功能主義視角下個人數據交易安全風險治理的進路轉向與構造

朱俊達*

摘　要　個人數據交易是促進個人數據有效流通、發揮數據價值、培育新質生產力的重要途徑之一，但與之相隨的個人數據洩露、被濫用等危害個人數據安全的現象亦日益凸顯。近年來，雖然國家相繼出台了多部法律對個人數據交易行為予以約束，但對個人數據交易安全風險的治理仍顯不足。究其原因，目前的規則供給與理論探索都體現了濃厚的規範主義色彩，多關注法律規則的概念化屬性與權利義務的傳統範式。然而，形式上完備整全的制度在實踐中可能出現效用不敷的困境。為此，對個人數據交易安全風險治理的探索可轉向功能主義，不再局限於規範本身，而是基於“目的—功能—手段”的分析框架，從培育治理主體、拓寬治理空間、延展治理時間和革新治理工具四個方面入手，構建功能主義視角下個人數據交易安全風險治理的新進路。

關鍵詞　個人數據交易　個人數據交易安全　安全治理　功能主義　規範主義

一、問題的提出

作為新質生產要素，數據要素參與經濟生產，形成新質生產力，促進社會財富的普遍增長。[1] 社會中的大部分數據由個人的日常活動產生，企業既能通過提供服務直接採集個人數據，也可通過數據交易的方式從數據來源主體獲取個人數據。關於個人數據交易概念的界定，學界對此有廣義與狹義兩種觀點。廣義論認為，除了企業間通過數據合同與數據傳輸行為進行數據交易以外，企業與個人之間藉由合同進行的持續的數據收集行為也屬個人數據交易之範疇。[2] 狹義論則強調數據交易

*　朱俊達，西南政法大學經濟法學院博士研究生。
本文係重慶市2025年研究生科研創新項目“企業數據資產化的制度構造研究”（項目編號：CYB25165）、2024年西南政法大學學生科研創新項目“企業數據資產質押融資的規範構造研究”（項目編號：2024XZXS-018）階段性成果。

[1]　參見黃尹旭、楊東：《“利益—權利”雙元共生：“數據要素×”的價值創造》，載《中國社會科學》2024年第2期，第49、61頁。

[2]　參見林洹民：《個人數據交易的雙重法律構造》，載《法學研究》2022年5期，第38頁。

主要是“對數據明碼標價進行買賣”，[3] 只不過相對於普通買賣，個人數據交易只是數據使用權的轉讓，賣方並未喪失對數據的持有與控制。[4] 基於這一界定，有學者指出個人數據交易多在企業間進行，而非發軔於數據用戶與企業之間。[5] 此外，《信息安全技術 數據交易服務安全要求》第 3.1 條也將數據交易定義為：“數據供方與需方之間以數據商品作為交易對象，進行的以貨幣或貨幣等價物交換數據商品的行為。”[6] 本文擬將狹義的個人數據交易作為研究對象，從解釋論的角度出發，其原因主要在於以下兩點：一是揆諸現行立法，如《個人信息保護法》和《數據安全法》業已將個人與企業間的數據流轉行為界定為收集行為，並於買賣行為相互區分。[7] 二是現行法律規範和政策當中已有諸如“數據交易場所”“數據交易中介服務機構”等指稱，這些概念中的“數據交易”應不包括“數據採集”之含義，從概念內涵一致性的角度考量，本文對個人數據交易作狹義解釋。

現有的個人數據交易活動主要涉及五類主體，包括數據來源方、數據供應方、數據交易服務機構、數據交易所以及數據需求方。上述主體參與的個人數據交易，在具體形式上可分為場外交易與場內交易兩種。場外交易一般由互聯網平台等數據供應方通過向數據來源方提供服務的方式收集大量個人數據，進而將相應的數據集合以動態或靜態的方式傳輸、共享給數據需求方，獲取一定的對價。在場內交易中，數據來源主體可不經數據供應方，而是通過“數據信託”等方式將個人數據授權給數據交易服務機構進行處理，再由數據交易服務機構經由數據交易所匹配數據需求方以達成交易。當然，收集個人數據的數據供應方也可以選擇在數據交易所內開展個人數據交易活動。

個人數據交易作為數據流通的重要形式之一，不僅能夠促進數據要素產生經濟價值，發揮乘數效應，而且是個人分享個人數據財產利益，平衡數據採集、處理等不同環節相關主體間利益分配的重要手段。在實踐中，貴陽大數據交易所在 2023 年完成了全國首筆個人數據合規交易，並為數據來源者分享了收益。[8] 然而與此同時，個人數據交易仍存在著不少危害個人數據安全的隱患。在交易進行階段，個人數據交易可能潛伏著個人數據濫用和倒賣的行為，還可能因為交易方安全資質不達標而無法防範系統漏洞、網絡攻擊等所造成的個人數據洩露現象。此外，安全風險並非僅來源於個人數據交易行為本身，還源自交易後對數據的處理、存儲等行為，如可能出現數據需求方超範圍使用數據，侵犯供方的合法權益，以及將數據進行二次流轉、轉賣等風險。[9] 數據交易使得個人數據處理的鏈條被無限拉長，從而進一步加劇了個人數據交易的安全風險。對此，立法者相繼出台了《數據安全法》《個人信息保護法》等法律進行規制。上述規範為個人數據交易行為提供了較為完備的規則指引，但是其中伴生的安全風險依然未被完全消除。在個人數據的場外交易場景中甚至存在著規模龐大、分工明確的數據黑產，對個人信息權益造成嚴重威脅。對此，需要回應的問題是：在當下數據保護、個人信息權益保護的制度已然確立的情形下，緣何個人數據交易中的安全問題依舊未得完滿解決？個人數據交易的治理存在何種缺憾以及應如何補足，以構建安全可信、便捷暢通

[3] 參見張莉主編、中國電子信息產業發展研究院編著：《數據治理與數據安全》，人民郵電出版社2019年版，第9頁。
[4] 參見張艷：《企業數據交易模式的構建》，載《法商研究》2024年第2期，第73頁。
[5] 參見陽雪雅：《數據要素市場下個人數據交易的證成與實現》，載《上海政法學院學報》2023年第5期，第93頁。
[6] 國家市場監督管理總局、中國國家標準化管理委員會《信息安全技術 數據交易服務安全要求》，GB/T 37932—2019。
[7] 例如，《個人信息保護法》第十條規定：任何組織、個人不得非法收集……他人個人信息，不得非法買賣……他人個人信息。《數據安全法》第三十二條規定：任何組織、個人收集數據，應當採取合法、正當的方式，不得竊取或者以其他非法方式獲取數據。
[8] 參見錢麗：《全國首筆個人數據合規流轉交易在築完成》，載《貴陽日報》2023年9月3日，第A01版。
[9] 參見劉業政等：《數據要素流通使用的安全風險分析及應對策略》，載《大數據》2023年第2期，第82頁。

的個人數據交易流通環境?

二、個人數據交易安全風險治理的規範主義現狀及迷思

現有規範以知情同意制度作為含括個人數據交易行為在內的所有個人數據處理活動的起點，並借助“權利——義務”的規範架構形塑起適用於個人數據交易主體的規範體系。然而，形式上完備整全的制度在實踐中可能出現效用不敷的困境。

（一）個人數據交易安全風險治理的規範主義實踐

規範主義注重法律的規範性和概念結構，擅長以民事權利義務為內容展開規範設計，其要害是從內在規範邏輯上區分不同的概念。[10] 目前，我國個人數據交易安全風險治理的實踐符合規範主義特徵，強調形式完備與權利義務的劃分。對此，可基於個人數據交易安全風險治理中知情同意制度這一制度始點展開分析，同時從個人信息保護與數據安全兩個面向，國家立法與地方立法兩個維度進行探討。具體而言，一方面，中國目前構建了以知情同意原則為核心的個人數據交易範式。個人數據作為記錄個人信息的數據，前者與後者是形式與實質的關係，[11] 個人針對其個人數據享有個人信息權益。[12]《個人信息保護法》構建了以“知情——同意”為核心的個人信息處理規則，[13] 個人數據交易也應將其作為合法性依據。《個人信息保護法》通過多個條文，對於實質同意、撤回同意和重新同意等設立了詳細規則予以保障，可以說，同意貫穿了個人信息的全生命週期。[14] 此外，針對敏感個人信息，《個人信息保護法》亦選擇通過強化知情同意制度予以特殊保護，即要求個人信息處理者須取得個人的單獨同意。針對個人信息處理者，《個人信息保護法》則規定了其處理個人信息的告知義務，要求其詳盡列舉應告知的事項；在敏感個人信息方面，個人信息處理者還應告知個人處理此類信息的必要性以及對個人權益的影響。

另一方面，通過“賦權規範 + 行為規範”的結構分別對個人數據進行個體賦權，並為個人數據交易需求方設定一定的義務。在國家立法層面，《個人信息保護法》賦予個人知情權、決定權、可攜帶權、更正補充權、刪除權等多項權利，並要求個人信息處理者承擔採取安全保障措施、設立保護負責人、定期合規審計、個人信息保護影響評估等義務。針對特殊的個人信息處理者，還增加了設立獨立的個人信息保護監督機構、制定平台規則、在平台內實施懲戒措施以及發佈社會責任報告四項義務。同時，在法律責任上，《個人信息保護法》與《數據安全法》分別對個人數據交易的相關主體進行處罰。例如，《數據安全法》規定了政府主管部門對數據交易中介服務機構履職不能的處罰；《個人信息保護法》概括性地規定了個人信息處理行為違法的罰則。上述規定皆旨在通過對個人信息處理活動的執法活動，實現對於個人數據交易行為的規制，從而防控安全風險。

在地方立法層面，各地對於數據交易的規制呈現出“場內交易為主，場外交易為輔”的現象。除少數地方立法如《貴州省數據流通交易管理辦法（試行）》，將適用對象設定為全省域的所有數據流通交易活動外，大部分地區均聚焦於規範數據交易場所內的交易活動，對場內交易行為率先立法。在監管端，如上海、深圳、天津等地出台的規則都將適用範圍限定於數據交易場所內，並且設

[10] 參見張平華：《基於功能主義的合同制度統合》，載《法律科學》2023年第6期，第149-150頁。
[11] 參見任丹麗：《民法典框架下個人數據財產法益的體系構建》，載《法學論壇》2021年第2期，第93頁。
[12] 參見程嘯：《個人數據授權機制的民法闡釋》，載《政法論壇》2023年第6期，第85頁。
[13] 《個人信息保護法》第六條對於個人信息的處理採取了廣義的界定，包括個人信息的收集、存儲、使用、加工、傳輸、提供、公開和刪除等行為。
[14] 參見姬蕾蕾：《企業數據交易的階梯式規則構建》，載《法學論壇》2025年第1期，第145頁。

立專章為相關部門履行監督管理職責提供依據。[15] 在合規端，現行規則主要針對數據交易場所設立了安全保障義務。例如，上海強調數據交易場所應健全數據安全、個人信息保護制度，應用技術保障數據交易安全；貴州要求數據交易場所應制定風控制度和應急處置預案，定期進行第三方數據交易安全風險評估；天津要求數據交易服務機構專設數據安全負責人和管理機構，並建立交易數據分級保護機制。

（二）規範主義下個人數據交易安全風險治理的挑戰

目前，由於嚴格的規範主義解釋範式，現行制度在對職權法定的理解上往往侷限於狹窄的範疇當中，多元主體協同治理與規則內容間存在張力，[16] 形成了治理資源不足與風險擴散不匹配的矛盾。同時，規範主義思維下的制度設計注重靜態的形式規則，未能充分考慮風險隨著個人數據交易鏈條動態擴散的現實狀態，也未能充分迴應知情同意制度出現的制度目標與實際效用脫節的困境。具體而言，可以從三個方面進行探討。

第一，在主體方面，權力概念的實踐意涵超脫規範本意，造成現有治理規則對個人數據交易安全的關照不足。一方面，權力實際內涵的演化膨脹傾軋個人信息權利的活動空間，“權利——權力”格局形成，權力主體類型逐漸多樣化。現有立法雖然為數據主體與數據處理者設定了相應的權利與義務，但還存在著權利兌現和義務落實的法律實踐問題。在社會現實中，大型個人數據處理者已獲得類似於公權力的地位，個人數據來源者與數據處理者之間地位平等的理論假設已被實踐中實質化的“權利——權力”非對等地位打破。借助算法技術，部分數據處理者擁有了改變用戶的強制力量，[17] 形成了“算法權力”。例如，購物平台可以對用戶的支付帳號採取取消收款、資金止付等強制措施，網約車平台能夠決定訂單分配、指定行駛路線、收取並分配行程費用、設立評分機制等。[18] 由於算法模型的複雜性和算法決策過程的“黑箱性”，算法作用於利益相關方和社會的過程具有高度的隱蔽性。[19] 用戶難以完全理解個人數據如何被收集和使用，這將致使個人知情權等權利難以被真切實現，同時造成“知情”這一環節變得愈加困難。失去了“知情”這一基礎，隨之而來的便是同意行為的形骸化。更為重要的是，個人活動受制於算法權力的支配，算法權力帶來的隱性規訓逐漸消解了個人的權利意識，[20] 被侵權而難以自知和尋求救濟，使得權利規範被束之高閣。同時，用戶難以依照合同自由理論，通過“要約——承諾”的反復磋商來實現交換正義，服務協議突破最初的民事權利義務關係而具有一定的強制性。[21] 然而，目前立法並未完全認識到這一點，不僅對此種權力規制不足，相反還採取了“給平台加責任”的監管方式，使得平台不僅身為一個龐大的“商業帝國”，還擁有了規則制定權、審查權、管理權和處分權，加劇了“準公權力”的特徵。[22]

另一方面，國家強制力量維度的公權力依舊局限在傳統規範框架之內，“權力——權力”格局打破傳統監管雙方間的均衡，個人數據交易治理主體單一。結合央地兩級立法可以看出，目前主要採取依靠政府部門公權力量進行剛性執法的模式對個人數據交易活動進行約束。從組織層面看，保

[15] 例如《上海市數據交易場所管理實施暫行辦法》第2條、第24條，《深圳市數據交易管理暫行辦法》第2條、第29條，《天津市數據交易管理暫行辦法》第2條、第37條、第38條，《廣西數據交易管理暫行辦法》第25條。

[16] 參見郭大林：《跨區域生態環境協同執法機制研究》，中國政法大學出版社2021年版，第19頁。

[17] Nathan Ogle, *The Digital Markets Act: A Blueprint for Modernizing American Antitrust Law*, 26 Transactions: The Tennessee Journal of Business Law 147, 151 (2024).

[18] 參見張淩寒：《算法權力的興起、異化及法律規制》，載《法商研究》2019年第4期，第64-65頁。

[19] 參見肖紅軍：《算法責任：理論證成、全景畫像與治理範式》，載《管理世界》2022年第4期，第200-226頁。

[20] 參見王懷勇、鄧若翰：《算法時代金融公平的實現困境與法律應對》，載《中南大學學報（社會科學版）》2021年第3期，第6頁。

[21] 參見解志勇：《超級平台重要規則制定權的規制》，載《清華法學》2024年第2期，第7頁。

[22] 參見馬長山：《數字時代的人權保護境遇及其應對》，載《求是學刊》2020年第4期，第104頁。

障個人信息安全的職責集中於網信、工業和信息化、市場監管等多個部門，統一的監管機構空缺，且存在監管職責不明確、監管機構職能分散和多頭交叉執法的情形，這往往易造成機構之間相互推諉。[23] 在信息層面，政府部門不直接參與個人數據交易環節，距離市場的實際運作相對較遠。同時，政府在監管信息的收集上存在被動依靠被監管者報送信息的路徑依賴，政府部門與市場主體間存在著較為明顯的信息偏在現象。這增加了監管失配的風險，影響個人數據交易治理整體的有效性和及時性。在技術層面，數據要素市場的參與者能夠迅速回應市場變化和技術更迭，相對於這些技術驅動型企業，政府機關更多地受到運行模式、業務結構的約束，難以即時跟進最新的技術發展，造成監管能效降低。可見，當下的單一主體模式存在治理失效的窘境，在“權力——權力”的治理格局中，公權力對於“準公權力”的約束存在客觀不足。

第二，在視角方面，目前治理模式存在點狀思維依賴與片面視野約束的不足。一是法律規範的節點式規制與安全風險在個人數據交易全鏈條彌散之間存在矛盾。涉及個人數據交易安全風險治理的規則分佈不均，主要密集投放於數據收集的單點時刻，而在個人數據收集後的數據傳輸、數據處理等過程則供給不足。事實上，數據交易具有明顯的時間鏈條性，數據收集只是交易的前序動作，之後還需要經過數據處理、數據傳輸以及交易後的再處理等階段。安全風險可能隨個人數據交易的後續接力行為而不斷累積，只有在數據收集環節的權利才得以保護，那麼數據被收集之後的權利怎麼保護，什麼法律法規可以提供保護？[24] 雖然《數據安全法》規定了數據處理者的風險預防、監測、報告和評估的義務，在形式上似乎邏輯縝密，但這些規則仍主要針對數據處理活動的某些特定階段，無法即時監控數據交易過程中數據流的動態變化，因此在操作上存在相當的局限性。二是場內交易治理規範供給的選擇性偏好與個人數據交易活動在場內場外全面展開的矛盾。在場外交易中，個人數據交易主體能夠以更低成本、更高效率完成數據交易，因此目前存在著場外交易活躍、場內交易冷清的現狀，但是場外交易的蓬勃發展卻伴隨著數據黑灰產業甚至數據犯罪的滋生。[25] 然而，目前各地出台的數據交易立法並未直接回應這一問題，相反主要聚焦於對數據交易所的規範，個人數據場外交易的治理仍然存在較為明顯的真空地帶。在場外交易治理不足的情況下，數據供需主體傾向於選擇政策環境更為寬鬆的場域，而數據交易所作為監管高地則“無人問津”，從而形成監管逃逸現象。更為重要的是，大量的個人數據流向場外，而場外未建立起交易安全的制度體系和防範機制，最終造成個人數據交易安全風險加劇的負向循環。

第三，在實效方面，紙面上的規範表達難以完全落地於個人數據交易安全風險的治理場面。有學者通過對司法裁判文書的實證分析得出，數據主體的權益保護並未隨著立法高效而達到預期成效。[26] 以立法規則和學界研究皆關注的知情同意規則為例，知情同意確實是個人信息處理行為的合法性依據，同時也是個人信息保護規則整套體系的邏輯起點，這一制度無論是在理論上還是實踐上都具有重大意義。因而，無論是立法者還是學界，都試圖通過規則改造和理論解釋來保障個人的實質性同意。在個人數據交易方面，由於其不同於一般的個人信息採集和處理行為，對效率提出了一定的要求，因此眾多學者嘗試從規範始點——知情同意制度展開研究，通過對現行規則進行適應性解釋來保全現有規範的體系完整性和邏輯自洽性。然而，該制度在保護隱私、防止信息損害與限制

[23] 參見李晗：《區塊鏈智能合約中個人信息安全的法律保護》，載《華東政法大學學報》2023年第4期，第54頁。

[24] 參見安柯穎：《個人數據安全的法律保護模式——從數據確權的視角切入》，載《法學論壇》2021年第2期，第64頁。

[25] 參見陳兵、郭光坤《國家級數據交易平台建設的法治方向及架構——以〈數據二十條〉為中心的解讀》，載《法治現代化研究》2023年第6期，第81頁。

[26] 參見馮果、薛亦颯：《從“權利規範模式”走向“行為控制模式”的數據信託——數據主體權利保護機制構建的另一種思路》，載《法學評論》2020年第3期，第71頁。

數據提取上的功能發揮並不樂觀，[27] 无法完全維護個人數據交易的安全。暫不討論實質性的同意是否能夠真切實現，事實上即使是實質同意也難以起到規避個人數據交易安全風險的作用。因為風險的發生僅具有蓋然性，所以數據主體為了接受高效便捷的服務，往往傾向於同意隱私條款。個人願意放棄一定程度的隱私，以換取被認為值得承擔信息披露風險的結果。[28] 從這一視角來看，知情同意制度並未良好地將個人與個人信息處理風險相互區隔，制度本身預設的目標或難以實現。

三、個人數據交易安全風險治理的功能主義轉進與思路

基於上述討論可知，目前個人數據交易安全風險的治理不能企圖通過單獨改造知情同意制度而“畢其功於一役”，更不能一味地將視角局限於規範本身，而是需要進一步考察已有規則在功能發揮上仍存何種不足，並探索如何歸正目前治理不能的局面，這一目標的實現僅靠教義學上對規範進行解釋可能是不夠的。對此，可從規範主義視野轉向功能主義視野，尋求個人數據交易安全風險治理的新路徑。

1992 年，馬丁·洛克林將公法研究的理想類型分為功能主義與規範主義兩種，二者分別呈現出不同的價值取向。與規範主義側重於法律的規範性和概念結構，關注法律邏輯連貫性和規則系統性相對，功能主義導向強調從形式性和規範價值走向實質性和公共意義，注重經世致用和法律的意圖與目標，而非形而上的抽象原則和法律的形式規範性和體系化，倡導採取目標取向及工具主義的思維模式，以解決現實問題為首要目標。[29] 同時，功能主義拒斥形而上學的假定，並且致力於用科學方法來解決政治、政府和法律中的難題。[30] 功能主義者考慮我們必須確保或滿足的東西，而不只是考慮我們據以努力確保或滿足這些東西的制度——就好像那些制度本身就是它們為之存在的終極目的似的。[31]

在功能主義視野下，探討個人數據交易安全風險的治理進路具有其優勢性。功能主義與規範主義本質上的區別便在於前者具有強烈的目的導向性，而後者強調規範性和形式性。功能主義思維下的治理模式直接關注其所採取的手段是否能夠達致現實的目標，而不會單純依循固定的規則和程序。這種以目的為導向的思維要求治理範式始終跟隨社會實際需要的動態變化而進行效用評估和調整。因此，功能主義下的個人數據交易安全風險的治理在構造之初就是動態的，以確保預設目標在不同的環境下得以實現。此外，在功能主義思維的指引下，個人數據交易安全風險的治理不再將目光停留在法律規則的概念化屬性以及權利義務的傳統範式之間，而是更為積極地回應目前存在的具體風險問題。由於功能主義一定程度上擺脫了僵化規則的桎梏，因此具有更強的社會適應性，使其得以靈活回應社會結構變動和技術發展帶來的新變化。功能主義思維能夠突破法律規則中關於權利和權力的傳統認知，覺察當下權力內涵的衍化形態，對互聯網平台等系統重要性數據處理者予以妥適規制，並以實現特定功能為目標驅動，擴大個人數據交易安全風險治理主體的範疇，實現“公權力主體”的擴容。同時，功能主義風格旨在適應一種與當時正在興起的技術導向的社會相容的法

[27] See Sebastian Benthall & Salomé Vilijoen, *Data Market Discipline: From Financial Regulation to Data Governance*, 8 Journal of International and Comparative Law 459, 460 (2021).

[28] See Tamara Dinev & Paul Hart, *An Extended Privacy Calculus Model for E-commerce Transactions*,17 Information Systems Research 61, 61 (2006).

[29] 參見劉志堅：《環境保護稅創制：功能主義和規範主義之辯——以超標排汙行為可稅性問題為中心》，載《甘肅政法學院學報》2018年第5期，第62頁。

[30] 參見[英]馬丁·洛克林：《公法與政治理論》，鄭戈譯，商務印書館2002年版，第193頁。

[31] 參見[美]羅斯科·龐德：《法律史解釋》，鄧正來譯，商務印書館2013年版，第204頁。

律風格。[32] 這種思維提倡在治理活動中應用更加靈活的法律工具和方法，鼓勵適用相應的技術標準等，從而促使治理主體能夠快速適應新技術帶來的變化，而非束縛於帶有滯後性的規則。個人數據交易作為當前數字經濟背景下技術密集型的市場活動，功能主義能夠促使治理理念和手段不斷調整和更新，充分發揮“以技治技”的優勢。

在整體的建構思路上，個人數據交易安全風險治理的功能主義進路可以沿著“目的——功能——手段”的分析框架進行探索。需要注意的是，無論在何種視角下，制度被建構出來自有其目的和功能。然而，規範主義下的目的與功能多被理解為制度的附隨屬性，且多停留在靜態層面。功能主義的獨特價值在於將目的與功能作為制度建構的邏輯起點和效用評價標準，並據此推動治理工具和治理路徑的調整，此種調整在必要時可能會突破既有的形式邏輯與範疇限制。具言之，在目的上，個人數據交易安全風險的治理並非旨在保障安全這一單一目標，而是要衡平安全與發展兩大重要目標，即既要保障個人數據交易安全，同時所採取的手段不能對數據流通造成不合理的、不成比例的限制。[33] 因此，保護數據安全，並非簡單地將數據“圈地為牢”，而是要讓數據在流動過程中防範化解危害行為。[34] 基於上述目標，新型的治理模式應當發揮三大功能，並為功能實現探索相應制度手段。具言之，一是實效評估功能。功能主義下，制度不僅是靜態的規範，更要在實踐中持續檢驗其效用。因此，風險治理要從原來強調規範的單視角轉換為“規範 + 實踐”的雙視角，通過不斷強化規則和標準的制定來為個人數據交易活動提供具體可行的行為標準。在此基礎之上，更加重視既有規則運行的實效，不斷完善治理主體的監督管理活動，以對個人數據交易行為的適法性進行動態評估。二是發展引導功能。功能主義不將個人數據交易安全風險治理侷限於傳統的制度強制和禁止，而是通過引導功能的啟發性與激勵性，藉助激勵相容原理，將治理行為轉化為促進個人數據交易發展的動力。對此，可以進一步明確數據交易所在個人數據交易中的功能定位，完善健全數據交易所的內部治理機制和數據交易機制，[35] 不僅發揮數據交易所在個人數據交易過程中的中介作用，而且應將其培育成個人數據交易安全風險的治理主體。同時，通過不斷完善場內交易的設施條件和配套服務，優化場內個人數據交易的環境，引導更多數據入場交易，從而將更多的個人數據交易行為置於數據交易所的監控之下，維護個人數據交易安全。三是預防強化功能。有學者認為，國內數據治理的一大短板在於數據交易之後的問責糾錯機制缺乏法律的有效保障。[36] 功能主義視角下的制裁不僅是事後的責任追究，更是形成前端威懾與持續防範的重要手段。通過建立完善的問責糾錯機制，對未起到安全注意義務的數據交易所和違法從事個人數據交易的行為與主體予以追責。對既有行為科以一定責任，在懲處既有行為的同時，還能對未來個人數據交易行為形成強有力的預防效果，從而大幅降低個人數據交易的安全風險。

四、功能主義視角下個人數據交易安全風險治理的展開

在探討個人數據交易安全風險治理時，功能主義的視角提供了一個全面深入的分析框架，並且

[32] 參見[英]馬丁・洛克林：《公法與政治理論》，鄭戈譯，商務印書館2002年版，第191頁。

[33] Andrea Stazi, *Data Circulation and Legal Safeguards: A European Perspective*, 10 Comparative Law Review 89, 113 (2019).

[34] 參見王雪誠、馬海群：《總體國家安全觀下我國數據安全制度構建探究》，載《現代情報》2021年第9期，第43頁。

[35] 參見鄭丁灝：《中國數據交易所政策變遷、功能定位與規範配置》，載《科技進步與對策》2024年第13期，第118頁。

[36] 參見楊力：《論數據交易的立法傾斜性》，載《政治與法律》2021年第12期，第4頁。

強調了構建一個多維度治理體系的重要性，對此可具體從四個方面展開。第一，治理主體培育，引入二元協同治理主體，提升治理效能並增強規則的實際運行效果，從而強化實效評估功能；第二，治理空間拓寬，將場內與場外交易一併納入治理範圍，即有效維護數據安全，也促進了數據可信流通，體現了發展導向功能；第三，治理時間延展，打破節點式的靜態治理格局，將風險防控嵌入交易的全鏈條當中，形成全程約束與監督，從而發揮預防強化功能；第四，治理工具革新，作為功能主義視角下因應發展需求的應有之義，數據沙箱的引入為創新交易模式提供可控安全環境，不僅在制度效用的檢驗中增強了實效評估功能，也在鼓勵試錯與容納創新中展現出發展導向功能。

（一）治理主體培育：數據交易所＋政府的二元治理主體

“特定的功能要由以特定方式組織起來的機構承擔”，[37] 要發揮個人數據交易安全風險治理的功能，在政府部門履行回應的治理職責之外，必須培育新的治理主體，構建多主体的治理格局。[38] 而數據交易所能夠承擔相應的職能職責，其不僅應發揮做市功能和驗證功能，還需要監督對商定條款和法律規則的遵守情況。[39] 首先，數據交易所應該進一步加強自身建設，優化服務提供質量，從而吸引更多數據通過交易所進行交易。在總體建設上，中國數據交易所的發展經歷了初創期、爆發期以及目前的平台期。在爆發期，數據交易所在全國“遍地開花”，甚至在同一地域同時設立數個數據交易平台，重複建設現象嚴重。當下，數據交易所的建設應由“量的積累”向“質的躍升”轉變，為數據交易所設立增添准入門檻，強化對數據交易平台數量的控制，優化數據交易所的區域佈局。在此基礎之上，將運營良好並具備一定規模的數據交易所上升為國家級數據交易平台，以回應“數據二十條”提出突出國家級數據交易場所合規監管與基礎服務功能的要求。在具體業務上，數據交易所應明確自身的功能定位，[40] 完善場內個人數據交易的審核規則、定價機制、交易流程和技術標準等，對個人數據交易的引導做到有章可循。交易規則混亂會使數據在不同主體間交換和流轉產生高昂的交易成本，抑制數據主體之間達成合作。[41] 數據交易所應當統一場內交易規則、簡化交易流程，降低場內個人數據交易的成本。此外，更為重要的是，目前阻礙個人數據交易陽光化運行的一大痛點在於個人數據交易存在合法性質疑，這導致數據供需雙方不敢公開進行交易。因此，數據交易平台還應當為個人數據交易提供風險合規機制，這是解決數據產品合法性與可交易性的關鍵路徑，[42] 從而提升企業進入場內交易的動力。[43] 數據交易所應該豐富業務形式，加強與數據商的聯動，通過數據信託、可信身份驗證統一授權等形式，實現個人數據的合法交易，提供個人數據交易的可信環境。

其次，數據交易所應與政府部門互相協作配合，構建個人數據交易的二元主體治理模式。一方面，數據交易場所直接接觸個人數據交易的真實過程，對交易的一手信息有較為全面的瞭解，因此有能力對交易雙方的身份以及個人數據來源、交易申請、交易磋商、交易實施和交易結束等個人數

[37] 張翔：《我國國家權力配置原則的功能主義解釋》，載《中外法學》2018年第2期，第292頁。

[38] See William McGeveran, *The Duty of Data Security*, 103 Minnesota Law Review 1135, 1146-1175 (2019).

[39] See Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harvard Law Review 2056, 2110 (2004).

[40] 參見朱康、唐勇、劉恬凱：《數據要素市場化進程研究——來自數據交易所設立的證據》，載《現代金融研究》2025年第2期，第59頁。

[41] 參見魏益華、楊璐維：《數據要素市場化配置的產權制度之理論思考》，載《經濟體制改革》2022年第3期，第43頁。

[42] 參見高富平、冉高苒：《數據要素市場形成論——一種數據要素治理的機制框架》，載《上海經濟研究》2022年第9期，第83頁。

[43] 參見丁曉東：《數據交易如何破局——數據要素市場中的阿羅信息悖論與法律應對》，載《東方法學》2022年第2期，第155頁。

據交易全流程進行審查。[44] 目前，在數據來源合法合規方面，交易平台一般均設置免責條款，由數據供應方保證數據的合法合規。[45] 然而此種做法無法發揮數據交易所應起到的個人數據交易的安全管理作用，因此需要補充數據交易所的責任追究機制。因此，除了明確個人數據供應者的瑕疵擔保責任外，[46] 平台明知或者應知個人數據存在質量瑕疵或不合法而未及時切斷交易的，應承擔相應的連帶責任；因過失未能履行上述義務的，應承擔補充責任。[47]

另一方面，打通數據交易方、數據交易所和政府部門之間監管信息傳輸的堵點，構建平台與政府之間實質化的聯動治理體系。對此，需要發揮數據交易所作為數據要素市場培育政策介導器的功能。[48] 個人數據交易是數據要素市場的重要活動之一，然而數據要素市場決非自動自發所能形成，而是需要政府採取監管措施、激勵機制以及行業自律等引導市場行為。[49] 作為社會中間層主體，[50] 數據交易所承擔著連接政府與個人數據交易者的任務。在“平台——市場主體”一端，數據交易所能夠將國家出台的法律和政策動態、個人數據交易發展實踐動態以及數據要素市場化配置理論動態實及時彙集公開。同時，結合國家政策要求，數據交易平台及時更新場內交易規則，通過調整數據交易平台自身的目標定位、主體准入、交易標的、服務模式等對交易主體產生直接影響，最終促成政策目標的實現。在“平台——政府部門”一端，可以考慮由數據交易所在個人數據交易雙方以及政府機構之間構建常設性的信息披露機制，定期持續性地開展信息收集和技術分析。[51] 通過動態傳送與定期報送相結合的方式，將個人數據交易信息、運行系統故障、數據存儲洩露等風險事件進行彙報和處置。

（二）治理空間拓寬：場內 + 場外的雙重治理場域

有學者坦言，儘管場外數據市場可以滿足一些企業的需求，但如何監管場外市場是一個巨大的難題，[52] 這確是眼下個人數據交易安全風險治理的痛點與難點。然而，難治理不能成為不治理的託辭，只有構建起場內場外兼顧的雙重治理場域，個人數據交易的安全風險才有機會得以真正化解。首先，在治理職能方面，目前對於個人數據場內外交易治理主體的分工並不明確。由於個人數據交易涉及眾多部門的職能範疇，此種九龍治水的格局極易產生治理空白與治理交叉並存的局面，然而簡單化地指派一個部門對個人數據交易全程進行治理並非當下完全切實可行的方案。因此，從現實情況出發，基於國務院機構改革實踐，在個人數據場外交易治理中，可以率先嘗試將數據主管部門設為統籌協調機構，組建部際協作機制。在場內交易中，由於交易活動在數據交易所內進行，數據交易所可作為個人數據交易的第一道審查機制，主要由數據交易所對個人數據場內交易進行治理。相對於場外交易，場內交易的流程環節比較清晰、標準化程度更高，相關交易信息由交易所匯總，

[44] 參見程嘯：《論個人數據交易的合法性審查義務》，載《華東政法大學學報》2025年第2期，第47頁。

[45] 參見張帆、李春光：《數據流通交易平台的全生命週期治理路徑研究》，載《學習與實踐》2022年第5期，第80頁。

[46] 參見時誠：《數據交易的合同法規則》，載《比較法研究》2025年第1期，第101-102頁。

[47] 參見雷震文：《以平台為中心的大數據交易監管制度構想》，載《現代管理科學》2018年第9期，第20頁。

[48] 參見朱俊達：《數據要素市場化配置下數據交易平台監管的雙重要求及完善路徑》，載《價格理論於實踐》2024年第5期，第56頁。

[49] 參見許可：《數據要素市場的法律建構：模式比較與中國路徑》，載《法學雜誌》2023年第6期，第118頁。

[50] 經濟法理論將經濟法主體分為國家干預主體、社會中間層主體、市場主體和消費者四大類別，其中社會中間層主體是指不同於政府與市場主體，為政府與市場、市場主體之間相互聯繫起中介作用的主體。參見李昌麒主編：《經濟法學》，法律出版社2016年版，第93頁。

[51] 參見徐玖玖：《從“數據”到“可交易數據”：數據交易法律治理範式的轉向及其實現》，載《電子政務》2022年第12期，第88頁。

[52] 參見歐陽日輝：《我國多層次數據要素交易市場體系建設機制與路徑》，載《江西社會科學》2022年第3期，第71頁。

因此可以設置單一部門與數據交易平台進行對接，以實現政府部門對個人數據場內交易的治理。

其次，在治理對象方面，場內交易的治理對象首先應為數據交易活動，一旦發現數據交易活動存在不合規之處，則應啟動對數據交易活動的審查，並因此審查相關數據交易雙方與數據交易所。換言之，在場內交易的治理中，首先關注的是個人數據交易行為本身。由於每一筆場內交易都要於數據交易所進行登記存檔，因此將交易行為作為治理對象具有效率優勢和成本優勢。而個人數據場外交易治理的難點便在於交易行為的隱蔽性，因此治理者很難即時察覺數據交易活動的存在。基於這一特徵，在治理對象的選取方面，應直接從數據交易方，尤其是從作為數據供應方的數據處理者入手。因為數據價值多與數據體量、質量以及準確性、及時性等因素相關，只有擁有一定價值的個人數據才具有交易的可能。而要滿足市場對於數據價值的上述要求，往往只有個人數據收集和處理能力較強的大型數據處理者才能成為合格的數據供應方。相對於非公開的數據交易活動，數據處理者是更容易被政府識別的對象。同時，注重差異化治理理念，依據治理對象的市場規模、業務複雜程度和系統重要性等標準對數據處理者進行分級治理，集中資源對高風險主體進行個人數據交易風險審查。

最後，在治理方式上，想要真正型構起場內 + 場外的雙重治理體系，當下應補強對場外交易的治理。一方面，可以考慮從加大違法懲戒力度的角度入手，提高違法成本。相對於場內交易，目前場外交易旺盛不僅因為存在治理死角，而且違法後果較輕，威懾能力不足。雖然現有立法已經對個人信息違法處理行為設置了高額處罰條款，但仍然值得進一步完善。例如，《個人信息保護法》第 66 條為個人信息違法處理行為設置了兩檔責任，一般情況下，由相關部門責令改正，拒不改正的處一百萬元以下罰款；情節嚴重的，處五千萬元以下或上一年度營業額百分之五以下罰款。換言之，在一般的違法情節下，只有在拒不改正的情況下才予以罰款處罰。個人數據交易行為時刻都在發生，個人數據違法交易行為難以達到情節嚴重的認定標準，無法適用加重條款，而適用一般標準又可能面臨著沒有實際處罰的窘境。因此，對於該條款可以將原來規定中的“情節嚴重”分為“情節嚴重”與“情節特別嚴重”，[53] 合理設置責任梯度，在針對個人數據交易的處置上，不僅需要避免“小過重罰”，更要防止“重過輕罰”甚至是“不罰”的現象出現，保證過罰相當。

另一方面，應不斷完善投訴渠道，提升公眾對個人數據安全的防範意識。可以說，個人作為個人數據最為關切的主體，當其發現個人數據被違規採集或者流通時可能更有動機採取行動。眾包理論（crowdsourcing）認為，通過挖掘與利用公民集體智慧的行動，能為公共問題的解決帶來新的洞見與創新。[54] 相對於組織或者機構，公眾具有數量龐大的優勢，可以形成一支強大的監督力量，整體上提高治理的細度和廣度，彌補個人數據交易安全風險治理中，尤其是在場外交易中，政府機構存在的視野盲區問題。對此，應培養公眾對個人數據保護的意識，不僅需要使數據主體意識到自身數據的利用價值，同時也要讓其瞭解數據處理可能存在的風險，並且向公眾傳達一定的識別個人數據被違法採集、交易等行為的技巧。在此基礎之上，專設個人數據違法處理行為的投訴舉報渠道，通過電話專線、線上平台等多種途經相結合的方式，簡化數據主體舉報流程，鼓勵個人對個人數據交易違法行為進行積極反映。同時，為了避免上述途徑的虛設問題，應對其進行大面積推廣宣傳，確保公眾知曉和利用相應渠道。

（三）治理時間延展：從節點式治理到週期式治理

數據要素安全治理的強化有賴於結合數據要素的特徵和全週期治理的理念順勢而為。[55] 在功能

[53] 參見孫瑩：《違法處理個人信息高額罰款制度的理解與適用》，載《華東政法大學學報》2022年第3期，第25頁。

[54] 參見李燕：《公共管理中的眾包機制:研究現狀與未來展望》，載《探索》2018年第5期，第148頁。

[55] 參見陳兵：《因應數據要素市場化配置全週期治理的挑戰》，載《法學》2023年第10期，第170頁。

主義的視野下，個人數據交易的安全風險治理應關注個人數據交易的整體週期。在交易前期，審查數據交易主體是否符合法律允許的進行個人數據交易的條件，審查用以交易的個人數據來源是否合法，是否經匿名化和去標識化等技術處理。在交易中期，需要審查個人數據交易是否獲得數據來源主體的授權，雙方之間的數據交易合同是否合法、交易傳輸過程是否安全可控和可追溯等。在交易後期，需要關注是否存在個人數據未按合同約定範圍使用，將個人數據進行二次流轉，以及未對交易數據採取安全保護措施等行為。總而言之，一方面需要監督數據的質量、效用是否符合數據交易需求方的要求，另一方面需要監督交易完成後數據是否在許可的範圍內進行使用，以形成對交易全週期的監督。[56]

在場內交易中，週期式治理的要求應該是較為容易實現的，數據交易所直接設定交易規則對場內交易行為進行約束，並對交易主體提供一定的技術條件支持，例如通過區塊鏈公鑰與私鑰的雙驗證技術對數據交易雙方的身份進行驗證，[57] 並且為交易雙方提供同態加密技術等，實現數據的可用不可見。這既能夠保障個人數據的安全，也能防止個人數據被二次交易。[58] 然而，在場外交易中，由於交易行為多以私下聯繫的方式進行，缺乏官方數據交易平台等外部約束機制，因此週期式治理的實現存在著一定困難。對此，首先應強調源頭治理，建立數據登記制度。目前，深圳、貴州等地已經對數據登記進行了地方性立法探索。數據登記具有證明功能、節約功能以及保護功能，其能夠保護數據權利和維護交易安全。[59] 在進行數據登記時，應要求申請人提交數據來源合法、真實的證明材料，並由登記機關進行審查。其次，要完善數據處理者的內部治理，尤其是需要加強對內部員工的管控，防止員工洩露個人數據的事件發生。例如，實施嚴格的數據訪問控制與監控策略，將具有接觸個人數據權限的員工範圍設置在最小必要的限度之內，並通過技術手段監控個人數據的訪問和使用情況。同時，加大對數據處理者的約束，以督促數據處理者將風險管理機制落到實處。例如，進一步完善數據處理者的報告機制，擴大數據合規信息報送的內容，將數據保護措施實施情況、數據洩露或安全風險的記錄和處置情況、員工數據保護培訓與管理情況以及數據處理安全風險自我評估情況等納入報告範疇。最後，為了保證政府部門的審查得以實質性開展，應規定個人數據交易雙方對交易信息的存檔義務，要求交易主體將數據交易主體和數據來源的核驗信息、個人數據來源主體的授權信息、個人數據交易合同文本以及個人數據交易的安全風險評估資料等予以留存，以供政府機構審查之用。

值得注意的是，週期式治理並非簡單地滿足於對個人數據交易的全流程進行關注，同時也強調從傳統上的靜態治理模式轉向動態治理。在靜態治理模式下，個人數據交易的不同環節只是被機械地串聯在一起，而動態治理涉及持續的監測、評估和反饋，確保治理措施能夠有效適應新的變化並應對新的挑戰。因此，政府機構需要因應技術治理的思路，對數據交易流通中因技術特徵引發的法律安全風險困境直接進行技術回應。[60] 因此，政府不僅需要增加主動檢查執法的頻次，完善執法檢查的內容，還應借助雲計算、人工智能等治理科技，加強對網絡流量、市場上數據流通情況的監

[56] 參見黃志雄主編：《數據治理的法律邏輯》，武漢大學出版社2021年版，第280頁。

[57] 參見陳華、李慶川、翟晨喆：《數據要素的定價流通交易及其安全治理》，載《學術交流》2022年第4期，第116頁。

[58] 參見朱曉武、黃紹進：《數據權益資產化與監管：大數據時代的個人信息保護與價值實現》,人民郵電出版社2020年版，第142頁。

[59] 參見程嘯：《論數據產權登記》，載《法學評論》2023年第4期，第138頁。

[60] 參見許可：《數據交易流通的三元治理：技術、標準與法律》，載《吉首大學學報（社會科學版）》2022年第1期，第43頁。

控，對數據處理者的非結構性、非傳統數據進行抓取，[61] 自動識別個人數據交易行為。在此基礎之上，可以開發一種帶有動態與自適應特徵的治理模型，通過算法而非靜態程序，實現模型的自我更新。[62] 借助這一自動化治理模型，實現對個人數據交易全週期的風險評估和風險預警，並根據風險評估結果與異常行為預警情況，動態匹配安全治理策略和措施。在個人數據交易風險化解後，模型對此次治理行為的效果進行收集和分析，根據分析結果不斷迭代和優化個人數據安全治理措施。

（四）治理工具革新：兼顧安全與流通的數據沙箱

沙箱的本義在於提供一個安全的隔離環境，允許技術在其中試驗並評估風險，[63] 後被英國金融行為監管局引入金融監管領域，旨在應對金融科技快速發展帶來的挑戰，隨後新加坡、澳大利亞等國也相繼使用了類似的沙箱工具。目前，沙箱工具已被推廣到數據保護領域，新加坡、英國等國家開始了相關實踐。在中國，國家發展和改革委員會也提出既要鼓勵企業在數據要素應用上的首創精神，又要建立有效的“數據沙箱”機制防範化解重大風險。[64] 作為一種治理工具，沙箱提供了一個可控空間，企業可以在監管當局的支持以及有限實踐的約束下，借助該空間測試和驗證新產品、服務和商業模式以及交付機制。[65] 數據沙箱具有鼓勵創新和防範風險的雙重功能，在沙箱環境下，個人數據交易雙方與數據交易所在一定程度上能夠不受當下規則的拘束，從而可以激勵數據交易主體大膽創新個人數據交易的方式。正如有學者指出，沙箱能夠鼓勵創新、包容試錯，既不必因擔憂風險將新興科技束之高閣，又不會導致全盤放開介入之後的不利局面。[66]

因此，可以在個人數據交易安全風險治理中設置數據沙箱，明確入選標準、監管豁免、測試時間、測試範圍、測試流程、評估標準等沙盒運行的框架。任何沙箱啟動和運轉都需要有透明的入選標準，在域外，沙箱的實踐經驗相對成熟。英國信息專員辦公室在開發人工智能監管沙箱時，將產品創新性作為如何測試的核心標準，具體包括：創新是否與該辦公室重點關注的問題領域一致、是否能够促進質量與效率的提升，是否能使社會公共獲益；同時，還需審查信息專員辦公室自身是否具備開展該項沙箱所需的資源與能力，以及沙箱計劃是否具備可行性。[67] 歐盟在金融科技領域的監管沙箱中則形成了一套更為細化的資格標準，例如，產品或服務是否具有真正的創新性；是否能够為消費者、金融穩定與金融市場帶來益處；申請主體是否已瞭解相關監管框架；項目是否達到足够成熟的階段；創新內容是否難以適應現有的監管框架；供應商是否已經對產品或服務的風險進行評估與緩解；是否承諾合規與投資者保護；是否服務本國市場。[68] 綜合而言，沙箱的入選標準主要集中在項目與產品範圍、創新性與風險特徵、市場價值與社會效益等方面。[69] 結合個人數據交易的特殊性，入選數據沙箱的產品或服務首先應當滿足“創新性”這一要求，這種創新必須達到實質性

[61] 參見秦文岩：《互聯網信息科技在金融監管創新中的應用》，載《南方金融》2021年第7期，第79頁。

[62] 參見[荷]馬克·舒倫伯格，里克·彼得斯：《算法社會：技術、權力和知識》，王延川、栗鵬飛譯，商務印書館2023年版，第141頁。

[63] 參見朱俊達：《新質生產力發展的制度保障：一種自適應的保障模式》，載《北方民族大學學報（哲學社會科學版）》2025年第1期，第127頁。

[64] 參見國家發展和改革委員會：《加快構建中國特色數據基礎制度體系　促進全體人民共享數字經濟發展紅利》，載《求是》2023年第1期，第45頁。

[65] See Wolf-Georg Ringe & Christopher Ruof, *Regulating Fintech in the EU: the Case for a Guided Sandbox*, 11 European Journal of Risk Regulation 604, 607(2020).

[66] 參見張欣：《生成式人工智能的數據風險與治理路徑》，載《法律科學》2023年第5期，第53頁。

[67] 參見张红、岳洋：《人工智能創新與監管動態平衡的規制設計——基於監管沙盒視角》，載《浙江學刊》2025年第1期，第77頁。

[68] See OECD, *Regulatory sandboxes in artificial intelligence*, OECD publishing, 2023, p.15.

[69] 參見戚聿東、劉健：《人工智能產業的包容審慎監管：理論內涵與實現路徑》，載《蘭州大學學報（社會科學版）》2024年第4期，第163頁。

程度，且無法通過常規的監管渠道進行處理；同時，此種創新應當有助於促進個人數據交易可信流通，並能夠促進數據要素市場的培育與完善。此外，產品或服務提供者應當已採取一定措施保障數據主體及相關方的合法權益，並提交完整、合理的項目計畫書以供評估審查。

數據沙箱的運作可以分為申報審核、測試運行以及結束退出三大階段。在申報審核階段，可以由符合要求的數據交易所、數據交易主體單獨或聯合作為申請機構提交相關的申報材料，並可考慮由數據主管部門進行審核。審核通過後，相關項目進入沙盒進行測試運行，在這一階段，主管部門應當定期聽取申請人對項目測試的匯報並進行評估，同時放寬部分法律規則的適用。當然，沙箱中的監管豁免並不等同於供應商不需要承擔任何責任，而是在行政處罰前設立緩衝區，採取較為寬容的策略，激勵其摒棄短期主義和監管套利行為。[70] 如若測試過程中發生個人數據交易違法事件或者安全風險問題，應暫停或終結試驗，同時可與申請人達成行政和解協議，對於承諾重新調整計畫、降低數據安全風險、未造成實質性損失或者對損失予以積極補救的，則可以對其從輕、減輕或者免除處罰。[71] 在結束退出階段，如果項目評估通過，那么可以將此類個人數據交易實踐正式進行市場推廣；如果項目評估未通過或者暫不具備推廣條件的，那麼應該由申請人申請延長測試時間，或者直接強制退出數據沙箱。當然，除了數據沙箱的內部運行架構外，還需要對數據沙箱制度本身進行規範，加快完善和規範監管沙盒制度的實施條件、操作流程、執行標準、管理模式與風控機制，儘量避免監管沙盒本身的操作風險和功能失效。[72]

五、結語

個人數據交易已經成為個人數據流通共享的重要方式之一，其具有社會收益與安全風險並存的複合特徵，只有及時化解個人數據交易中的安全風險，才能推動個人數據交易持續健康發展，助力數據要素市場化配置改革。在法律規範較為完備的客觀情況下，個人數據交易安全問題仍時有發生，既有治理模式略顯捉襟見肘。基於此，個人數據交易安全風險的治理不宜依循傳統的規範主義視角，而是可以考慮轉向功能主義進路，以一種更加靈活的思維方式，探索個人數據交易安全風險治理的創新方案。當然，功能主義引導下的個人數據交易安全風險治理，並非意在矮化或者法律規範的重要作用，相反，其也應當在規則建構的框架內運作，同時需要法律制度對其運行予以保障。

[70] 參見許多奇：《论监管科技的双层容错机制》，載《政治與法律》2024年第1期，第154頁。
[71] 參見陳振其：《監管沙盒：數據要素治理新方案》，載《圖書館論壇》2024年第4期，第145頁。
[72] 參見陸岷峰、歐陽文傑：《現代金融治理體系視角下的監管體制改革研究》，載《經濟學家》2023年第8期，第93頁。

Abstract: Personal data trading is crucial for enhancing data circulation and value, fostering new quality productivity forces. However, issues such as data leakage and misuse that threaten personal data security have also become increasingly prominent. Despite new laws aimed at regulating these transactions, governance of their security risks is still lacking. This shortfall stems from a focus on normative approaches, emphasizing legal rules and traditional rights obligations, which may not be effective in practice. Shifting towards a functionalism perspective, this exploration advocates moving beyond mere norms to an "objective—function—means" framework. It suggests refining governance through cultivating governance entities, expanding governance spaces, extending governance timing, and innovating governance tools, offering a new approach to managing personal data trading security risks under functionalism.

Key words: Personal Data Trading; Personal Data Trading Security; Security Governance; Functionalism; Normativism

（責任編輯：晉晨東）