# Data Ownership and Digital Governance: Promoting Enterprise Cooperation and Sustainable Development

Lexuan Chen *

Department of Management, Beijing Sport University, Beijing, China

* Corresponding Author Email: 2016150269@jou.edu.cn

**Abstract.** In the contemporary data-driven era, the triad of data ownership, digital governance, and government-enterprise cooperation is woven intricately into the fabric of the digital landscape. At the core of this interconnected web lies the imperative to strike a delicate balance between safeguarding data rights, fostering data sharing, and upholding data security, all pillars underpinning the sustainable growth of digital ecosystems. This paper aims to illuminate the profound interplay between data ownership complexities, enterprise management strategies, and the overarching domain of digital governance. Furthermore, it delineates the landscape of pertinent legal frameworks that govern this intricate terrain. By embracing a nuanced, scenario-driven approach to data protection and by nurturing collaborations among diverse stakeholders, this article embarks on a quest to unravel how the implementation of effective cooperation models can serve as catalysts for the sustainable evolution of the digital economy. Simultaneously, these models advocate for responsible data governance, ensuring that the fundamental values of individual privacy and corporate interests remain duly safeguarded.

**Keywords:** Data ownership; digital governance; government-enterprise cooperation.

## 1. Introduction

In the era of digital transformation and data-driven innovation, the concept of data ownership has emerged as a pivotal issue. Enterprises increasingly view data as a valuable asset, making the protection of data rights and interests a top priority. However, the conventional approach of enforcing strict and exclusive property rights for data often clashes with its inherent nature, characterized by non-exclusivity and non-competitiveness. It is within this context that the importance of robust digital governance becomes evident.

The crux of the matter lies in the relationship between government-held data and corporate giants, particularly concerning the potential for data misuse incidents and their far-reaching consequences on the digital industry. The prominence of big business in the data landscape raises concerns about their ability to exert defacto control over data ("data ownership") due to a combination of technological, behavioral, and legal barriers. Such ownership-oriented approaches tend to stifle data sharing and limit opportunities for innovative data reuse. The impacts of data misuse incidents, when data falls into the wrong hands or is abused, can have profound repercussions on not only individual privacy but also the digital ecosystem as a whole.

To navigate these challenges, a multifaceted approach to data governance is proposed:

(1) Typed and Scenario-Based Data Protection. Recognizing that data comes in various. forms and is utilized in diverse contexts, the article advocates for a nuanced, scenario-based approach to data protection. Non-public corporate data should benefit from trade secret protection, safeguarding sensitive and proprietary information. Semi-public database data should receive special rights protection similar to the EU model, acknowledging their unique attributes. Public network platform data requires competition law protection to deter unethical practices.

(2) Proactive Data Protection. Enterprises should have the autonomy to proactively disclose data, aided by the creation of whitelists and blacklists. Such flexibility allows companies to manage data sharing in alignment with their preferences.

(3) Balancing Personal Data and Corporate Data. Legal frameworks should harmonize the protection of personal data and corporate data, ensuring that personal data privacy remains paramount while upholding corporate data rights and interests.

In this intricate landscape, government-business cooperation is essential to strike a balance between data rights and data sharing. Governments play a pivotal role in crafting regulations and frameworks that foster responsible data usage and data security. By developing and enforcing guidelines, governments can promote ethical data practices among enterprises and facilitate responsible data sharing. Furthermore, cooperation between governments and businesses is crucial in responding to data misuse incidents. A collaborative effort can help identify, mitigate, and rectify data breaches swiftly, safeguarding both individual rights and the integrity of the digital industry.

## 2. Literature Review

In contemporary society, characterized by the prevalence of algorithms, the utilization of extensive datasets has become essential for economic entities to effectively leverage the advantages of data-driven innovation (DDI). Nevertheless, the current system that revolves around data ownership presents notable constraints, especially when considering non-personal data. This system primarily relies on the control of data holders, leading to data access barriers that hinder data sharing and innovative data uses [1].

One way to address these challenges is by exploring alternative data management mechanisms. Commons-based data management emerges as a promising solution. Commons management focuses on access and freedom rather than exclusive ownership, making it particularly relevant for raw non-personal data (RNPD). We can view RNPD as a cooperative infrastructural resource that is available to a wide range of actors. Additionally, treating RNPD as a common aligns with the functional nature of data, facilitating its use for fundamental rights and human flourishing [1].

There has been a notable increase in the adoption of data governance frameworks aimed at effectively managing conflicting interests in data across multiple academic areas. The central challenge is to create a data governance framework that balances openness and accessibility with the need for control [2]. The necessary shift entails a move from conventional property rights in data to obligations pertaining to data access and exchange.

To address these complexities, data collaboratives empowered by decentralized learning techniques have been proposed as a potential remedy. These collaborative computational approaches can enhance control over data while ensuring its availability to various stakeholders [2]. The process of formalizing established technology solutions has the potential to enhance present data governance practices and play a significant role in attaining the policy objectives outlined in data strategies such as the European Strategy for Data.

In discussions about digitization and the data economy, there's a recurring theme of data subjects being considered owners of their data. However, this notion of data ownership encompasses a wide range of demands, making it challenging to define a unifying concept. Four conceptual dimensions of data ownership have been identified, suggesting that these calls aim to redistribute material resources and enhance the socio-cultural recognition of data subjects. Rather than rejecting data ownership claims outright due to the non-existence of property in data, it's essential to interpret these claims as attempts to renegotiate the status quo [3].

The utilization of big data and analytics (BDA) has become more essential for firms to prosper in the digital economy, as a result of the abundant data generated by connected devices and digital apps. The issue of data ownership assumes significant importance within the context of Big Data Analytics (BDA), particularly in relation to its "soft" components. This is due to the fact that the intended use or purpose of data processing in data lakes is sometimes unclear or uncertain [4]. This article examines the principles of data ownership and categorizes them into three separate types: data ownership, platform ownership, and product ownership. The aforementioned findings serve as a basis

for comprehending the progression of data management within the realm of Big Data Analytics (BDA), emphasizing the necessity of effective governance pertaining to data and analytics [4].

The rise of big data offers numerous opportunities for organizations to create value. However, adequate data analytics governance is essential to overcome fragmented data analytics activities. Governance mechanisms, including structural, procedural, and relational aspects, are vital in addressing these challenges. This article introduces a reference framework for data analytics governance, informed by literature reviews and case studies, which assists managers in designing governance mechanisms tailored to their organizations [5].

Efforts to facilitate efficient data and information sharing within organizations have often faced unexpected difficulties. One reason for these challenges is differing perceptions of data ownership among individuals or parties within an organization. This paper explores philosophical theories of ownership and property to gain insights into the origins of these perceptions. The proposition posits that the notion of "implicit" concepts pertaining to information ownership exerts an influence on the determination of the rightful possessor of particular data or information within an organizational context [6]. Understanding these implicit theories highlights the challenges of achieving compelling data and information sharing.

Data ownership and cooperation between government and enterprises are pivotal in the digital age. The proposition posits that the notion of "implicit" concepts pertaining to information ownership exerts an influence on the determination of the rightful possessor of particular data or information within an organizational context. Commons-based data management offers an alternative approach to overcoming data access limitations. Furthermore, contemporary data governance frameworks and data collaboratives that utilize decentralized learning techniques offer potential solutions for resolving divergent interests in data.

The implementation of robust data analytics governance is of utmost importance for businesses seeking to leverage the full potential of big data and analytics. This form of governance incorporates several processes, including structural, procedural, and relational aspects, in order to enhance the efficiency and effectiveness of data analytics activities.

Perceptions of data ownership within organizations play a significant role in shaping data-sharing behavior. Understanding these perceptions can provide insights into the challenges faced in achieving efficient data and information sharing.

In summary, navigating the digital landscape requires a nuanced understanding of data ownership, collaborative data management, and effective data governance mechanisms. These elements form the foundation for cooperation between government and enterprises to promote sustainable development in the digital economy.

## 3. Data Ownership and Enterprise Management

### 3.1. Perception of the Value of Data

#### 3.1.1 Data as a key resource for enterprise competitiveness

The importance of data in business management has attracted widespread attention, and it is regarded as one of the critical resources for enterprise competitiveness. Which Internet company has more data and makes better use of it? Which Internet company may have a leading edge in the competition? Businesses use data, mining, and leveraging to gain critical insights to make strategic decisions, improve products and services, optimize operations, and enhance customer experiences. This data-driven approach not only improves the efficiency of the enterprise but also strengthens the company's competitive position in the market.

A related research paper highlights the critical role of big data analytics in business management. The authors discuss in detail how data can be a competitive advantage for businesses and how innovation can be driven through data-driven decision support [7].

### 3.1.2 Different values for different types of data

Upon receipt of the paper, it is understood that the associated authors have granted us the copyright to utilize the paper for the specific book or journal under consideration.

The value of data is not generalized, and different types of data have different values and impacts on businesses. Structured data, such as sales data and customer information, is often easy to analyze and apply and can be used to predict trends and make strategic plans. In contrast, unstructured data, such as social media content and text reviews, may contain more emotions and consumer perspectives, helping to improve product design and marketing strategies. As a result, businesses need to identify and leverage the potential value of different data types to develop targeted data strategies.

Some scholars have delved into the application of unstructured data in marketing. The study highlights the importance of unstructured data and how it can become market insights and competitive advantage. This shows that different data types have different strategic values in business management [8].

## 3.2. Challenges of Data Ownership

### 3.2.1 The relationship and conflict between government data and big business

The relationship and conflict between government data and large enterprises: The data relationship between governments and large enterprises involves multiple aspects such as data ownership, data access, and data sharing. Governments have a lot of public data critical to public policymaking and the well-being of citizens. But large companies also accumulate vast amounts of private data, including customer information, market trends, and trade secrets. The relationship between the two can lead to conflict, especially regarding data privacy, security, and governance.

When studying the interaction between government data and private enterprises, some scholars pointed out that the openness and sharing of government data can promote innovation and economic growth. Still, it also needs to address data privacy and security issues [9].

The clarification of data ownership on the platform remains uncertain. Platform data frequently encompasses various qualities, including a substantial volume of personal information, hence necessitating the safeguarding of individuals' data privacy rights. Enterprises and governments engage in the collection of platform data, hence acquiring commensurate rights and interests in said data. Nevertheless, it is important to note that platform data has the potential to be publicly accessible, hence lacking exclusivity in terms of ownership by individuals, governments, or companies. Additionally, the properties of platform data are often highly dependent on specific scenarios. Based on these characteristics, this paper argues that platform data should be protected in a scenario-based manner, and whether it is personal data or enterprise data, rules should be formulated through bottom-up case-by-case judgment. When examining specific instances, it is imperative to take into account the characteristics of the platform, the type of data involved, and the characteristics of data crawlers. It is crucial to strike a balance between safeguarding data privacy, protecting data rights, and facilitating data exchange between businesses and governmental entities.

### 3.2.2 The challenge of data attribution management within the enterprise

Large enterprises often have multiple departments and business units, each of which may generate and manage large amounts of data. This can lead to confusion in data ownership and data management, and there may be data contention and data sharing issues between different departments. Organizations need to establish clear data ownership policies to address these challenges and ensure data legality and security.

Solving the internal data management challenges of an enterprise is a key step to ensure efficient data processes, data security and controllability, and maximize data value.

Data management within an enterprise faces multiple challenges that can affect the security, availability, and value of data. The following are some common in-house data management challenges:

Data security and data quality are the primary challenges of enterprise internal data management. Protecting data from unauthorized access, leaks and malicious attacks is critical. Data breaches can lead to privacy violations, compliance issues, and reputational damage; at the same time, businesses need to ensure that data is accurate, complete, and consistent so that the data has a high level of confidence to support decision-making and business operations.

When it comes to data security and attribution, determining which department or individual owns ownership of specific data, and how ownership of that data is managed and maintained can lead to controversy and complexity. Many industries and geographies have data privacy and compliance regulations, and businesses must ensure their data management practices comply with these regulations or risk fines and legal action.

The process of ascertaining the appropriate authorization for employees or departments to access and alter particular data is intricate in the context of data access restrictions. Inappropriate data access controls can lead to data misuse or error, and employee misconduct can lead to data breaches or loss. Data management involves complex technical requirements, including data storage, data analysis, data cleaning and data integration. Businesses need to continuously upgrade their technology infrastructure to meet these demands.

These challenges need to be considered comprehensively, and appropriate strategies and solutions should be adopted to optimize enterprise internal data management and ensure data management and utilization in a safe, efficient and controllable environment.

Some scholars have systematically studied data governance within large enterprises. The study summarizes best practices for data governance, including strategies for data ownership, processes, and security. This study offers useful insights into addressing the internal data management difficulties faced by organizations and establishes the groundwork for the development of scientific research big data platforms [10].

## 4. Digital Governance and Legal Framework

### 4.1. Overview of International and Domestic Data Protection Laws

References Examining China's practice, it can be found that after years of exploration, the protection level of personal data and enterprise data in the three central departments of criminal law, civil law, and administrative law in China has far exceeded the protection level of property liability rules. In the 2009 Criminal Law Amendment (7), Article 253 of the Criminal Law was added to Chapter 4, "Crimes of infringing on citizens' personal and democratic rights," including infringing on citizens' personal information as criminal sanctions.According to Article 111 of the General Principles of the Civil Law, which is no longer in effect, there is a provision that safeguards the personal data of individuals by legal means. Any entity or individual seeking to acquire the personal information of others must adhere to legal requirements and implement measures to safeguard the security of such information. The Civil Code protects personal information under personality rights and requires agreement from natural persons or their guardians for data processing unless otherwise allowed by legislation and administrative regulations. The Consumer Rights Protection Law, amended in 2013, states in Article 14 that customers have the right to legal protection of personal information and develops an informed consent-based system for the first time in China's public law. The Cybersecurity Law and Personal Information Protection Law strengthen the informed consent-based information protection system and enforce severe legal obligations to protect individual information rights. Article 14 of the People's Republic of China's Government Information Disclosure Regulations states that government information that may endanger national security, public safety, economic security, and social stability if disclosed, is state secrets. Article 15 states that administrative agencies shall not divulge government information including corporate secrets, personal privacy, etc. that would impair third parties' legitimate rights and interests. If the third-party consents or the administrative agency deems non-disclosure will severely harm the public interest, it will be disclosed. Although there are still many controversies on the nature of the security of personal

information by the three major departmental laws, such as whether it is rights protection or rights protection, whether it is individual rights protection, personality rights protection or national security protection, and what is the relationship between rights and interests. There is a need for more harmonious and consistent legal interpretation and the legal protection of personal information by the three major departmental laws. It has fully reached the protection level of property rules. In this case, even if individuals are granted data property rights, the liability rules can only be applied and have no practical significance.

For enterprise data, although Chinese laws have never clearly defined rights, and regulations such as the Anti-Unfair Competition Law have not even stipulated the concept of "data," different directions provide adequate protection for data rights. In the case of unfair competition dispute between Beijing Zhongrui Cultural Communication Co., Ltd. and Beijing Horizon Market Investigation and Analysis Company in the Supreme People's Court Gazette, the court found that "commercial information that is practical to specific industry practitioners and can bring economic benefits to the rights holders" belongs to the business secrets of the enterprise, if the trustee discloses the relevant commercial information obtained during the investigation, it means that the principal's trade secrets are made public, which is an unfair competition behavior that infringes on trade secrets and should bear corresponding civil liability The protection standards applied by the court, in this case, are similar to the liability rules.

European and American countries generally protect data rights and promote data utilization through trade secret protection laws, intellectual property laws (protecting copyright and database rights), contract laws, competition laws, personal information protection laws, criminal laws, etc [11].

In the case of Ryanair, which was presented to the Court of Justice of the European Union by the Dutch Supreme Court, the Court ruled that in the absence of specific legal protections for databases, licensors are not prohibited from imposing contractual restrictions, provided that such restrictions do not contravene competition law. The right holder is permitted to employ contractual arrangements to safeguard its data rights and interests, including the retention of data or engagement of third parties, based on the particular circumstances at hand.

### 4.2. Inadequate Corporate Data Protection under Current Loss

For the legal protection of enterprise data, although the existing legal framework provides different forms of protection, these other protection methods and approaches also have shortcomings. First, as far as trade secrets are concerned, trade secrets have a limited scope of protection for enterprise data. Trade secrets can protect enterprise data that is not disclosed, and enterprises take reasonable measures to ensure their confidentiality. However, trade secrets cannot adequately safeguard semi-public or public data collected by Internet enterprise platforms [12].

Secondly, protecting enterprise data by competition law faces the problem of uncertain rules. Take China’s current unfair competition judgments involving data as an example. The majority of assessments rely on the provisions outlined in Article 2 of the Anti-Unfair Competition Law. This article mandates that companies adhere to the principles of voluntariness, equality, fairness, and integrity, while also complying with laws and business ethics. Furthermore, it stipulates that acts which disrupt the order of market competition and harm the legitimate rights and interests of other operators or consumers are considered instances of unfair competition. From a jurisprudential point of view, this competition law provision is closer to a standard or moral requirement and lacks the rigidity of rules that can guide referees [13].

Although this provision can provide a certain degree of legal protection for various types of corporate data, it may also confuse all parties. What is "business ethics"? What is "disrupting the order of market competition"? Laws often lack clear legal interpretation and application standards. As a result, businesses often face higher costs in terms of compliance and data practices.

To ensure their data compliance, some companies may prohibit or cancel the data services they initially engaged in, or they may be unwilling to open the data they were initially willing to open because they are worried that the law will not protect their data enough.

Thirdly, protecting corporate data utilizing criminal and tort laws will also face some problems. The criminal law protection of enterprise data may be too strict. In terms of legal theory, certain rights will generally be protected by private law or administrative law first. Only when the protection of personal and administrative law is exhausted criminal law punishment will be adopted. Directly using criminal law to protect certain rights and interests, although it will have a significant deterrent effect, is contrary to the modesty of criminal law. Specific acts of illegal data acquisition have not yet reached the level of criminal punishment, although they are only like unfair competition, infringement, or other civil violations. Although tort law can provide additional protection for corporate data, this protection also faces uncertainty. When a company obtains another company's data, the tort law cannot answer which situation is data infringement and which case is the typical data acquisition. It still relies on the definition of law on data ownership issues.

Finally, contract law is not enough to protect corporate data. In protecting enterprise data through contract law, the premise is that there is a pre-contractual arrangement. That is, there is an express or presumed contractual relationship. Most companies cannot enter into data contracts with potential infringers in advance. Even if there is such a contract, companies cannot exclude unspecified third parties from infringing on their data rights. In real life, the acquisition of corporate data often comes from third parties, and it is difficult for contract law to provide relief for these third-party violations.

## 5. Corporate Obligation to Work with the Government

### 5.1. The Role of Business in Public Services

The involvement of businesses in public services has become more significant, necessitating a critical partnership between businesses and governments to ensure the delivery of effective, accessible, and innovative public services.

#### 5.1.1 Businesses using health codes as an example cooperate with the government

The health code has been an essential tool in the response to global epidemics in recent years, helping governments and public institutions to track, manage, and control outbreaks. However, implementing health codes requires vast data collection, processing, and analysis capabilities, which many government agencies cannot accomplish alone. This leads to cooperation between businesses and governments.

Businesses can provide governments with critical technology and resources to support the implementation of health codes. For example, technology companies can develop health code applications that collect users' health information and generate corresponding health codes. Cloud computing and big data companies can provide data storage and analytics services to help governments process health data at scale. IoT companies can make intelligent sensors that monitor people's body temperature and other health indicators. The cooperation between these companies and the government has made it possible to efficiently roll out and manage health codes, helping to contain the spread of the epidemic.

Furthermore, organizations have the capability to offer assurances about security and privacy in order to safeguard the integrity of health code data. The preservation of data security is a fundamental concern within the realm of public services, given that the occurrence of extensive data breaches has the potential to jeopardize the well-being and confidentiality of the general population. The utilization of enterprise knowledge and technological advancements can assist governmental entities in establishing resilient data security mechanisms aimed at safeguarding health code data from malevolent intrusions or unlawful breaches.

In conclusion, taking the health code as an example, the cooperation between enterprises and governments has played a vital role in responding to the challenges of the global pandemic. This collaboration not only offers technical and resource assistance but also contributes to the safeguarding of data security and privacy. This underscores the significance of the role of business in the realm of public service, particularly in the context of addressing emergencies and global challenges.

### 5.1.2 The potential value of commercial data to social services

In addition to collaboration in emergencies, commercialized data also has potential value for social services. In the course of their regular operations, enterprises amass substantial volumes of data that possess the potential to enhance the efficacy and caliber of social services.

First, commercialized data can be used to predict and optimize the delivery of public services. For example, power companies can use smart meter data to predict energy demand to ensure a stable power supply. Transportation companies can use mobile app data to monitor traffic flow to improve urban traffic management. The commercialization of these data not only helps enterprises improve operational efficiency but also makes public services more sustainable and environmentally friendly.

Secondly, the commercialized data can also be used to improve the personalization of social services. By analyzing users' consumption behavior and preferences, companies can provide more personalized services. For example, e-commerce platforms can recommend products that users may be interested in, and healthcare companies can develop customized treatment plans based on individual health data. This not only improves user satisfaction but also improves the effectiveness of social services.

Finally, proceeds from commercialized data can be used to support social service projects. Businesses can use part of their proceeds for socially responsible projects such as education, healthcare, and environmental protection. We call this model "enabling philanthropy," which integrates business and social services to create a win-win situation. For example, a study exploring the value of commercialized data in social services demonstrated the commercial potential of personal data and its application in social services [14].

In summary, collaboration between business and government and the potential value of commercial data highlight the critical role of business in public services. This cooperation and innovation not only help to improve the efficiency of public services but also brings more opportunities for innovation and sustainable development in the field of social services. Therefore, treating businesses as partners in public services is a critical step towards more effective and intelligent social services.

## 5.2. Government-Business Cooperation Model

### 5.2.1 Facilitate data sharing with data protection.

The public nature of data does not mean that enterprise data does not need legal protection. On the contrary, the reasonable safety of enterprise data rights and interests can promote data sharing, and the goal of data sharing needs to protect the data rights and interests of enterprises reasonably. First, providing reasonable protection for enterprise data rights and interests will help enterprises produce data and improve the overall quantity and quality. One of the essential reasons for intellectual property protection is to encourage innovation by granting enterprises exclusive copyright or patent rights to enable enterprises to make venture capital and create new and valuable academic achievements [15].

### 5.2.2 Data cooperation under the principle of co-construction and sharing

This principle undoubtedly applies to data production as well. By reasonably protecting the rights and interests of enterprise data, enterprises will avoid the risk of being free ridden by competitors in data collection and data use and have the incentive to collect more data and conduct more valuable data analysis. Conversely, if the law does not protect corporate data adequately, enterprises may lack motivation to manage and utilize data actively and may rely more on free riders to obtain data. Second, providing reasonable protection for enterprise data rights and interests helps enterprises open and share data. For semi-public or non-public data owned by enterprises, enterprises may disclose such data or information more if the law provides sufficient protection for enterprise data to avoid a competitive disadvantage from disclosure and access to data. After all, the disclosure of enterprise data is also a kind of soft power of enterprises, which can radiate downstream to enterprises and other related enterprises and individuals and encourage other enterprises and individuals to pay more attention to and rely on the enterprise. Furthermore, as highlighted by Mark Lemely, in situations

involving trade secrets, corporations are more likely to refrain from implementing stringent secrecy measures for nonpublic material when legal provisions offer protection for trade secrets [16]. At the same time, trade secret data can also enter the trading market, allowing the circulation and diffusion of trade personal data [17].

## 6. Conclusion

In the digital age, data ownership and collaboration between government and business are critical. Shared resource-based data management provides an alternative approach to overcoming data access limitations, and modern data governance frameworks and data collaboration powered by decentralized learning technologies offer promising avenues for reconciling conflicting interests in data.

Today, the importance of data to enterprises is beyond doubt, and the analogy of data as "oil" in the new era has long been deeply rooted in the people's hearts. But this metaphor only reflects one of the multiple attributes of data - it only emphasizes the growing property rights of data but does not reflect the public attributes of data. Strengthening the reasonable protection of enterprise data rights and interests is conducive to promoting the opening and sharing of data. Under the appropriate security of the legal system, companies will have more incentives to disclose and share data and avoid taking excessive confidentiality or protective measures on data.

## References

[1] Fia, Tommaso. An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons. Global Jurist, 2021, 21(1): 181-210.

[2] Zuziak M K, Hinrichs O, Abdrassulova A, et al. Data Collaboratives with the Use of Decentralised Learning. Proceedings of the 2023 ACM Conference on Fairness. Accountability, and Transparency. 2023: 615-625.

[3] Hummel P, Braun M, Dabrock P. Own data? Ethical reflections on data ownership. Philosophy & Technology, 2021, 34(3): 545-572.

[4] Fadler M, Legner C. Data ownership revisited: clarifying data accountabilities in times of big data and analytics. Journal of Business Analytics, 2022, 5(1): 123-139.

[5] Baijens J, Helms R W, Velstra T. Towards a framework for data analytics governance mechanisms. 2020.

[6] Hart D. Ownership as an Issue in Data and Information Sharing: a philosophically based review. Australasian Journal of Information Systems, 2002, 10(1).

[7] Chandra S, Verma S. Big data and sustainable consumption: a review and research agenda. Vision, 2023, 27(1): 11-23.

[8] Zhan, Y., Tan, K.H., Li, Y. et al. Unlocking the power of big data in new product development. Ann Oper Res 2018, 270: 577-595 .

[9] D Robinson, H Yu, WP Zeller, EW Felten.,Yale JL & Tech., Government Data and the Invisible Hand, Government data and the invisible hand, 2008.

[10] Mikalef, P., Pappas, I.O., Krogstie, J. et al. big data analytics capabilities: a systematic literature review and research agenda. Inf Syst E-Bus Manage 2018,16: 547-578.

[11] European Commission. Legal Study on Ownership and Access to Data: A Study Prepared for the European Commission DG Communications Networks. Content & Technology by Osborne Clarke LLP, 2016.

[12] Chandra S, Verma S. Big data and sustainable consumption: a review and research agenda. Vision, 2023, 27(1): 11-23.

[13] Richard Posner. The Problems of Jurisprudence. Cambridge: Harvard University Press, 1990: 42-61 .

[14] Kalapesi C. Unlocking the value of personal data: From collection to usage. World Economic Forum technical report, 2013.

[15] Mark A. Lemley. The Economics of Improvement in Intellectual Property Law. Texas Law Review, 1997, (75) : 989-1084 .

[16] Mark A. Lemley. The Surprising Virtues of Treating Trade Secrets as IP Rights. Stanford Law Review, 2008,61: 311-353 .

[17] Kenneth J, Arrow. Economic Welfare and the Allocation of Resources for Invention. The Rate and Direction of Inventive Activity, 1962: 609-615.