4 of the Interim Measures for the Management of Generative AI Services highlights potential monopoly behaviors, it still struggles to provide specific references for identifying illegality of specific practices. From the enterprise-to-enterprise perspective, startups may lack sufficient time and resources to accumulate enough data, let alone train data through AI. Therefore, startups entering data markets such as search engines and social products may face high entry barriers. Meanwhile, enterprises controlling massive data worry that data disclosure or sharing may be improperly utilized by competitors, threatening their market positions. A typical case is the "prisoner' s dilemma" : Enterprise A and Enterprise B can reduce overlapping data costs through cooperation and data sharing, but Enterprise A worries that Enterprise B may develop more competitive services for short-term gains, while Enterprise B has the same concern. From the enterprise-to-individual perspective, enterprises achieve product or service iteration and upgrading through deep data value mining, then enhance user stickiness and expand market scale through precise, personalized user experiences. This scale effect improvement in turn further optimizes products or services and strengthens enterprises' data advantages, forming a self-reinforcing upward spiral. Meanwhile, enterprises with massive data resources often demonstrate stronger production efficiency, driving them to expand production scale and transaction frequency. During this process, enterprises create more data and use such information for "real-time pricing" to extract more consumer surplus, then accumulate more data to strengthen production efficiency, forming a "Data Feedback Loop." Evidently, such increasing data returns drive enterprises to practice price discrimination against individuals to extract excess profits, thereby harming fair market competition.

IV. Legal Responses to Enterprise Data Governance in the Digital Intelligence Era

How to promote efficient and orderly enterprise data circulation is the core issue of the digital intelligence era. Reasonable solutions include linking legal norms with data standards at the formulation level, emphasizing dynamization

of the "notice-consent" framework at the implementation level, and adopting basic strategies for diversified governance methods at the guarantee level. These three paths cooperate and co-govern synergistically. The formulation level provides dual legal and technical constraints for enterprise data governance, the implementation level concretizes these constraints into operational rules and processes, and the guarantee level ensures effective implementation of these rules and processes through diversified governance methods.

(I) Formulation Level: Linking Legal Norms and Data Standards

Currently, China has initially formed a data security strategic layout with the "three laws and one regulation" as the main line, supplemented by documents such as the Data Twenty Articles, but has not yet issued national-level legislation specifically on enterprise data governance. Meanwhile, due to evolving data governance and insufficient practical experience, directly enacting separate laws indeed poses difficulties, making it necessary to link relevant legal norms with data standards. The reason is that hard-law regulations sometimes struggle to conduct regular adjustments on data governance with universal, technical, and timely characteristics, while soft-law data standards can play more direct, effective, and transitional roles through diversity and flexibility. In this regard, it is recommended to use the "National Data Standards System Construction Guide" issued by the National Development and Reform Commission and other departments in September 2024 as an important reference. Specific linking can be divided into content requirements and enforcement supervision.

Regarding content requirements, enterprise data business standards, quality management, investigation and inventory, and resource registration should be appropriately linked with relevant laws and regulations. First, enterprise data business planning must be based on lawful collection and use, strictly complying with provisions on data legality in the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. Then, differentiated protection strategies should be implemented according to data sensitivity and importance. Second, security indicators such as enterprise data leakage rates, tampering rates, and integrity should be incorporated into data quality evaluation systems, with regular assessment reports issued. For instance, important data processors required under Article 30 of the Data Security Law must submit risk assessment reports, and personal information protection impact assessments required under Article 55 of the Personal Information Protection Law. Encryption technologies, access control technologies, and data desensitization technologies that comply with laws and regulations should be used to evaluate data quality. Third, in data investigation and inventory, privacy protection requirements should be fully considered, and technical means such as de-identification and desensitization should be used to process sensitive data. Finally, during data resource registration, security reviews should be conducted on data sources, usage purposes, and processing procedures, such as security certification information stipulated in Article 23 of the Cybersecurity Law.

Regarding enforcement supervision, independent regulatory agencies and their responsibilities and authority should be clarified. Such agencies should be directly accountable to the board of directors or shareholders' meeting, supervise enterprises' compliance systems and risk impact assessments, and possess necessary authority for data retrieval and violation disposition recommendations to ensure independence and authority in enterprise data governance supervision. Taking unfair competition judgments involving data as examples, most judgments rely on Article 2 of the Anti-Unfair Competition Law, requiring enterprises to "follow principles of voluntariness, equality, fairness, and honesty, and abide by law and business ethics." From a legal theory perspective, this provision is closer to a standard or principled rule. Therefore, regulatory agencies should issue warnings, fines, and order rectifications for enterprises violating laws, regulations, and data governance standards.

(II) Implementation Level: Dynamization of the "Notice-Consent" Framework

Despite its flaws, the standardized "notice-consent" framework remains the mainstream solution adopted globally because it achieves bidirectional cost optimization for individuals and enterprises. Currently, dynamic adaptation of information application scenarios is the core driver of information technology development. For individuals to make decisions truly reflecting their will, the "notice-consent" framework must be dynamized, enabling individuals to achieve "keeping pace with the times" awareness under continuously updated information states. Therefore, one-time "general consent" cannot cover the entire data lifecycle. The dynamized "notice-consent" framework aims to achieve "absolute control" over information—namely, "information self-determination" —to bridge information gaps formed by professional barriers in information processing and sensitive characteristics of information content.

In the pre-notification stage, appropriately set "separate notification"corresponding to "separate consent." Articles 29, 30, and 55 of the Personal Information Protection Law respectively stipulate "separate consent" for processing sensitive personal information, "notification" content, and "impact assessment," but have not specified specific notification forms. Given the limited nature of individual expression in information processing, after enterprises conduct pre-risk assessments, they may appropriately conduct "separate notification" to individuals based on principles of flexibility, minimal necessity, and scenario respect, and set up separate notification pages or pop-ups to elaborate processing purposes, methods, and risks, thereby alleviating information overload from "package notification" and "general notification" and enhancing individual autonomy and precision in controlling their information. Second, effectively construct efficient and smooth communication channels between individuals and enterprises. Embed a "term feedback" button at key locations such as Privacy Policy pages and App settings menus, supporting one-click marking of obscure terms (e.g., highlighting, noting questions). Open 7$\times$24-hour intelligent customer service

channels that automatically identify screenshots of terms submitted by individuals. Meanwhile, set up interactive term graphs where clicking "penalty" can expand calculation formulas, such as "penalty amount = contract total × 20%," and use animations to demonstrate complex processes, such as decomposing "insurance claim process" into three steps: reporting → damage assessment → compensation.

During the in-process stage, clarify enterprises' full-process, continuous notification obligations. Enterprises should follow up in real time on changes in key elements such as data processing purposes, methods, and scopes. When information processing activities change, enterprises need to timely retain specific matters, reasons for changes, and impacts on individual rights, then notify individuals of updated content through multiple channels including phone, email, and website announcements. Meanwhile, individuals have the right to review historical archives of each notification to understand changes in information processing activities. According to Article 14(2) of the Personal Information Protection Law, "when the purpose, method, and type of personal information processed change, consent shall be obtained again." Second, clarify that individuals can withdraw previously given consent. As things develop, information generates new information, and individuals' interests and needs change, so individuals may claim withdrawal due to regretting initial consent. When individuals withdraw initial consent, enterprises lose the legal basis of individual consent and have no right to process personal information. Notably, since individual unilateral consent can establish legal relationships, individual withdrawal of consent also does not require any form of enterprise approval.

In the post-control stage, minimize adverse impacts. First, conduct data desensitization using replacement methods, masking methods, and dynamic encryption to sever connections between data and individuals. Second, classify and grade risks based on different enterprise data scenarios and data types to formulate targeted and accurate response plans. By business scenario, categories include development, testing, and production. By data type, categories include personal data, trade secrets, and public data. By sensitivity level, categories include low, medium, and high sensitivity. Through matrix lists, risk classification and grading can be visualized. For instance, for core data with high-risk scenarios, strict data encryption and access control measures can be formulated. For general data with low-risk scenarios, basic access and data backup methods can be adopted.

(III) Guarantee Level: Basic Strategies for Diversified Governance Methods

As mentioned above, the full lifecycle of data collection, storage, and use involves stakeholders such as governments and industry organizations. Essentially, single governance subjects or approaches struggle to effectively address continuous, dynamic, and diversified data risks. Examining foreign governance practices reveals universal emphasis on both traditional law and diversified gov-

ernance methods including market mechanisms, technical standards, industry self-discipline, and social autonomy. Therefore, even in "prisoner' s dilemma" games, cooperation and appropriate punishment among participants are needed to ensure sustainable development of digital society.

First, at the national level, regulatory agencies play a leading and promoting role. Since the establishment of the National Data Bureau in 2023, the situation of multiple departments managing data separately has changed. On this basis, data security measures can be formulated to regulate enterprise compliance obligations, improve enterprise information collection transparency, link relevant legal norms with data standards, and promote collaborative governance between central and local governments and across sectors. Second, at the industry level, as a key link connecting government and enterprises, industry organizations play an irreplaceable coordinating and standardizing role. The Data Security Law and other documents mention relevant content on joint participation of enterprises and industry organizations in data governance. Therefore, enterprises and industry organizations should actively interact to jointly formulate industry standards and norms for data governance based on professional field characteristics and needs. Then, refine requirements on data security protection and data sharing cooperation to safeguard specific data governance actions. Meanwhile, establish industry self-discipline mechanisms to appropriately constrain member units' data governance behaviors and maintain industry order and fair competition, drawing on foreign experience where the US federal government respects industry self-regulatory norms on data use and transactions between private entities. Additionally, maintain good government-enterprise cooperation relationships. Industries can feedback problems and needs in data governance processes to the government, which can then promote orderly data governance development through policy guidance and financial support. Third, at the societal level, as an important supplement to government supervision and industry self-discipline, social oversight cannot be ignored. For instance, media can regularly publish lists of enterprises with behaviors such as irregular information collection or suspected data monopolies through official websites and WeChat public accounts, specifying the time, methods, and scopes of irregular information collection to enhance information transparency and warning effects.

Additionally, ensure data portability. Promote joint participation of diversified entities including government, academia, and enterprises in data standards implementation and improvement, gradually establishing standardized transfer procedures among enterprises. First, when submitting data transfer requests, individuals must clearly identify the recipient and specific data scope to be transferred. Enterprises should verify individual identity authenticity through multi-factor authentication mechanisms, while simultaneously conducting compliance reviews of legal frameworks and existing data agreements. Second, during data transmission, adopt standardized protocols (e.g., HTTPS/SFTP) and normalized interfaces to reduce compatibility obstacles from software and hardware differences such as database type diversity and operating system heterogeneity. At the data format level, prioritize machine-readable formats with

cross-platform parsing characteristics such as CSV, XML, and JSON to maintain semantic accuracy and format integrity, thereby reducing "data distortion" or garbled text. Third, in the data export stage, export process design should emphasize user-friendliness, considering secure and convenient visualization interfaces and Application Programming Interface (API) calls. Finally, recipient qualification verification of individuals is indispensable, and pre-agreed interface specifications must be followed to achieve effective data docking. In practice, leading enterprises including Microsoft, Facebook, Google, and Twitter jointly announced an open-source plan on the Data Transfer Project in July 2018, with secure and seamless data transfer between different enterprises being the core goal of this plan.

Data governance is the process of realizing data value, and enterprise data governance is the key link to releasing data value. If data security risks are not effectively controlled, they can easily induce data compliance risks. Long-term accumulation of data compliance risks may further breed data monopoly risks. Over time, this situation not only inhibits innovation vitality driven by data but also poses substantive obstacles to overall development in the digital intelligence era. In depth, enterprises universally face security risks such as data leakage and privacy infringement throughout the full lifecycle of data collection, storage, and processing. If enterprises neglect data security risks, they may not only cause sensitive information leakage due to technical vulnerabilities or management negligence but also trigger compliance risks such as ultra vires data collection and "big data price discrimination." With long-term accumulation and diffusion of compliance risks, especially when leading enterprises with data resources, capital strength, and technological advantages abuse market dominance, they are highly likely to evolve into data monopoly risks, thereby distorting market competition patterns and harming consumer rights. Therefore, at the formulation level, legal norms and data standards must be linked to establish fundamental principles and requirements for data governance. At the implementation level, these norms must be refined into actionable rules and processes to ensure concrete execution of governance requirements. At the guarantee level, diversified collaborative governance through government supervision, industry self-discipline, and social oversight provides comprehensive supervision and support for effective rule and process implementation. Through these legal responses, enterprises can achieve secure data governance, providing beneficial approaches for future research and application.

Note: Figure translations are in progress. See original paper for figures.