Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 12, No. 2, 2025

Challenges to Data Sovereignty Under CBAM and China's Legal Response

Xinran Han *

Southwest University of Political Science and Law, Chongqing, 401120, China
*** Corresponding author Email:** 2022022071@stu.swupl.edu.cn

Abstract: The EU's Carbon Boundary Adjustment Mechanism (CBAM) poses a significant challenge to data sovereignty, especially for China and other developing countries. This paper systematically explores the legal nature of data sovereignty, the implementation process of CBAM and the data sovereignty conflicts it has triggered. It analyses how CBAM's requirements for emissions data disclosure affect China's legal and regulatory framework. In addition, the paper examines how other countries have responded to similar challenges and extracts valuable lessons for China's response. By assessing the international experience and the specific challenges faced by China, this study proposes a Chinese response strategy to strengthen China's data sovereignty while ensuring the necessary co-operation in the global carbon trading mechanism. The findings emphasise the need for China to improve its legal framework, strengthen cross-border carbon data regulation, and actively participate in international co-operation to mitigate the risks to data sovereignty under CBAM.

Keywords: CBAM; Data Sovereignty; Developing Country; International Economic Law.

1. Introduction

The global move towards green trade has given rise to regulatory mechanisms such as *the European Union's Carbon Border Adjustment Mechanism* (CBAM), which aims to address carbon leakage by imposing tariffs on imports based on their carbon footprint. While CBAM is seen as an environmental policy tool, it also has significant implications for data sovereignty. In its implementation, companies in exporting countries, including China, are required to disclose a large amount of emissions-related data in order to comply with EU standards. These requirements have raised concerns about the leakage of sensitive industrial data, giving rise to controversy over whether they infringe on national sovereignty.

This article explores the legal nature of data sovereignty and its implications in the context of CBAM. The paper first examines the theoretical underpinnings and legal definitions of data sovereignty, laying the groundwork for understanding the conflicts that have arisen during the implementation of CBAM. It then delves into the CBAM implementation process to identify key regulatory and compliance requirements. The study further analyses the specific challenges China faces in adapting to CBAM while protecting its data sovereignty and why. In addition, by reviewing international experiences, the paper highlights strategies that China can adopt. Finally, this paper proposes legal and policy solutions tailored to China's needs, advocating for improved regulation, enhanced data protection measures, and diplomatic engagement in global carbon governance. By addressing these issues, this study aims to contribute to a broader discussion of the contradictions between environmental policy and state sovereignty in international law.

2. International Law Basis of Data Sovereignty

The international law basis of data sovereignty is primarily rooted in the principle of State sovereignty. Sovereignty is an essential characteristic and special attribute of the State. Traditional sovereignty includes physical space such as territory, territorial sea and airspace, but with the development of science and technology and globalisation, modern sovereignty extends to the virtual space of the Internet, and even more so to the data under the jurisdiction of a country's territorial land, sea, airspace and network [1]. Although the concept of data security has not been formally put forward in the relevant international documents, in the *Tallinn Manual 2.0*, an important international handbook in the field of cyberspace made by the collective research of all countries, led by the United States, it is made clear that the various aspects of cyberspace and the cyber actions of a country cannot go beyond the scope of the principle of sovereignty, and it is confirmed that the principle of national sovereignty applies to the data within the territory of a country. Thus, Article 2 of *the Charter of the United Nations*: 'The principle of the sovereign equality of States and of non-interference in their internal affairs' provides a jurisprudential basis for the right of States to control data within their territories [2].

In recent years, a number of resolutions adopted by the UN General Assembly, such as *the 2013 resolution on the Right to Privacy in the Digital* Age as well as regional agreements, such as *Convention on Cybersecurity and Personal Data Protection of the African Union* have progressively recognised data sovereignty as an important component of modern sovereignty. In addition, *Information Technology Agreement (TIA)* under the WTO framework allows member states to restrict cross-border data flows on the basis of national security or public policy, further strengthening the legitimacy of data sovereignty However, the international community has yet to create a unified data sovereignty treaty, and countries practice this principle mainly through domestic legislation (e.g., *China's Data Security Law*), leading to inconsistencies in cross-border data governance.

3. Disputes about Data Sovereignty under CBAM

The implementation of the CBAM regulations is divided into two phases, a transition period from 1 October 2023 to 31 December 2025 and a formal implementation period begin at 2026, while it has structured the rules through three legislative documents (*CBAM Regulation, Transitional Phase Implementation Regulation and Annexes*): Firstly, the transitional reporting obligation. Third-country exporters are required to submit quarterly reports to the EU covering the 'total actual implied emissions' of imports from six major industries, including iron and steel, cement and fertilisers, including direct and indirect emissions. The report requires the disclosure of highly sensitive data, including: 1. details of the production process: country of origin of the goods, geographic coordinates of the production unit, name and contact details of the company; 2. technical parameters: production process routes, emission factors, power consumption data and emission factors; 3. description of differences in the accounting methodology: if a non-EU-standard methodology is used, core parameters such as the monitoring process need to be submitted additionally [3]. These data are related to corporate know-how, supply chain privacy and geographic information, and may be categorised as 'important data' or even 'confidential data'. Second, the obligation to make formal periodic declarations. Importers are required to declare the total volume of imported goods and their General House Gas (GHG) content for the previous year by the end of May each year and submit proof of payment of the carbon price. Chinese exporters need to systematically collect and maintain carbon price certificates throughout the supply chain, but the difference in carbon accounting standards between China and Europe (e.g., China adopts industry benchmarking, while the EU requires a full life-cycle assessment) will lead to a surge in data compliance costs. Finally, data control risk. Although Article 13 of the CBAM promises to honour confidentiality obligations for 'confidential data', it leaves two exceptions: the 'data sharing exemption' ,which permits the disclosure of confidential information to other relevant authorities or institutions when necessary for implementing CBAM effectively, and the 'priority of policy objectives', which allows the overriding of confidentiality obligations if doing so serves broader public policy goals, such as environmental protection or regulatory enforcement. These exceptions pose a potential risk to data sovereignty as they enable the EU to access and use sensitive data outside the control of the exporting country, despite formal guarantees of confidentiality.

This is a significant legal and compliance challenge for many countries included China, with requirements to disclose such data could expose industrial secrets and private information, which potentially undermines national data sovereignty. Specifically speaking, CBAM's data protection controversy is primarily a dispute between its unilateral extraterritorial jurisdiction and WTO compliance [4]. First, under international law, a country's regulations can only constrain behaviour within its territory, but CBAM's requirement that foreign companies disclose to the EU data on carbon emissions from their entire supply chain, including sensitive information on production outside their borders, constitutes a substantial interference with the data sovereignty of other countries. Some scholars argue that such a unilateral rule violates *the Vienna Convention* on the Law of Treaties' principle of "prohibition of interference in internal affairs" and may also contradict the non-discrimination requirements of *the WTO's Technical Barriers to Trade Agreement (TBT Agreement)*. For example, the EU's requirement that non-members adopt its carbon accounting methodology without reciprocally recognising other countries' certification systems is suspected of being a TBT. In addition, the EU's practice of unilaterally appointing third-party auditors further undermines the data control rights of data source countries.

4. The Nature of Data Disputes under CBAM

The data sovereignty controversy triggered by CBAM is essentially a transnational conflict between data sovereignty and data access rights in the context of globalisation. Data sovereignty emphasises a country's absolute control over data within its borders, while the right to use data is reflected in the fact that international actors, through regulation, compel the data source country to transfer part of its control in order to achieve specific policy goals. In *United States v. Microsoft Corp.* the U.S. government demanded that Microsoft provide email data stored on servers in Ireland, and Microsoft refused to cooperate on the grounds that the data was stored overseas, reflecting the conflict between data sovereignty and the right to use.

Under the CBAM framework, the EU required exporters to submit carbon emission data covering the entire supply chain, including sensitive information such as raw material acquisition and production processes, creating a conflict between data sovereignty and the right to use data. The root of this conflict lies in the EU's unilateral rules to impose its own carbon data standards on other countries, forcing the others to disclose industrial data. For example, the EU requires Chinese companies to provide data on the energy used in the smelting process, whic h could expose details of supply chains in sensitive industries such as rare earths and threaten China's industrial security, while the EU has neither similarly disclosed the same kind of data from local companies nor committed to restricting the use of the data, further highlighting the asymmetry of power. This controversy is not only a battle for legal jurisdiction, but also a competition in the era of the global digital economy. In the face of this conflict, the international community should strengthen cooperation to clarify the boundaries between data sovereignty and the right to use, as well as to build a fair mechanism for mutual recognition of technical standards.

5. Conflicts Between CBAM and Data Sovereignty of China

For China, the potential risks of data sovereignty associated with CBAM are substantial. The disclosure of carbon emissions data, including information on the energy mix, manufacturing processes, and supply chains, could expose Chinese industries data to regulatory scrutiny beyond the EU. Moreover, the need to verify and disclose this data could involve significant administrative and compliance costs, disproportionately affecting smaller companies and industries with limited resources to manage complex data reporting systems. Besides, there are also concerns regarding the potential misuse of sensitive information.

China faces data sovereignty issues arising from CBAM, mainly caused by the following reasons: i) stringent data exit policies and fragmented legislation, leading to ambiguous

application of the rules; ii) insufficient data classification and full-cycle regulatory mechanisms, making it difficult to balance security and efficiency; and iii) the lack of an effective interface with the CBAM rules, and the lack of an international mutual recognition mechanism [5]. These problems reflect the contradiction between sovereignty and openness in the governance of cross-border data flows in China.

5.1. Stringent Data Exit Policies and Fragmented Legislation

China is currently adopting a regulatory model of 'sovereign protection of data security', with the *Cybersecurity Law*, *the Data Security Law* and *the Personal Information Protection Law* as the core of its strict control over the export of data[6]. China's policy of requiring data operators in key areas to store data within its borders and subject it to security assessments and ongoing monitoring when it leaves the country hinders the free flow of data. For example, routine corporate carbon emissions data may be categorised as 'important data', triggering unnecessary security reviews and increasing compliance costs.

Meanwhile, China's current legislation is also flawed. First, the rules are scattered. Data exit clauses are scattered across multiple laws and industry regulations (e.g., the Central Bank's '*Guidelines for Financial Data Security Classification*'), and the lack of a unified top-level law makes it difficult for companies to understand the data regulation rules. Second, the core concept is vague. The definition of 'important data' and 'core data' is unclear, and documents such as the Network Information Office's '*Regulations on the Management of Network Data Security (Draft for Public Comments)*' do not specify the specific classification of carbon emissions data, leading to ambiguity. Lastly, the lack of industry rules. The six major industries covered by CBAM, such as iron and steel and cement, are all strategic industries in China, but the lack of data exit rules for carbon emission scenarios has led to compliance conflicts for enterprises [7]. For example, the production process routes required to be disclosed by the EU may involve core data prohibited from leaving the country under Article 36 of *the Data Security Law*, but there are no clear exemption clauses or security assessment guidelines in China.

5.2. Insufficient Data Classification and Full-Cycle Regulatory Mechanisms

Although China has initially established a data classification system in the industrial and financial sectors, there is still a gap in the classification standards for carbon emissions data. Existing rules are based on economic and security impacts, but are not adapted to the strategic attributes of carbon emissions data. For example, the 'smelting process parameters' of an iron company may be classified as ordinary production data, but its relevance to the layout of the country's resources means that the actual risk far exceeds the classification. In addition, the lack of clarity in categorisation has led to regulatory problems. The scope of China's outbound data security assessment is vague, with routine carbon data easily generalised as 'important data' triggering a complex approval process, and there is no accountability mechanism for the misuse of data outside China after the fact. Although the Regulation on *the Regulation and Facilitation of Cross-border Data Flows (Draft for Public Comments) 2024* has made some initial improvements, there are still no specific rules for CBAM high-frequency data flows [8].

5.3. The Lack of an Effective Interface with the CBAM Rules

China's existing legislation is not sufficiently compatible with international rules. China's data legislation focuses on regulation within its borders and lacks effective interface with data governance rules in other countries. For example, there are technical barriers between China's carbon accounting standards and the EU's full life-cycle assessment methodology, and the lack of mutual recognition agreements requires companies to repeatedly submit data, leading to a surge in compliance costs.Besides, international participation is lagging behind. Europe and the United States have constructed exclusive data alliances through the Privacy Shield Agreement and so on, while our country's process of joining *the Digital Economy Partnership Agreement (DEPA)* and *the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP)* has faced conflicting rules. China lacks cooperation with other countries on cross-border data governance. Below is the revised section for your document. It's written in English and incorporates real, broadly described practices from Brazil and India—without fabricating details—and then presents China's responses accordingly.

6. China's Response Strategies to Data Sovereignty Challenges under CBAM

China faces significant challenges under CBAM due to the EU's extraterritorial demands for detailed carbon emissions data. To address these challenges, China can learn from real-world practices in other countries, particularly Brazil and India, and then tailor responses that suit its unique legal, regulatory, and industrial landscape.

6.1. Building a Carbon Emissions Data Classification and Management System, and Perfecting Domestic Regulation

Developing countries lag behind developed countries in terms of information technology and data processing, and lack strong data diversion capabilities; once fully deregulated, a large amount of data will flow to developed countries, leading to reduced competitiveness in trade; therefore, countries such as Brazil and India focus on the local protection of data in data governance. Brazil has taken a major step forward in data protection and regulation through the enactment of *the General Data Protection Act (Lei Geral de Proteção de Dados, LGPD)*. The LGPD, which comes into force in 2020, provides a comprehensive legal framework for classifying and categorising data, clarifying data definitions, setting strict conditions for cross-border data transfers, clarifying the responsibilities of data controllers and processors, and clarifies the responsibilities of data controllers and processors. For example, Article 33 provides that cross-border transfers of key industry data are subject to approval by *the National Data Protection Agency (ANPD)*. In addition, Brazil has implemented initiatives such as *the Brazilian Greenhouse Gas Registry (Registro Brasileiro de Emissões e Remoções de Gas de Efeito Estufa)*, which serves as a centralised system for tracking carbon emissions data. This registry supports transparent monitoring and its structured data classification methodology provides the basis

for data classification, which helps to protect sensitive information.

As a developing country, China should also focus on protecting indigenous data. Drawing on Brazil's example, China should consider developing a similar framework tailored to its carbon emissions data. First, China should improve laws such as *the Data Protection Law*, set clear procedures for cross-border flow of data, and define data [9]. Secondly, carbon emission data has both property and public attributes, and its reasonable classification and grading is the key to balancing security control and cross-border flow efficiency. China can classify data into general data, core data and important data based on the existing Cybersecurity Standard Practice Guidelines - Guidelines for the *Classification and Rating of Network Data.* General data refers to non-sensitive basic information, such as total product carbon emissions. Important data usually involves national security or public interest, e.g. carbon emission production parameters of steel exporters. Core data refers to data that directly threaten strategic security, such as the energy structure of rare earth smelting. The categorised data is then refined according to industry, taking into account factors such as data complexity, industry scale and industry requirements, to create a final inventory of carbon emissions data. The most important thing in this process is to distinguish between personal information and important data. For personal information, reference can be made to the relevant provisions of *the Digital Economy Multilateral Economic and Trade Agreement (DEPA)*, to which China is a party, and the Personal Information Protection Act for protection. The identification of critical data under the CBAM framework can follow the following methodology, firstly, determining whether the data involves core technology or supply chain information in key industries such as energy and defence. Second, verify whether the exporting enterprise is a critical information infrastructure operator. Again, clarify whether the data contains technical details of environmental monitoring that have not been disclosed by China. Finally, assess whether the coordinates of the country of origin of the goods, the place of production and the total amount of data meet the scale values set by the state. Through multiple verifications, high-risk carbon emission data can be precisely targeted.

6.2. Setting up a Dedicated Cross-Border Carbon Emissions Data Regulator

With the booming of the digital economy, effective regulation of data security has become an important issue. The regulation of carbon data has also become an important element in green trade. In order to further cater for this development, clarify the responsibilities of the regulatory body of cross-border data and improve its internal coordination system, China can learn from the EU experience and set up a specialised cross-border data regulator to co-ordinate cross-border data flows at the national level. With the booming of the digital economy, effective regulation of data security has become an important issue [10]. The regulation of carbon data has also become an important element in green trade. In order to further cater for this development, clarify the responsibilities of the regulatory body of cross-border data and improve its internal coordination system, China can learn from the EU experience and set up a specialised cross-border data regulator to co-ordinate cross-border data flows at the national level.

Chapter 6 of the EU's General Data Protection Regulation (GDPR) stipulates that member states are required to set up independent data regulators, whose core functions include two aspects: one is to protect the fundamental rights and freedoms of EU citizens in cross-border data flows, and the other is to promote the free flow of personal data within the EU. Under the GDPR, these supervisory authorities must be independent from government and other external interventions and exercise investigative, corrective, authorising and recommending powers in accordance with the law. At the same time, the regulators are required to cooperate with each other through consistency mechanisms, including sharing regulatory information in an electronic, standardised format and handling cross-border cases through a joint decision-making process, in order to avoid regulatory conflicts between member states. This system balances data protection and flow through a combination of independent regulation and exchange and cooperation.

Applying the EU GDPR experience to China's practice of exploring the cross-border flow of data, China's carbon data outbound regulator needs to have the following responsibilities:

Coordinate the cross-border data regulation of different industries and contents to avoid the problem of duplicated regulation due to the problem of unclear internal division of labour and unequal standards. Carbon emission related enterprises also need to take certain responsibilities. Enterprises should strengthen self-management and assessment and formulate data monitoring plans. Before carbon data leave the country, preliminary judgement should be made on the data involved, i.e. whether they are important data, the legitimacy of the data leaving the country, and the ability to resist risks, so as to reduce the burden on the relevant state subjects and strengthen the effectiveness of the supervision. Meanwhile, full-cycle supervision of cross-border data, from collection, transmission, storage, processing, exchange to destruction, to solve the problem of insufficient supervision after leaving the country. Focus on post-data supervision. Existing regulatory measures are limited to risk-taking and recourse for data processors, and a mechanism for continuous tracking and reporting of data out of the country should be established, as well as a withdrawal system. At the same time, regulatory cooperation on data exit should be strengthened. Through multilateral agreements or international conferences, mutual trust and mutual recognition of data cross-border regulatory policies with data powerhouses such as the United States should be established, and joint efforts to create a regulatory mechanism on [11].

6.3. Enhancing International Dialogue and Building Trust through Multilateral Agreements and Secure Data Transmission Channels

Although attitudes towards data flow vary greatly from country to country due to economic and cultural differences, international co-operation is bound to become an important means of cross-border flow of carbon data. At present, of all the free trade agreements in which China participates, only *the Regional Comprehensive Economic Partnership* (RCEP) directly provides for cross-border data flow, and with the development of global trade, cross-border data is urgent.

For CBAM, China can realise cooperation on cross-border carbon data flow in the following approaches. Firstly, Setting up database. Currently, *the Intergovernmental Panel on*

Climate Change (IPCC) requires that data cited in climate change assessment reports must come from EU or the US. The EU CBAM mechanism uses a carbon accounting database developed by the EU's Environment Department. China's carbon emission data are mainly released by the governments or scientific research institutes of developed countries, and the lack of an independent accounting organisation affects export trade and economic development. The Government and relevant institutions can take the lead in building a carbon emissions data platform with international influence and based on the national conditions of developing countries. It can break the monopoly of Europe and the United States through an independent database and avoid the inflated cost of carbon tariffs.

Secondly, Opening a carbon emission data transmission channel between China and EU. Many countries around the world have facilitated the mutual recognition of carbon data with the EU through the establishment of carbon emission data transmission channels. For example, the United States and Europe have promoted the integration of their carbon data protection systems through three ministerial meetings of the US-EU Trade and *Technology Committee (TTC)* Based on the GDPR, the UK has actively reached a trade agreement with the EU and reached cooperation on carbon pricing. Meanwhile, Japan has docked into the EU data space through the 'Ouranos system'. China can reach an agreement with the EU on the transmission of carbon emission data between China and the EU on the basis of respect for data sovereignty and promote a mechanism for cross-border mutual recognition of carbon emission data. China can agree with the EU on responsibilities and try to promote to the EU the full-cycle supervision measures adopted by China based on its data classification system, so as to strengthen data protection and supervision and provide a favourable data protection environment for the development of the digital economy [12].

Building on these international practices, China should promote coordination and co-operation on data sovereignty issues through bilateral, inter-regional trade agreements (RTAs) or free trade agreements, pursuing dialogue and cooperation at both bilateral and multilateral levels to develop a secure, mutually acceptable framework for carbon data exchange under CBAM.

7. Conclusion

The implementation of the EU's Carbon Boundary Adjustment Mechanism (CBAM) highlights the tension between global environmental governance and national data sovereignty. For China, CBAM's extraterritorial data disclosure requirements pose significant risks to sensitive data. Domestically, China must improve its data governance framework by establishing a clear categorisation for carbon emissions data. Strengthen cross-border data regulation through a dedicated oversight body. Internationally, China should advocate for mutual recognition of carbon accounting standards and seek bilateral or multilateral agreements to ensure fair data sharing mechanisms. Initiatives such as developing an independent carbon emissions database and negotiating secure data transfer channels with the EU could reduce reliance on external frameworks while maintaining sovereignty. These approaches have broader implications for developing countries in dealing with similar relationships of sovereignty and global economic integration.

References

[1] Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge University Press.

[2] Leal-Arcas, R., Faktaufon, M., & Kyprianou, A. (2022). A legal exploration of the European Union's carbon border adjustment mechanism. European Energy and Environmental Law Review, 31(4).

[3] Zhang, H. Y. (2023). Regulatory dilemma of carbon emissions data export and China's solution: Against the background of CBAM. Peking University Law Review.

[4] Geng, X. Y. (2024). The governance of cross-border data flows in trade agreements: A study on the "freedom–regulation" dilemma. Journal of Changzhou University (Social Science Edition), (3), 52–62.

[5] Wolff, H. V. H. (2013). Territorial sovereignty and neutrality in cyberspace. International Law Studies, 89, 123–124.

[6] Hong, Y. Q. (2021). On classification and hierarchical protection of data from the perspective of national security. China Law Review, 5.

[7] Zhang, Q., & Chen, Y. (2022). Research on data classification and grading methods and practices. Technology and Market, 29(8), 150–153.

[8] Xu, D. S. (2022). Building a cross-border data flow system aligned with international rules. Foreign Economics and Trade Practice, (1), 72–76.

[9] Hong, Y. Q. (2021). Data classification and grading protection from the perspective of national security. China Law Review, (5), 142–158.

[10] Chen, S., & Ma, Q. (2022). China's approach to regulatory coordination of cross-border data flows. China Business & Market, 36(9), 116–126.

[11] Liang, Y., & Wu, D. (2018). Implications of the EU's GDPR strict regulatory model for data governance in China's financial industry. Finance Technology Times, (9), 27–29.

[12] Zhang, Z. L. (2024). A study on the carbon emissions data reporting obligations under the EU CBAM. Journal of Information Science, 43(7), 172–178.