

Research on Cross-border Data Flow Governance Under RCEP: A Case Study of the Current Situation of Ningbo's Smart Manufacturing Enterprises Going Global

GU Xiang

College of Science & Technology Ningbo University, China

Received: March 11, 2026

Accepted: April 15, 2026

Published: June 30, 2026

To cite this article: GU Xiang. (2026). Research on Cross-border Data Flow Governance Under RCEP: A Case Study of the Current Situation of Ningbo's Smart Manufacturing Enterprises Going Global. *Asia-Pacific Journal of Humanities and Social Sciences*, 6(2), 011–020, DOI: 10.53789/j.1653–0465.2026.0602.003

To link to this article: <https://doi.org/10.53789/j.1653–0465.2026.0602.003>

Abstract: At present, data, as a new type of productive force, has greatly promoted the development of the global digital economy. However, it should also be noted that while digital trade promotes the integration of regional digital economies, it also brings multiple challenges such as privacy protection and cyber security. Therefore, different countries have successively formulated corresponding laws and regulations and established dispute resolution mechanisms for cross-border data flows within the region. Among them, the Association of Southeast Asian Nations (ASEAN) countries, in order to strengthen economic exchanges, signed the Regional Comprehensive Economic Partnership (RCEP), which initially established the basic rules for cross-border data flows within the region in the e-commerce chapter, reflecting the attitudes of various countries towards data governance and being an exploration and attempt to balance the free flow of data and national security. As an important cluster area of smart manufacturing, Ningbo City in China is facing practical pressures and challenges in terms of cross-border data compliance, privacy, and security. Based on the relevant provisions of RCEP, this paper discusses the construction of a multi-center collaborative cross-border data governance model and puts forward policy suggestions from multiple levels such as regional organizations, countries, localities, and enterprises, with the aim of providing references for promoting the high-quality and safe development of the regional digital economy.

Keywords: Cross-border data flow; RCEP; digital governance; data risk identification; multi-center governance

Notes on the contributor: GU Xiang holds a doctorate degree in Law, and she is a lecturer and researcher in Area Studies at the College of Science & Technology, Ningbo University. Her major research interest lies in the intersection of Area Studies and Law. Her email address is guxiang1015@foxmail.com.

RCEP 跨境數據流動治理研究

——以寧波智造企業出海現狀為例

顧 鄉

寧波大學科學技術學院

摘要:目前,數據作為新質生產力,極大推動全球數字經濟的發展。但是也應注意到數字貿易在推動區域數字經濟融合的同時,也會帶來隱私保護、網絡安全等多重挑戰。為此,不同國家都紛紛制定相應的法律法規,並且構建區域內的數據流動的爭端解決機制。其中,東盟各國為了加強經濟交流,簽訂的《區域全面經濟夥伴關係協定》(RCEP)在電子商務章節初步確立了區域內數據跨境流動的基本規則,體現了各國治理數據的態度,是在促進數據自由流動與維護國家安全之間的平衡的探索和嘗試。中國寧波市作為重要的智能製造集聚區,面臨跨境數據合規、隱私與安全等方面的現實壓力和挑戰。本文基於 RCEP 相關條款,探討構建多中心協同的跨境數據治理模式,並從區域組織、國家、地方及企業多個層面提出政策建議,以期為推動區域數字經濟高質量與安全發展提供參考。

關鍵詞:跨境數據流動;RCEP;數字治理;數據風險識別;多中心治理

一、引言

在全球數字化轉型的浪潮中,數據是關鍵生產要素與戰略性資源,其跨境流動不僅推動經濟增長,也在重塑國際競爭與合作的模式。^[1] 傳統國際貿易主要圍繞貨物、資本和服務展開,而在智能製造、跨境電商、平臺經濟和全球供應鏈高度融合的背景下,數據已經成為連接研發設計、生產協同、物流調度、客戶服務和市場反饋的關鍵生產要素。然而,跨境數據流動在提升資源配置效率和推動區域數字經濟融合的同時,也帶來了隱私保護、網絡安全、商業秘密泄露、數據主權衝突和監管管轄權重疊等複合型風險。因此,如何在促進數據自由流動與維護數據安全之間形成制度平衡,已經成為國際經貿規則競爭和全球數字治理的重要議題。^[2]

《區域全面經濟夥伴關係協定》(RCEP)的簽署與生效,為亞太地區跨境數據流動的治理提供了新的制度框架與實踐契機。作為當前全球規模最大的自由貿易協定,其人口與經濟總量約占全球三成,也被視為推動區域內數字互聯互通、構建『數字絲綢之路』的關鍵機制之一。^[3] RCEP 不僅關涉貨物貿易、服務貿易和投資便利化,也在第十二章『電子商務』中對線上消費者保護、線上個人信息保護、計算設施位置和通過電子方式跨境傳輸信息等問題作出規定。該框架傾向於採取『有條件開放+合作治理』的路徑,^[4] 體現出亞太國家在數據主權與數字開放之間的務實平衡。RCEP 所代表的折中式治理嘗試,為區域內協調數據政策、深

[1] 洪永渺,張明,劉穎:《推動跨境數據安全有序流動引領數字經濟全球化發展》,《中國科學院院刊》,2022年第10期,頁1418-1425。

[2] 張學博,王智韜:《RCEP 數據跨境流動規則與中國數據跨境流動立法研究》,《特區實踐與理論》,2024年第1期,頁98-105。

[3] 馬文婷:《中國—東盟共建『數字絲綢之路』:問題表征及路徑選擇》,《經濟問題》,2025年第4期,頁23-31。

[4] 同註②,第2頁。

化數字貿易合作奠定了制度基礎,但其能否在實踐中妥善調和數據自由流動與安全管控之間的張力,^[1]仍有待進一步觀察與檢驗。

對中國而言,RCEP 既為國內數據跨境流動法律體系的完善提供了外部契機與對接框架,也為中國在亞太區域數字治理中發揮建設性引領作用、提升規則話語權創造了重要窗口。寧波作為我國重要的製造業基地、港口城市和外向型經濟重鎮,為觀察 RCEP 框架下跨境數據流動治理提供了具有代表性的地方樣本。2025 年,寧波市進出口總值達到 2.6 萬億元;其中,對東盟進出口 2162.2 億元,同比增長 15.2%,顯示出寧波與 RCEP 區域市場之間日益緊密的經貿聯繫。更重要的是,寧波的外貿結構與智能製造、機電產品、家用電器、通用機械設備、汽車零部件等產業密切相關,這些產業在出海過程中高度依賴數字化供應鏈管理、跨境售後服務、遠程設備運維和海外市場數據反饋。換言之,寧波企業參與 RCEP 區域合作的過程,不僅是貨物貿易擴張的過程,也是數據跨境流動頻率、規模和複雜性不斷提升的過程。^[2]

基於此,本文擬圍繞以下問題展開研究:第一,RCEP 電子商務章節中的跨境數據流動條款體現了何種制度邏輯,其與美國、歐盟及其他亞太數字貿易規則相比具有何種差異?第二,寧波智能製造企業在參與 RCEP 區域貿易和產業鏈協作過程中,主要存在哪些跨境數據流動場景和風險類型?第三,在 RCEP 柔性治理框架下,如何構建兼顧數據自由流動、企業合規成本和國家安全利益的多中心治理模式?

二、RCEP 數據條款的制度理論框架

跨境數據流動並非單純的技術傳輸問題,而是嵌入國際經貿秩序、國家監管權力、企業合規結構與區域制度協調之中的複合型治理問題。RCEP 框架下的數據條款不能僅從貿易自由化角度理解,而應置於制度經濟學、風險治理和多中心治理的交叉視野中加以分析。

從制度性質看,RCEP 數據條款體現出一種典型的『嵌入式自由化』邏輯:一方面,其通過跨境信息傳輸和計算設施本地化規則,推動區域數字貿易便利化;另一方面,又通過合法公共政策目標和基本安全利益例外,為成員國保留必要的監管空間。這種制度安排既不同於強調數據高度自由流動的市場優先模式,也不同於以隱私權和數據保護為中心的強監管模式,而是在成員國發展階段、監管能力和安全關切存在顯著差異的背景下形成的折中式制度選擇。由此,RCEP 跨境數據流動規則的理論解釋,應當圍繞三個問題展開:第一,制度差異如何影響數據跨境流動的交易成本;第二,數據流動如何生成跨國擴散性風險;第三,在規則柔性和風險複雜性並存的條件下,何種治理結構更能實現開放與安全之間的動態平衡。

(一) 新制度經濟學視角下的跨境數據流動

以諾斯為代表的學者指出,不健全或彼此衝突的制度設計會顯著推高交易成本,阻礙資源有效配置,從而制約經濟發展。同樣,在全球化貿易的背景下,各國政策不同是導致貿易摩擦的主要原因之一。就跨境數據流動而言,各國在數據出境、存儲與保護等方面的法律與監管政策各有不同,存在顯著差異,呈現碎片化的特征,這會加重企業合規負擔,產生顯著的『制度摩擦』。

跨境數據流動中的『制度摩擦』本質上是不同國家數據治理規則不一致所形成的制度性交易成本。對於寧波智能製造企業而言,這一問題尤為突出。智能製造企業的跨境經營並不只是出口產品,還涉及訂單

[1] 李瑤:《RCEP 框架下的數據跨境流動規製與中國立法調適》,《安徽大學學報(哲社版)》,2025 年第 5 期,頁 95-102。

[2] 寧波市人民政府辦公廳. 寧波市人民政府辦公廳關於印發中國(浙江)自由貿易試驗區寧波片區建設『樞紐自貿區』行動方案的通知(甬政辦發〔2023〕2 號). (20230119)[20260506]. https://www.ningbo.gov.cn/art/2023/2/21/art_1229716426_59451434.html.

管理、供應鏈協同、遠程設備運維、售後服務、客戶反饋和工業算法優化等連續性數據交換。如果 RCEP 成員國之間的數據規則缺乏協調,企業就必須在多個監管體系之間反復切換,進而削弱數字貿易的效率優勢。

(二) 風險社會理論對跨境數據流動的啟示

德國社會學家烏爾里希·貝克認為現代社會即風險社會,現代性在推動技術進步與工業發展的同時,也催生出大量難以預測、超越國界的系統性風險。這些風險往往具有全球擴散性,難以被傳統的民族國家治理體系所有效應對。

RCEP 數據條款所體現的核心張力在於:跨境數據流動需要開放規則以釋放數字經濟紅利,但數據風險又要求成員國保留必要監管權。二者並非簡單對立,而是需要通過比例原則、透明原則、非歧視原則和必要性審查加以協調。換言之,風險治理不能成為任意限制數據流動的理由,數據開放也不能以犧牲基本安全和公共利益為代價。RCEP 的制度挑戰正是在開放與安全之間建立可操作、可預期、可協調的平衡機制。

(三) 數字治理理論的應用

數字治理理論認為在面臨現代複雜的數據治理問題時,應突破傳統國家-政府的模式,轉向『多中心治理』模式。該模式認為,單一決策中心往往難以有效應對複雜局面,而多個相對獨立又相互關聯的決策主體,可通過協作、競爭與互補形成更富韌性的治理網絡,^[1]例如『國際區域組織-國家-政府-企業』這種多中心結構更能適應動態、跨域的政策環境,也有助於提升治理的整體效能與創新空間。具體而言,不僅包括國家、政府間的協議對接與政策協調,也需要企業切實承擔數據保護責任,同時離不開行業協會等組織在標準製定與合規指導方面的專業支持。^[2]

綜上所述,制度差異產生制度摩擦,制度摩擦提高企業合規成本;數據流動帶來風險擴散,風險擴散強化安全監管需求;RCEP 柔性規則提供基本協調框架,但其有效運行依賴區域、國家、地方和企業之間的多中心協同。跨境數據治理要結合多種理論共同搭建立體框架。新制度經濟學表明唯有通過國際協調與規則銜接,才能降低由此引發的合規與交易成本。風險社會理論則進一步指出,數據流動本質上嵌入了現代技術社會的系統性風險——數據泄露、網絡攻擊等威脅具有天然的跨國擴散性。而這些都是單一國家難以獨立處理的,必須依靠跨域協同的治理,推動國際組織、國家、政府、企業等多方主體共同參與,在動態平衡中實現跨境數據流動的有效治理。

三、RCEP 數據條款的制度及生成邏輯

RCEP 電子商務章節中的數據規則,是亞太區域數字貿易治理的重要制度嘗試。RCEP 第十二章明確提出,其目標包括促進締約方之間電子商務發展、創造可信任的電子商務環境以及加強締約方在電子商務發展方面的合作。

從制度性質看,RCEP 數據條款並非單純追求數據自由流動,也並非采取嚴格的數據本地化和安全優先模式,而是形成了一種『原則性開放、例外性保留、合作性協調、柔性化執行』的制度結構。其核心特征在於:一方面承認數據跨境流動對數字貿易和區域供應鏈協作的重要作用,另一方面又充分保留成員國基於公共

[1] 齊英程:《數據合規協同激勵體系的構建與完善》,《東方法學》,2024年第2期,頁98-108。

[2] 於清,石焱文,孫可欣,張兮:《數據要素市場發展影響因素組態分析——基於多中心治理的視角》,《科學學與科學技術管理》,2024年第4期,頁157-172。

政策、網絡安全和基本安全利益進行監管的空間。這種制度安排反映了 RCEP 成員國之間在發展階段、數字產業能力、監管能力和數據主權觀念上的差異，也體現了亞太區域數字治理的務實主義取向。

（一）RCEP 數據條款的核心內容與制度設計

RCEP 電子商務章節（第 12 章）專門規定了關於跨境數據流動的條款，^[1]其中包括關於數據傳輸、數據本地化及相關例外規則的內容。核心條款包括：

1. 基礎規則

RCEP 第十二章首先通過無紙化貿易、電子認證、電子簽名和電子傳輸免征關稅等規則，為區域數字貿易奠定基礎。無紙化貿易要求成員方努力接受電子形式貿易管理文件與紙質文件具有同等法律效力，電子認證和電子簽名規則則降低了跨境交易中的身份確認和合同締結成本。此類規則雖然並不直接規定數據出境條件，但其制度功能在於推動貿易流程數字化，使訂單、報關、物流、支付、售後等信息能夠在區域內更高效地傳輸和處理。

2. 消費者保護與個人信息保護規則

跨境數據流動能否持續發展，不僅取決於技術效率，也取決於交易主體對數據安全和隱私保護的信任。RCEP 第十二章第七條規定線上消費者保護，要求成員方採取或維持法律法規，以保護使用電子商務的消費者免受欺詐和誤導行為的損害；第八條則規定線上個人信息保護，要求每一締約方採取或維持保護電子商務用戶個人信息的法律框架，並在製定相關框架時考慮國際標準、原則、指南和準則。

3. 跨境信息傳輸與計算設施位置規則

RCEP 數據條款中最直接體現數據自由流動原則的是第十四條和第十五條。第十四條『計算設施的位置』規定，成員方不得將要求涵蓋的人使用或設置本地計算設施作為在其境內開展商業行為的條件；第十五條『通過電子方式跨境傳輸信息』規定，成員方不得阻止涵蓋的人為進行商業行為而通過電子方式跨境傳輸信息。

4. 合作、對話與柔性爭端處理規則

RCEP 數據條款的另一重要特征，是通過合作和對話機制處理成員國之間的制度差異。第十二章第四條規定成員方可以在幫助中小企業克服電子商務障礙、加強電子商務法律框架、開展能力建設、分享信息和最佳實踐等方面進行合作。第十六條進一步規定電子商務對話，成員方可就數字產品待遇、源代碼、金融服務中的跨境數據流動和計算設施位置等新興問題進行討論。

一般而言，數字化程度較高的發達國家更傾向於推動數據自由流動，以促進數字貿易與技術創新，例如日本和韓國；而部分發展中國家則更為關注數據安全、隱私保護及本土產業成長空間，例如柬埔寨和老撾可以在五年內暫不實施，允許適當延遲實施某些義務，體現了包容性。^[2]針對這一現實，RCEP 採取了『原則開放、例外靈活』的規範路徑，既確立了數據跨境流動的總體導向，也為成員國基於公共政策、安全等考量採取限制措施保留了空間。^[3]

[1] 中華人民共和國商務部. 區域全面經濟夥伴關係協定(RCEP): 第十二章 電子商務. (2020-11-15)[2026-05-06]. http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_cn.pdf.

[2] Bailey, Rishab & Parsheera, Smriti. (2018). Data localisation in India: Questioning the means and ends (NIPFP Working Paper No. 242). National Institute of Public Finance and Policy.

[3] 陳麗娜:《我國跨境數據流動規則的理論邏輯與體系重塑——基於圍獵博弈模型的分析》，《科技與法律(中英文)》，2023年第5期，頁61-72。

(二) 與其他國際協議的比較分析

為了準確理解 RCEP 數據條款的制度特征,有必要將其置於全球主要數據跨境流動規則模式中比較。總體而言,當前國際數據治理大致形成三種典型路徑:美國主導的自由流動優先模式、歐盟主導的隱私保護優先模式,以及亞太區域中較具折中性的開放—安全平衡模式。

1. 美國自由流動優先範式

美國在跨境數據流動治理上倡導高度自由化的模式,其主導的協議(如《美墨加協定》,USMCA)通常以推動數據完全自由流動為核心原則。這類協定往往嚴格限制成員國採取數據本地化措施,僅允許在極少數特定情況下對數據流動進行限制,並通過具有約束力的爭端解決機制保障條款執行。在此範式下,國家安全等理由難以構成設置數據流動壁壘的充分依據,成員國維護數據主權或加強隱私保護的國內舉措,容易被視為變相的貿易壁壘而受到約束。^[1]

2. 歐盟隱私與保護優先範式

歐盟則通過《個人數據保護條例》建立了一個嚴格的個人數據保護體系,相較於美國松散的管理模式,更強調個人信息和個人隱私保護,特別是對個人數據的跨境流動設定了高度的合規要求。歐盟模式下,數據流動受到強烈的隱私保護驅動,相較而言,RCEP 則更注重各國各自國家不同的法律規定,更具有包容性。^[2]

3. 亞太折中範式

CPTPP 與 RCEP 二者都規定了數據自由流動的規則,強調數據存儲本地化。其中 CPTPP 第 14.11 條要求允許跨境數據傳輸,且需『不構成任意或不合理歧視』並『不得較必要程度更嚴』。與 RCEP 相比,CPTPP 對『合法公共政策』這一例外原則做了更嚴格的限定,並未授權各國可以隨意使用此原因限制數據的自由流動。^[3] 另外,CPTPP 的數據條款對於各成員國而言更具有法定的效力,^[4]而 RCEP 通過在條款中明確國家安全可作為跨境數據流動的例外原則,客觀上允許了成員以安全為由保留部分數據管制。^[5] 這種靈活性是基於 RCEP 成員國各國的現實需求所決定的,因為其多為發展中國家,更希望保護數字主權的完整。而同為成員國日本、澳大利亞、韓國等多個發達國家,更希望獲得自由貿易的機會。由此可見,這些國家在數據主權、技術標準和數字產業發展思路上各有不同,立場並不完全一致。RCEP 區域內的數據流動規則已經不僅僅是一個經濟或法律問題,還被附加了地緣政治的色彩,各方在數據跨境合作中更加謹慎,要製定一體化規則顯得較為困難。整體而言,RCEP 的數據治理制度具有鮮明的『亞洲特色』,注重靈活性、包容性和合作性。^[6]

四、跨境數據流動現狀與風險

RCEP 框架下跨境數據流動治理的現實意義,只有放置到具體產業和地方經濟場景中才能得到充分理

[1] Geist, M. (2018). Data rules in modern trade agreements: Toward reconciling an open internet with privacy and security safeguards. *CIGI. Data Governance in the Digital Age; a CIGI Essay Series*. Waterloo: Centre for International Governance Innovation, 108-113.

[2] 熊光清,張素敏:《中國個人信息保護規範的域外適用:國際比較的考察》,《哈爾濱工業大學學報(社會科學版)》,2025年第5期,頁48-59。

[3] Canton, H. (2021). Organisation for economic co-operation and development—OECD. In *The Europa directory of international organizations* 2021 (pp. 677-687). London: Routledge.

[4] 宋俊榮:《我國數據跨境流動規製措施與 RCEP 服務貿易規則相符性及應對》,《當代法學》,2025年第2期,頁147-160。

[5] 蔣慧:《RCEP 背景下國際數字貿易規則的比較、挑戰與中國因應》,《廣西社會科學》,2024年第1期,頁77-84。

[6] 同註①,第3頁。

解。寧波作為我國重要的港口城市、製造業基地和外向型經濟高地，其智能製造企業在參與 RCEP 區域貿易過程中，已經形成高頻率、多類型、跨法域的數據流動結構。因此，寧波智能製造企業具有觀察 RCEP 跨境數據流動治理問題的典型樣本意義。

（一）智能製造企業跨境數據流動的典型業務場景

寧波製造業長期具有外向型、集群化和供應鏈嵌入程度高等特點。隨著智能製造和數字化轉型深入推進，企業生產經營過程中的數據密度顯著提高。數據既可能服務於普通商業活動，也可能涉及個人信息、商業秘密、重要生產數據乃至潛在的重要數據。因此，寧波智能製造企業的跨境數據流動，不應被簡單理解為『數據能不能出境』的問題，而應理解為『哪些數據、在何種場景下、以何種路徑、向哪些主體、基於何種法律依據出境』的精細化治理問題。結合寧波智能製造企業的出海實踐，可以將其跨境數據流動概括為四類典型場景：供應鏈協同數據流動、客戶服務數據流動、遠程運維數據流動和技術輸出數據流動。

1. 供應鏈協作與管理

供應鏈協同是寧波智能製造企業跨境數據流動最基礎、最頻繁的場景。在智能製造模式下，企業往往通過數字平臺進行實時管理，供應鏈數據呈現連續化、結構化和平臺化特征。例如，境外客戶可能實時查詢訂單進度，境外倉儲物流企業需要接收庫存和發貨指令，境外售後服務商需要獲取產品批次和零部件信息。隨著數據共享範圍擴大，企業面臨的合規問題也由單一貿易單證管理轉向全鏈路數據治理。該場景中的主要風險並不必然來自個人信息，而是來自供應鏈數據的商業敏感性。訂單規模、客戶名單、核心供應商、生產周期和庫存信息，均可能反映企業經營狀況和市場競爭策略。一旦相關數據被境外合作方不當使用，或因第三方平臺安全能力不足而泄露，企業可能遭受商業秘密損失、客戶流失和供應鏈議價能力下降。

2. 客戶服務與數據傳輸

客戶服務場景主要出現在跨境電商、海外售後、會員管理和用戶反饋等過程中。寧波智能製造企業銷售產品後，通常需要收集境外消費者的姓名、聯繫方式、地址、購買記錄、維修記錄、使用偏好和產品反饋等信息。若產品具有智能化功能，還可能進一步涉及設備識別碼、位置數據或影像數據。該場景的風險核心在於個人信息保護。企業如果沿用國內統一模板處理所有境外用戶數據，可能無法滿足目的國監管要求。例如，在日本、新加坡、澳大利亞等個人信息保護制度較成熟的市場，企業通常需要更加重視隱私政策透明性、用戶授權有效性、數據最小化和第三方共享限制。RCEP 第十二章也要求成員方採取或維持保護電子商務用戶個人信息的法律框架，並鼓勵企業公布與個人信息保護相關的政策和程序。^[1]

3. 工業數據跨境傳輸與安全邊界模糊

遠程運維是智能製造企業區別於傳統製造企業的重要數據流動場景。遠程運維數據的法律屬性較為複雜。一方面，設備狀態、故障日誌和維護記錄通常服務於售後目的，可能屬於一般經營數據；另一方面，如果這些數據能夠反映生產工藝、產能水平、設備運行規律、算法模型或客戶生產安排，就可能具有商業秘密價值。尤其是當企業使用境外雲服務平臺進行數據存儲、分析和遠程訪問時，數據控制權、訪問權限、平臺安全責任和境外監管調取風險都需要進一步評估。該場景說明，智能製造企業的數據出境合規不能僅以『是否包含個人信息』為判斷標準。工業數據雖然未必涉及個人信息，但其可能具有產業競爭價值和安全敏感性。企業需要通過數據分類分級、訪問權限控制、加密傳輸、日誌留存、境外接收方安全評估和遠程運維協議等方式，建立更精細的治理邊界。

4. 商業機密和算法模型輸出

[1] 郭德香：《RCEP 數據跨境流動基本安全例外條款適用問題研究》，《當代法學》，2025 年第 4 期，頁 149-160。

技術輸出場景主要包括境外建廠、海外聯合研發、智能工廠建設、工業軟件授權、算法模型部署和工藝流程共享等。寧波智能製造企業在拓展 RCEP 市場時,可能需要向境外子公司、合作夥伴或客戶提供產品設計方案、設備參數、工藝流程、工業軟件、算法模型和生產優化方案。這類數據通常具有較高技術含量和商業價值,是企業核心競爭力的重要組成部分。^[1]

(二) 跨境數據流動的風險識別

基於上述業務場景,寧波智能製造企業在 RCEP 區域跨境數據流動中主要面臨四類風險:制度合規風險、個人信息與消費者信任風險、數據安全與網絡攻擊風險、商業秘密與產業競爭風險。

1. 制度合規風險

目前東盟各國數據法規之間的差異與監管要求的分歧,^[2]制度的不統一,是造成寧波智能製造企業數據合規的首要解決難題。各國基於本身國情、法律傳統和現實需求,正沿各自路徑推進數據立法:^[3] 歐盟注重個人數據的保護,所以嚴格管理跨境數據,美國側重以市場為導向的數據自由流動,而中國則更強調數據主權與安全的優先地位。儘管 RCEP 在區域內倡導數據流動自由化,其條款仍允許成員國以『合法公共政策』和『基本安全利益』為由設置例外限制。

中國 2024 年《促進和規範數據跨境流動規定》實際上為企業提供了更加精細化的出境規則:部分國際貿易、跨境運輸、跨國生產製造和市場營銷活動中的一般數據可以適用便利化安排;達到一定個人信息數量或者涉及重要數據時,則需要履行更嚴格義務。這意味著企業合規能力的核心,正在從『是否申請審批』轉向『能否準確識別數據屬性並匹配適當合規路徑』。

2. 個人信息與消費者信任風險

在跨境數據流動過程中,個人數據的傳輸與存儲極易觸發隱私泄露風險。由於各國在個人數據的界定、保護標準及同意機制等方面存在明顯差異,例如中國的個人信息隱私與日本相關範圍就有所不同。所以,數據跨境行為可能因違反當地的消費者保護法規而造成侵權行為,從而影響企業聲譽與市場信任。例如,某升降桌企業就因未獲得用戶同意收集身高數據,而被罰款。^[4]

近年來,RCEP 各成員國持續加強個人信息保護立法,並對數據泄露事件采取日趨嚴格的執法措施。區域各國法律環境的不均衡,要求寧波企業在開展客戶數據跨境傳輸時,必須針對不同目的國的規定采取相應措施,如落實數據脫敏、遵循最小必要原則、獲取用戶明示同意等。若未能建立並執行這類技術與管理層面的高標準防護機制,企業將同時面臨合規處罰與客戶流失的雙重壓力。^[5]

3. 數據安全與網絡攻擊風險

跨境數據流動需要在不同司法管轄區域之間傳輸和存儲信息,這也使得數據面臨網絡攻擊與泄露的風險明顯上升。具體來看,在跨境傳輸過程中,數據容易遭遇中間人攻擊或惡意截取,導致敏感信息在傳送中被竊取或篡改。^[6] 具體而言,數據在跨境傳輸鏈路上易受到中間人攻擊或惡意攔截,導致敏感信息在傳輸過程中被竊取或篡改。^[7] 跨境數據流動,本質上是數據在不同法域之間的『遷移』。這個過程看似簡單,實則每一步都可能觸發不同的法律與安全機制。無論是供應鏈協同,還是客戶數據回傳,幾乎都離不開境外

[1] 劉洪槐,李欣波,許尚坤:《中美歐數字貿易發展戰略與政策比較研究》,《國際經濟合作》,2025 年第 5 期,頁 67-77。

[2] 許多奇:《個人數據跨境流動規製的國際格局及中國應對》,《法學論壇》,2018 年第 3 期,頁 130-137。

[3] 湯諍:《數據跨境流動國際規則碎片化與協調路徑》,《江西社會科學》,2025 年第 6 期,頁 112-124。

[4] 李姝卉:《數字貿易中的隱私權保護》,《華東政法大學學報》,2025 年第 1 期,頁 135-146。

[5] 梁燕妮:《數字經濟背景下的數據交易風險與合規治理研究》,《廣西科學》,2024 年第 2 期,頁 395-404。

[6] 文銘,李星熠:《「自由-規製」框架下跨境數據流動治理及中國方案》,《中國科技論壇》,2024 年第 4 期,頁 106-116。

[7] 廖麗,武子微:《國家安全例外條款在數據跨境流動中的適用研究》,《國際貿易》,2024 年第 8 期,頁 87-96。

雲基礎設施或第三方平臺。

4. 商業秘密與產業競爭

商業秘密與產業競爭風險是智能製造企業最容易被低估的風險。工業數據的風險在於，其價值往往不是單一數據本身，而是多組數據結合後形成的推斷價值。例如，單個設備運行參數可能並不敏感，但長期運行參數、故障日誌和生產節拍結合起來，可能反映企業核心工藝水平；單個訂單信息可能價值有限，但訂單頻率、客戶結構和交付周期結合起來，可能反映企業市場策略和供應鏈能力。因此，企業不能只按照傳統文件密級管理工業數據，而應關注數據聚合後的商業價值和安全敏感性。

五、RCEP 數據條款的制度『多中心治理』應對措施

面對跨境數據流動治理所呈現的複雜性與風險的多元性，急需一個多中心治理的模式，該模式應突破傳統政府為治理主體的思維模式，轉向『國際組織、國家、地方及企業』多元主體的協同治理模式，緩解因制度差異引發的治理衝突，從而抵禦風險。

（一）國際層面：加強規則協調與跨國合作

儘管 RCEP 已初步設定了數據流動框架規則，但各成員國的法律規定仍有不同，呈現碎片化的特點。制度的不銜接會導致貿易摩擦，所以有必要進一步細化相關規則，達成區域內的共識。例如可以在 RCEP 架構下成立專門的數據治理工作組，定期評估成員國相關法律法規的動態。該工作組還可為各國政府與企業提供政策解讀與操作指引，從而減少因規則差異引發的合規不確定性。

（二）國家層面：制度完善與政策創新

在 RCEP 框架指導下，各成員國需在國內層面加快完善國內立法與規則的銜接，為企業提供可預期的政策指引和良好的營商環境。

首先，健全分級分類的跨境數據監管法律框架。首先要建立數據分級標準，根據數據的性質和內容，將其分類為『一般數據—重要數據—核心數據』，並根據不同數據類別作出不同的法律規定和監管準則，實現精準化的管理。

其次，在自貿區中設立『沙盒監管』試點。可在自貿區或經濟特區建立建設監管點，幫助企業進行場景化的模擬和測評。同時，監管部門也可以實現實時的動態監測，並且及時調整政策。

（三）地方層面：地方試點與示範區建設

以寧波為例，在國家層面政策支持下，地方政府也應當積極探索體現地方產業特色的跨境數據治理實踐模式，履行服務型政府職能。

第一，『跨境數據流動綜合服務平臺』試點。寧波市政府可牽頭設立一站式服務平臺，整合政策諮詢、合規評估、風險預警等職能，為企業提供全流程輔導。

第二，構建『政產學研用』協同體系。可依托本地高校、研究機構及重點企業，聯合組建跨境數據治理研究中心，開展面向區域國別差異的政策研究。

第三，形成『行業自律+企業自查』的體系。鼓勵本地智能製造、跨境電商等主導產業的協會或聯盟，牽頭製定國家法規的行業數據保護公約與跨境流動操作指引。

(四) 企業層面:企業合規管理與技術創新

企業在參與跨境數據流動時,需主動提升數據合規意識,培養相關人才。

第一,建立常態化的數據合規體系。企業應設立專職團隊或崗位,負責跟蹤 RCEP 及各相關國家的數據法規動態,並據此完善內部跨境數據管理流程。通過定期的合規審計與風險評估,確保數據出境活動持續符合國際規則與目的地國法律要求。

第二,強化數據安全的技術保障與創新應用。在技術層面,應加大對傳輸加密、隱私計算等安全技術的投入。

第三,構建跨境數據風險應急體系。企業應提前製定跨境數據安全事件應急預案,一旦發生數據泄露、違規傳輸等事故,能夠迅速啟動處置程序,控制影響範圍。

六、總結:推動區域數字治理的可持續發展

RCEP 框架下的跨境數據流動治理,是一項長期的系統性工程。本文所構建的『國際—國家—地方與企業』多中心治理路徑,其核心在於承認沒有任何單一主體能夠獨立解決所有問題,必須通過各中心間的分工、協作與良性競爭,形成治理合力。國際層面著力於『建橋』以減少制度隔閡,國家層面致力於『立規』以穩定市場預期,地方與企業層面側重於『賦能』以激發內生動力。唯有如此,才能在享受數據跨境流動所帶來的巨大數字紅利的同時,有效駕馭其伴隨的各類風險,最終在 RCEP 區域內構建起一個開放、有序、安全且充滿韌性的數字命運共同體。

(Editors: LI Ruobing & Bonnie WANG)