

On the Classification and Grading of Data in Civil Law

Guoqi Zhang

Graduate University of Mongolia, Ulaanbaatar, Mongolia

Abstract: This article explores the dual legal attributes of data from a civil law perspective, analyzes the classification and grading experiences abroad, and combines these with Chinese actual needs for data protection to construct a classification and grading path that fits Chinese legal system. Based on whether data carries personal information and whether it is publicly disclosed, this article proposes four categories of data and explains their applicable legal rules; it also divides data into three levels based on the degree of damage caused by data breaches, and proposes corresponding protective measures.

Keywords: Data classification and grading; civil law regulation; data protection; data rights; data trading.

1. Introduction

With the rapid development of information technology, the economic value and social significance of data have become increasingly prominent. Data transactions occur frequently, leading to issues such as data infringement, making it an urgent and important topic to regulate data under civil law. Scientific and reasonable classification and grading of data form the foundation for effective regulation. This helps clarify the rights, applicable rules, and protection levels of different types of data, thereby promoting the healthy development of the data industry and safeguarding the legitimate rights and interests of data subjects.

2. Basic Concepts and Legal Attributes of Data

(1) Definition of data concept

In different industries and fields, the definition of data varies. In the field of computing, data is presented in the form of bits, which are combinations of 0s and 1s; in the communication sector, data can be categorized into different layers. However, from a civil law perspective, data is property that arises and accumulates during human life and production activities, recording information about the objective world. It exists outside the human body, possessing certainty and independence. For instance, in cases involving the theft of online game equipment and disputes over the inheritance of email accounts and online stores, data is regarded as property with object status, highlighting its importance in civil law.

(2) Clarifying the relationship between data and information

In legal documents and research, data and information are often used interchangeably. In fact, there is an essential difference between the two. Information represents ideas and content, manifesting in various forms such as text, symbols, and images. It is a fundamental resource for knowledge and social development and can exist independently of data in traditional media; data, on the other hand, serves as the carrier of information, presented in binary form, encompassing all aspects of information. However, in terms of legal protection, some laws do not clearly distinguish between the two. For example, in EU-related laws, personal data and personal information protection measures are similar.

(3) Analysis of the legal attributes of data

1. Personality right attribute

Data reflects personality attributes when describing subjects, closely linked to the individuals character. It can be identified through technical processing to recognize specific individuals, such as personal data and organizational data. Once data is misused illegally, it may threaten personal safety and property. Although data does not directly affect the personality of producers, it indirectly reflects personality rights through its impact on production and business operations. Therefore, in data processing, the personal interests within the data should be fully protected.

2. Property rights attribute

Data has economic value and plays a crucial role in corporate decision-making and business profit acquisition. Data production and storage incur costs but can also generate revenue through transactions, as demonstrated in the hiQ v. LinkedIn dispute. Additionally, data is tradable, meeting both technical and legal conditions for trading. Although it requires balancing the interests of all parties, transactions can be conducted legally and compliantly, indicating that data possesses property attributes and should be protected by law.

3. The Necessity of Data Classification and Grading in Civil Law and The Reflection of Existing Research

(1) The necessity of classification and grading

Theoretically, the dual legal nature of data and complex dispute scenarios highlight the importance of classification and grading. By adopting a typological approach, we can delve deeper into data attributes and incorporate them into appropriate legal norms. In practice, judicial precedents continue to grow, such as the case of Luo v. a Shenzhen tech company and the case of Chongqing Guangs motorcycle company against Guangzhou Sans motorcycle company, indicating that different types of data are subject to different rules. Classification and grading help resolve disputes and promote a balance between data circulation and protection.

(2) Shortcomings of existing research

The existing research in China has inconsistent data classification standards. For instance, data can be categorized by the rights holder into personal, corporate, government, or public data, or by their source into raw, derived, and anonymized data. Data classification also lacks a unified standard. Although attempts have been made to classify data based on importance or industry sectors, these methods all have their issues. Categorizing data by rights holder fails to

resolve disputes over data ownership, while classifying it by source does not adequately reflect differences in data value. Moreover, current classifications do not fully consider civil law factors, failing to meet practical needs.

4. Experience of Classification and Grading of Data Outside the Region

(1) The American model

The United States adopts a decentralized legislative model, specifying data classification and grading in federal, state laws, and industry standards. For instance, federal laws categorize data based on sensitivity levels, while state laws such as the California Consumer Privacy Act provide further details. Industry rules, like the credit card industry's data security standards, also have corresponding classifications and grading. The innovation lies in combining classification and grading with risk assessment, and proposing a framework for public interest data sharing. However, it relatively overlooks the protection of individual data rights.

(2) The EU model

The EU adopts a unified legislative model, with the European Union Data Protection Regulation (GDPR) at its core. The regulation roughly categorizes personal data into general and special data, and specifies sensitive data such as political views and genetic information through special provisions. Member states supplement and refine these provisions based on this framework. The EU prioritizes the protection of personal information rights, establishing data committees and enforcement bodies to ensure the implementation of regulations. However, the EU's regulations on data classification are relatively insufficient.

5. Construction of Classification and Grading Path of Data in Civil Law

(1) Classification principles and standards

The principle of mutual independence and complete exhaustion should be followed to ensure that data classification is not repeated or omitted, while taking into account comprehensiveness, systematicness and scientificity, taking into account social, economic and cultural factors, and selecting classification standards based on reliable case analysis to protect the rights and interests of data subjects.

Classification is based on two dimensions: whether the data carries personal information and whether it is publicly disclosed. The key to determining if the data carries personal information lies in whether it can directly or indirectly identify a natural person's identity; anonymized data that does not carry personal information cannot be restored. Whether the data is publicly disclosed depends on whether the public can access it; data companies can change the data status according to their own needs.

(2) Specific classification and rules

Public data that does not carry personal information, such as query and aggregation platform data, is subject to the rules for the reasonable use and infringement of public data. Web crawlers must follow industry agreements when obtaining such data; if they violate these agreements, it may constitute an infringement. In determining infringement, the actual harm caused to the data company by the data scraping must be considered.

Public data containing personal information is commonly found on social platforms. Processing such data requires user consent or meets the conditions for reasonable use. To

determine whether a competitor's data scraping constitutes infringement, the key lies in whether the company has been harmed and whether users have the right to carry such data. The scope of the right to carry must be determined based on specific circumstances.

Non-public data that does not carry personal information is produced by enterprises and enjoys property rights and is protected by trade secrets. Data transactions can be transferred or licensed through open API, and transaction contracts can be similar to sales contracts or intellectual property license contracts and are subject to relevant laws.

Non-public data carrying personal information, such as user registration information on social platforms, is subject to relevant personal information protection regulations. Collection and change of use require user consent, data circulation is limited by user authorization, and enterprises need to process data within the scope of user consent, otherwise they may lose the property right of data.

(3) Principles and methods of classification

Classification principle, referring to the Data Security Law of the People's Republic of China, and combining the civil laws concern for individual interests, data is divided into 1-3 levels based on the degree of damage to individuals and organizations caused by data leakage. At the same time, the hierarchical relationship between personality rights and property rights is considered, with personality rights, especially material personality rights, taking precedence over property rights.

Classification method: Non-public data and public data that do not carry personal information are protected at level 1, governed by property rights rules and industry conventions; public data that carries personal information is protected at level 2, subject to personal information protection principles and internet self-regulation conventions; non-public data that carries personal information is protected at level 3, with the strictest protection required, balancing both individual personality rights and corporate property rights.

(4) Tiered protection measures

Primary data protection: Non-public data that does not carry personal information can be handled by enterprises according to property rights rules, transactions are subject to contractual constraints, changes in rights follow the principle of public notice, guarantees or usufructuary rights can be set, and others who illegally obtain such data must bear responsibility; Public data that does not carry personal information is owned by enterprises as property rights, it is subject to reasonable usage rules for public data, and unfair competition requires accountability.

Secondary data protection, the public data carrying personal information shall be processed with the consent of users. Enterprises and users shall bear corresponding rights and obligations respectively, and enterprises shall bear tort liability in violation of regulations.

Third-level data protection, non-public data carrying personal information, follows relevant rules, users agree to affect the change of data property rights and transactions, enterprises need to process and protect data according to regulations.

6. Concluding Remarks

The application of data classification and grading in civil law is a complex yet necessary exploration process. This study, based on the theoretical and practical needs of civil law, has designed a classification and grading path and protection

mechanism adapted to Chinese legal system. However, due to the dynamic development of data technology and the implementation of laws, continuous improvements to relevant rules are still required in the future. By establishing a scientific classification and grading framework, not only can legal issues related to data infringement and transactions be resolved, but it also provides important references for the rule of law construction in Chinese data economy era.

Reference Documentation

- [1] Tong Yunfeng. Certification and promotion: Civil Law Classification and Graded Protection of Readers Personal Information [J]. Modern Intelligence, 2021,41(12):97-106
- [2] Wei Ying. Research on the Classification and Grading of Data in Civil Law [D]. Shanghai Normal University, 2024
- [3] Zheng Xianghan. Research on the Civil Law Regulation of Data Trading [D]. Hebei Normal University, 2023