基於比較法的大灣區金融數據跨境流動規則研究

談 蕭*

摘 要 粵港澳大灣區具有探索我國金融數據跨境流動規則的獨特優勢，但目前尚存在遵循制度不同、標準差異較大、制度銜接較差等法律難題。歐盟涉及多關境、多司法區；美國雖為單一關境，但屬於聯邦制國家，且市場經濟高度發達；二者的金融數據跨境流動或共享規則，對於“一國兩制、三法域”的粵港澳大灣區具有借鑒價值。在金融數據跨境流動或共享的立法理念上，歐盟強調個人數據嚴格保護基礎上的跨境流動，美國則強調共享基礎上的個人數據權利保護；在金融數據跨境流動或共享的監管模式上，歐盟是主動型監管，美國是限制型監管。二者的共性規則有：金融數據流動共享“知情-同意”規則；明確的金融數據流動共享者法律義務與責任；高效協調的金融數據流動共享監管機制。歐盟和美國的經驗能給粵港澳大灣區帶來防範個人金融數據流動共享法律風險、構建金融數據流動共享法律規則、協調金融數據流動共享監管機制等方面的啟示。結合目前存在的問題，借鑒歐盟、美國經驗，粵港澳大灣區需要強化金融數據管理制度的對接、提升金融數據跨境流動的法律保護水準、構建金融數據流動聯合監管機制。

關鍵詞 粵港澳大灣區 金融數據 跨境流動 數據共享

因較少受制於空間、時間區隔的數字經濟、數字金融的飛速發展，金融數據跨境流動的需求當前較為迫切也非常巨大，粵港澳大灣區（下文一般簡稱為“大灣區”）數字經濟和數字金融的發展領先全國，金融數據跨境流動的需求更為巨大。以大灣區2021年開始試點的跨境金融業務“跨境理財通”為例，截至2023年末，大灣區共有67家銀行、6.9萬名個人投資者參與該業務，累計辦理相關資金跨境匯劃金額128億元。2023年，“跨境理財通”相關資金跨境匯劃金額105.9億元，同比增長3.8倍。2023年，廣東省跨境人民幣業務額則高達7.39萬億元，同比增長25.1%，占本外幣結算量的53.1%。在數字金融和數字全球互聯互通的背景下，如何通過金融數據跨境流動以實現其商業價值，需要在合法合規的框架內尋求平衡數據流動與數據安全、金融監管的可行路徑。大灣區作為我國開放程度最高和數字經濟高速發展的區域之一，加之地處“一國兩制、三法域”的特殊制度和法律環境之中，對於我國探索金融數據跨境流動規則，具有得天獨厚的優勢。2023年6月29日，國家網信辦與香港創新科技及

* 談蕭，法學博士，廣東外語外貿大學法學院教授。

工業局簽署《關於促進粵港澳大灣區數據跨境流動的合作備忘錄》，提出在國家數據跨境安全管理制度框架下，建立大灣區數據跨境流動規則，推動數據要素安全自由有序流動。2023年12月13日，國家網信辦與香港創新科技及工業局共同發佈《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同實施指引》，金融數據在粵港兩地大量傳輸成為可能，香港金融機構和內地金融機構之間的合作將更為便利。2023年12月21日，經國務院批復、國家發改委頒佈的《前海深港現代服務業合作區總體發展規劃》明確，“支持香港金融機構在前海設立研發中心、數據中心、運營中心等，試點征信數據等金融數據深港跨境流動。”這些文件不僅為大灣區金融數據跨境流動提供了政策依據，也起到了推動作用。然而，由於大灣區三地在個人信息保護、立法理念與司法執法體制等方面存在較大差異，金融數據跨境流動仍面臨法律規則銜接不暢、出境與保護標準差異較大、法治保障水平不足等諸多問題。

一、大灣區金融數據跨境流動存在的法律障礙

（一）金融數據跨境流動所遵循的制度不同

根據我國《網絡安全法》《數據安全法》《個人信息保護法》與《數據出境安全評估辦法》等相關規定，大灣區內地九市向境外提供金融數據，必須在數據出境風險自評估基礎上，通過國家網信部門組織的數據出境安全評估。香港《個人資料條例》，指定香港個人資料私隱專員公署為個人資料保護主管機構，並規定移轉至香港以外地方的個人資料，必須符合轉移“白名單”條件，即轉移目的地必須有完善的資料保護制度，資料當事人必須書面同意，資料使用者必須採取合理防範措施等。2014年，個人資料私隱專員公署公佈《保障個人資料：跨境資料轉移指引》，對包括白名單機制、個人資料權利主體書面同意、避免對個人資料權利主體不利行動影響及其他豁免情形，就《個人資料條例》適用原則、範圍和主體進行瞭解讀，並對相應流程作了一系列指引。澳門《個人資料保護法》則規定，只有在遵守該法且法律體系能確保接收轉移資料安全情況下，方可將個人資料轉移到澳門以外的地方，而判斷安全的決定主體是“公共當局”，即澳門個人資料保護辦公室，但截至目前該辦公室尚未承認任何一個國家或地區具有“適當程度”保護能力。該法還規定了例外情況，認定主管機關作出個人信息跨境轉移決定，個人信息被合法公開登記，或經保護主管機關審查許可後跨境轉移，資料控制者“確保有足夠保障他人的私人生活、基本權利和自由機制，尤其通過適當的合同條款確保這些權利行使”；另外，基於特定目的進行個人資料跨境流動，如維護公共安全、預防犯罪、刑事偵查和制止刑事違法及保障公共衛生需要，則無需保護主管機關介入。[1]

按照內地數據分級規則，金融數據大多屬於重要數據。重要數據是指一旦遭到篡改、破壞、洩露或非法獲取、非法利用等，可能危害國家安全、經濟運行、社會穩定、公共健康和安全的數據。[2] 內地相關法律法規強調重要數據保護，並對重要數據識別、風險評估、保護義務等內容作了明確詳盡的規定。大灣區內地九市主要是根據國家《數據安全法》《網絡數據安全管理條例》，實行數據分類分級保護制度，但截止目前，香港和澳門兩個特別行政區尚未建立重要數據分級分類保護制度，且現有執法和司法實踐中，沒有金融數據跨境流動的典型案例，因此大灣區金融數據跨境流動仍面臨較大的安全風險。

---

［1］ 參見楊曉偉、張譽馨、賈丹：《粵港澳大灣區數據跨境流動的挑戰與對策研究》，載《工業信息安全》2023年第4期，第73-78頁。

［2］ 參見國家網信辦《數據出境安全評估辦法》第十九條。

（二）金融數據出境與保護標準差異較大

在金融數據出境與保護標準方面，大湾区內地九市依據《個人信息保護法》第38條、第40條以及國家網信辦《數據出境安全評估辦法》第4條的規定，關鍵信息基礎設施運營者、數據處理者，處理個人信息100萬人以上，自上年1月1日起累計向境外提供10萬人以上，或敏感個人信息1萬人以上，均需經網信部門組織數據出境安全評估。非以上情況的，需在專業機構對個人信息保護認證的基礎上，按照國家網信部門制定的標準與境外接收方訂立合同，然後通過內地締結或參加國際條約或協定出境。大灣區內地九市遵照的《個人信息保護法》及配套行政法規、部門規章，已對個人數據出境流程、轉移方式、保護責任及處罰等級等作出明確規定，違法違規向境外提供個人信息的處罰包括責令改正、暫停轉移或終止服務、停業整頓、實施罰款等。香港和澳門都尚未出台體系化的個人數據出境管理制度。香港《個人資料條例》於1995年制定，其中第33條對個人資料跨境轉移有諸多限制。2014年和2022年，香港個人資料私隱專員公署先後發佈《保障個人資料：跨境資料轉移指引》和《跨境資料轉移指引：建議合約條文範本》，但均為行政指引文件，不具有強制力。澳門雖無相關規定，在實踐中已發生多起對個人資料轉移出境未向澳門個人資料保護辦公室申報的行政處罰案例。

（三）金融數據保護和出境制度銜接較差

在金融數據跨境流動範圍、保護義務和法律責任等方面，大灣區內地九市執行的《個人信息保護法》與香港《個人資料條例》和澳門《個人資料保護法》存在較大差異。

首先，在金融數據作為個人信息的範圍方面，內地《個人信息保護法》中的“個人信息”概念與香港《個人資料條例》和澳門《個人資料保護法》中的“個人資料”概念的範圍差別較大。大灣區內地九市依法認定的“個人信息”強調的是“已識別”和“可識別”信息，即包括個人具體身份信息和個人關聯信息，而對於敏感個人信息，依據內地《個人信息保護法》也有非常嚴格的保護要求。香港《個人資料條例》第2條規定的個人資料，是指直接或間接與在世個人有關，直接或間接地可確定有關個人身份，存在形式予以查閱及處理切實可行。澳門《個人資料保護法》規定的個人資料，則是指包括聲音、影像、識別編號及其他任何可反映資料當事人特徵，進而確定資料當事人的信息。

其次，在金融數據作為個人信息的保護義務方面，香港《個人資料條例》和澳門《個人資料保護法》均無內地《個人信息保護法》規定的“單獨同意”、“合規審計”、“影響評估”等要求，也未對指定個人信息保護負責人、處理行為等加以規定。

再次，在金融數據作為個人信息保護的法律責任方面，三地的行政處罰規定也不同。內地《個人信息保護法》規定的罰金最高，責任單位罰款可高達人民幣5000萬或上年度營業額的5%，直接責任人可處10萬以上100萬以下罰款；香港《個人資料（私隱）條例》規定首次可判處第5級罰款（即罰款50000港幣）及監禁2年，如屬持續犯罪則每日加罰1000港幣，其後相同犯罪可處第6級罰款及監禁2年，屬持續犯罪則每日加罰2000港幣；澳門《個人資料保護法》規定的處罰最輕，責任單位最高可處20萬澳門元罰款，但對具體責任人則無明確處罰的規定。[3]

［3］ 參見楊曉偉、張譽馨、賈丹：《粵港澳大灣區數據跨境流動的挑戰與對策研究》，載《工業信息安全》2023年第4期，第73-78頁。

二、歐盟、美國金融數據流動共享的法律經驗

（一）立法理念

1．歐盟：嚴格保護個人數據基礎上的流動與共享

歐盟於2016年頒佈、2018年生效的《通用數據保護條例》（General Data Protection Regulation，GDPR），是歐盟針對個人數據保護的全面性核心立法。據此，歐盟採用一部涵蓋各行業的通用法律的形式對數據開展保護，也就是說，個人金融數據與其他類型個人數據無異，同樣受到GDPR的約束。[4]

GDPR在立法理念上，將個人數據權利作為一項基本人權，強調數據收集與共享的合法性，保護自然人基於個人數據所享有的權利。GDPR在涉及個人數據處理的領域，對於收集與共享的目的和數據限度都有相應的限制性規定。GDPR還規定了個人數據權利主體“同意”的構成要件，強調“同意”應是個人數據權利主體在自由意志下所作出的意思表示。

GDPR大幅增加了個人數據主體的權利，強化和明確了數據控制者及處理者分別必須承擔的責任和義務，將數據保護常態化和系統化。此外，在歐盟GDPR項下，數據主體具有知情、糾正、刪除以及反對等權利。[5] 在個人數據共享方面，GDPR還單獨設一章，增加了數據控制者的義務和責任，提高了用戶同意的標準，並為數據控制者增設了數據洩露告知、對隱私影響評估等義務。同時，為了保護個人隱私，GDPR特別強調了對數據控制者的行為監管。GDPR還明確規定數據控制者在個人數據收集與共享中的義務，並規定其處理個人數據的目的須滿足合理性要求。

2．美國：共享基礎上加強個人數據權利保護

推動個人數據共享與利用始終是其金融領域立法的主要目標。在特定的金融領域，該理念得到廣泛認同，與其他機構共享金融數據的範圍和條件也在逐步擴大，以便更好地服務於金融市場。美國聯邦《金融服務現代化法案》（The Gramm-Leach-Bliley Act, GLBA）的制訂的目的就是為了推動金融市場的發展與競爭，同時該法案對金融機構與關聯機構和非關聯機構之間的“同意”形式採取區分原則，[6] 主要體現在：該法案對關聯機構採取“無需同意”[7] 和非關聯機構採取“默示同意”兩種授權方式。[8]

---

［4］ 參見洪延青：《個人金融信息收集和共享的基本原理：基於中美歐規則的展開》，載《中國銀行業》2019年第12期，第29-32頁。

［5］ GDPR規定數據主體享有以下權利：（1）知情權，即從數據控制者處獲取關於數據處理細節和信息的權利，並且應當被主動告知擁有哪些權利；（2）訪問權，即可以從數據控制者處確認自己的個人信息是否正在被處理、哪些信息被處理、如何處理等；（3）糾正權，數據主體有權要求控制者及時糾正或補充完整關於自己的個人信息；（4）刪除權，除某些例外情況，數據主體有權要求徹底清除自己的個人信息；（5）限制處理權，數據主體可以對數據的準確性提出質疑，並且限制數據處理的範圍、方式等；（6）可攜帶權，數據主體有權以通用可讀的方式帶走個人數據，將其傳輸至某第三方，並且不因此受到特殊對待或限制；（7）反對權，數據主體可以在某些情況下禁止對其數據進行處理，或拒絕對自己進行數據畫像及自動化決策。

［6］ See Steven R.Roach,William R.J.Schuerman, *Privacy Year in Review:Recent Developments in the Gramm-Leach Bliley Act,Fair Credit Reporting Act,and Other Acts Affecting Financial Privacy*,A Journal of Law and Policy for the Information Society,Vol.1, 2005, p.385-390.

［7］ 美聯儲頒佈的《Y監管條例》（12 CFR Part 225 - Bank Holding Companies and Change in Bank Control,Regulation Y）擴大了金融控股公司的業務範圍，該條例第28條規定了金融控股公司“允許從事的非銀行業務清單”(List of permissible nonbanking activities)，範圍包括“數據處理”公司，即銀行控股公司及其子公司可以設立專門進行數據處理、數據存儲和數據傳輸活動的公司。

［8］ 在金融機構與其關聯機構之間，無需經過同意而可自由共享非公開個人數據；在金融機構與非關聯機構之間，應告知消費者可以通過“選擇退出”的方式拒絕共享非公開個人信息。

為回應社會對金融隱私保護的憂慮，各州也通過立法確立各自的隱私保護法和數據安全法，其中2018年通過的《加州消費者隱私法》（California Consumer Privacy Act，CCPA）[9]是美國州層面消費者隱私法立法的一個重要里程碑，它雖是立足於州層面，但卻被認為是美國該領域立法的標杆。該項法案明確了收集加州消費者個人數據的企業的適用範圍，擴展了個人信息的定義，並強化了對消費者隱私的保護，賦予消費者對企業使用數據情況的知情權以及拒絕、刪除、修改數據等權利。[10]而後的《2020年加州隱私權法》（California Privacy Rights Act，CPRA）規定，如果某企業收集個人數據並出售或共享給第三方，或披露給服務提供者、承包商用於商業目的，該企業必須與第三方、服務提供者或承包商簽署信息安全保護協定。在協議中，應當明確規定個人數據的處理和使用方式，以及收集和使用個人數據的目的，以及被收集者的權利。[11]此外，CPRA還創新性地提出，利用與個人資料相關的行政罰款來設立“消費者隱私基金”，用來支付由州法院、總檢察長以及加利福尼亞州保護署為執行CPRA所需費用。[12]

（二）監管模式

1．歐盟：主動型監管

主動型監管的國家是全球推動個人金融數據流動共享的主力，歐盟無疑最積極的推動者。歐盟在2016年就推出了歐盟支付服務指令PSD2（Payment Service Directive 2），旨在促進歐盟金融市場的開放和穩定性，提高支付服務的安全性，保護金融消費者的利益，並鼓勵創新。它要求歐盟境內的支付服務提供者提供開放的支付服務，以及利用技術和服務來改善支付服務的安全性和數據保護。

同時在數據監管機構上，歐盟設立了“歐盟數據保護理事會（European Data Protection Board，EDPB）[13]——各成員國數據監管機構——數據處理者內部的數據保護專員”三級數據監管機構。首先，EDPB是歐盟最高級別的、獨立的個人數據監管機構，其主要職責是對個人數據安全進行宏觀監管，對歐盟GPDR在各成員國實施標準進行統一，以及對各成員國之間的分歧進行協調，並提出建設性建議或作出最終決定。其次，各成員國監管機構對其轄區範圍內的數據控制者和處理者所開展的數據處理活動進行監管，並確保其行為符合GDPR及其上級機構制定的規定，以確保各項規章制度得到貫徹執行，並能夠在必要的時候對數據處理活動作出相應的決策。[14]再次，數據處理者內部的數據保護專員是由數據處理者自行指定的專門負責數據保護事務的職位或部門，負責監督和管理組織內部個人數據的處理和保護。GDPR還要求雇員數量超過250人的大型企業必須設立數據保護官。[15]因此，這

---

［9］《加州消費者隱私法案》(CCPA)是美國首部關於消費者隱私保護和數據安全的全面立法。

［10］CCPA規定了數據主體即消費者的主要權利包括：（1）獲取信息的知情權，及消費者有權要求公司披露收集、使用、共享、出售了自己的哪些個人信息，以及進行上述行為的原因；（2）刪除數據的權利，消費者有權要求公司及其服務提供者刪除已經收集的任何個人信息；（3）不受歧視的權利，CCPA要求公司不能因為消費者行使了上述合法權利而對其進行任何形式的歧視，例如拒絕提供產品或服務、對該消費者收取更高的費用、對給消費者的產品或服務品質與其他消費者有所不同等。

［11］2020年11月3日，美國加州選民投票通過了《加州隱私權法案（2020）》（即CPRA）。CPRA補充並擴展了《加州消費者隱私法（2018）》（即CCPA），尤其是它為加州居民確立了新的數據隱私權，對企業和服務提供者施加了新的義務和責任，並將創建一個獨立的數據監管機構，授權其實施該法並起訴違規行為。CPRA於2023年1月1日起生效，給予企業2年的過渡期。

［12］參見許娟、黎浩田：《個人金融信息風險民事責任的實現》，載《江蘇社會科學》2022年第1期，第181-191頁。

［13］EDPB，全稱European Data Protection Board，譯作歐洲數據保護委員會。其由GDPR於2018年5月成立，前身是第29條數據保護工作小組（“W29”）。W29根據《數據保護指令》設立，因《數據保護指令》被GDPR替代而被EDPB替代。

［14］參見彭德雷、張子琳：《數字時代金融數據跨境流動的風險與規制研究》，載《國際商務研究》2022年第1期，第14-25頁。

［15］數據保護官（DPO）的主要任務就是保證其所服務的組織對其員工、顧客、供應商，以及其他任何人（即GDPR框架下的“數據主體”）的個人數據的處理，符合適用的數據保護規定。

三級數據監管機構之間存在著緊密的聯繫，這在提高數據監管權力運行效率、加強個人數據保護和數據合規利用等方面都發揮了非常關鍵的作用，也充分體現出保護個人數據的價值取向。

2．美國：限制型監管

美國對本國金融科技公司，採取的是“按部就班”的功能性監管，即不論金融科技公司以何種形態出現，只要其具有金融公司的本質屬性，就將其所涉及的金融業務按照其功能納入現行金融監管體制之中。也就是說，在美國金融科技公司被當成金融公司一樣監管，美國這種限制性監管是相對比較嚴格的。正因為如此，美國眾多科技巨頭都未曾像中國的一樣大規模涉入金融領域，這也導致美國出現大量的優秀的金融科技公司，但沒有出現大型的金融科技巨無霸。美國的金融市場很大，金融機構服務的完善和普及，但對金融科技公司來說，沒有太多的發展的空間。當優秀的金融科技公司發展到一定高度時，可能遭遇市場規模、金融牌照和數據瓶頸等困境。美國也在反思，相對嚴格的金融科技監管是否阻礙了其創新和發展。目前美國監管趨勢在逐步調整和鬆綁，推動金融數據流動共享就是其中一項舉措。但美國政府監管並沒有公開支持個人金融數據流動共享，此外，金融機構必須遵守金融行業協會制定的行業規範，以及行業自律組織設定的嚴格的程序要求和行為準則，從而對金融機構處理個人數據的活動進行約束和規範。美國公司還設立首席隱私官（Chief Privacy Officer，CPO），[16]負責確保組織遵守國家和地方隱私法律，遵守適用的標準，妥善保護個人數據，實施隱私政策，建立隱私流程和保護措施，及時發現和處理可能存在的隱私問題。

（三）共性規則

1．金融數據流動共享“知情-同意”規則

雖然美國和歐盟採納了不同的立法理念，但本質上二者都在“同意”的形式上在加強對個人數據的權益保護。“知情-同意”規則是個人數據保護中的“帝王”條款，也是個人金融數據流動或共享法律規制的核心。金融數據權益是公法性質的私權利，對於私權利的保護應當充分尊重意思自治。為避免將對個人金融數據流動共享的方式被認定為“概括授權”，應注意避免將金融消費者個人數據共享的授權條款直接勾選為同意；在取得金融消費者授權時應明確金融數據授權的目的、方式和範圍；允許客戶撤回金融數據授權的同意，以及避免採用“相關信息”等模糊不清的表述。因此，在個人金融數據流動共享的過程中，還應嚴格遵循“知情-同意”規則。

2．金融數據流動共享者的法律義務與責任

歐盟和美國在關於相關的立法文書中，都規定了金融機構的責任和義務，明確了作為數據處理者，金融機構所應當承擔的責任。美國法律規定了金融機構處理個人數據的條件和範圍，以及必須以合理的方式向金融消費者提供隱私權的相關政策，同時也強調了金融機構必須以合理的方式向個人數據主體進行通知，以便保護金融消費者的隱私權和數據安全，違反此類規定的金融機構需承擔法律責任。歐盟法律規定，金融機構對個人數據的合法性使用，必須在符合數據主體本人授權、履行法定職責等情況下，並要求採取必要性保護措施。

3．高效協調的金融數據流動共享監管機制

在監管模式上，歐盟傾向於設立專門的個人數據保護的專職機構，並強調監管的全面性和協調

［16］ 首席隱私官（Chief Privacy Officer，CPO），指專門負責處理與用戶隱私權相關事宜的人，CPO直接對企業的最高領導人負責。其任務是處理內部和外部隱私事務，內部事務包括政策的制定、展開和適應及同公司現有及過去員工的聯繫，外部事務包括公司和其他商家及公共領域、股東、客戶、媒體的交流。

性，其優勢在於將金融數據流動或共享的監管權集中於一個監管機構，從而使得監管執法的標準、程序更加統一，有助於提升監管的效率。美國的金融監管則比較注重市場自我調節，強調市場的自由度和競爭力，也重視行業自律組織的作用，通過行業協會等組織進行自律監管。

三、歐盟、美國經驗對大灣區的啟示

歐盟作為多關境、多司法管轄區地區，與大灣區有類似之處；美國雖然不存在多關境、多法域，但由於是聯邦制國家，各州之間的法律規則、監管體系也不盡相同，同時因其高度發達的市場經濟體系，也是大灣區值得學習的國家。歐盟和美國在金融數據流動及共享方面的立法理念、監管模式及共性規則，都能為大灣區相關規則的構建和協調帶來啟發。

（一）防範個人金融數據流動共享法律風險

1．保障金融消費者的知情選擇權

在金融數據流動共享的環節，保障金融消費者的知情選擇權，就是將知情權與選擇權作為金融機構共享數據的前置條件、合法依據。在消費者與金融機構之間的契約關係中，數據作為合同客體，必須尊重金融消費者的意思自治。當數據被金融機構所掌控時，金融機構有責任保護數據主體的隱私權和人格權，在進行數據共享前，金融機構應當以通俗易懂的語言，真實、準確地向金融消費者披露可能影響其決策的信息，法律也應當賦予金融消費者擁有權利介入數據共享環節，以保護金融消費者的數據權益並及時控制對其數據權益可能造成損害的處理行為。這是數據共享中數據主體行使知情權的一種表現。

在數據處於金融機構控制時的流動共享過程中，數據主體依然享有自主選擇權，可以根據法律規定來選擇是否同意進行數據共享。在特定情況下，金融機構進行金融數據流動共享仍然需要告知金融消費者並由其做出最後決策。這也是金融消費者自主決策權的重要體現之一。例如在金融機構向關聯機構共享個人數據的情況下，金融消費者應當有權拒絕共享。在此種情況下，金融機構應當盡可能及時準確地向金融數據主體傳達數據共享行為，並且為金融數據主體提供必要的行為選擇，以便金融消費者可以行使其退出權；在金融機構向非關聯第三方共享個人數據的情況下，由金融消費者自行決定是否同意共享其個人數據，當金融消費者基於自身意願，決定退出服務並終止金融機構的數據共享行為，金融機構則應在合理範圍內，及時停止向其提供相應的服務。

2．規範隱私保護計算技術的應用

除了傳統的管理風險，金融機構還面臨著更多的技術風險。然而，法律的發展速度往往難以跟上信息技術的迅猛發展。目前的風險防範方式主要依賴于金融消費者手中的硬體設備進行二次確認，以確保金融數據流動共享的安全性。然而，對於金融機構後台存儲的數據和帳戶數據的保護仍然需要進一步加強。[17] 因此，在法律制度無法及時規制的領域，可以通過技術手段來彌補這一不足，從技術應用層面上避免金融數據流動共享所可能帶來的危害。

隱私保護計算是一種跨學科技術體系，包含人工智能、密碼學、數據科學等眾多領域。作為一種技術化解決手段，隱私保護計算可以在保障金融數據安全與個人隱私的前提下提升金融數據流程通和

［17］ 參見王建文、彭洋愷：《論網絡背景下金融隱私權的法律保護》，載《西北大學學報(哲學社會科學版)》2015年第2期，第97-106頁。

共享能力。隱私保護計算是隱私權保護下金融數據流動共享的技術實現路徑。隱私保護計算一般通過三個環節保證數據和模型隱私。首先，通過對原始數據進行去標識化處理，以確保合作的第三方機構無法通過數據逆向推導出數據主體的身份，但要盡可能地保留數據的“信息價值”，做到共享數據的“可算不可識”。其次，提升數據和模型計算環境的安全性，確保全程安全可控，可以通過硬體化、安全沙箱、存取控制、數據脫敏、流轉管控、即時風控和行為審計等手段實現安全性。再次，保護數據涉及的隱私，在不暴露原始數據情況下進行數據流動、共享和價值實現，可採用智能計算技術，如多方安全計算、差分隱私和聯邦學習等方法實現數據的“可用不可見”。[18]

隱私保護計算適用的法律設計是影響金融數據流動共享發展的關鍵。在大數據時代，金融數據的法律保護面臨一些固有風險，可能導致以“知情-同意”為核心構建的金融數據保護體系在應用價值方面出現一定程度的失效，從而影響金融消費者與金融機構之間的信任基礎。在隱私保護計算的應用路徑中，需要考慮以下方面：（1）法律合規性：隱私保護計算必須符合適用的數據保護法律法規，如個人信息保護法、隱私保護條例等。在數據處理過程中，必須遵循法律法規的規定，包括數據收集、存儲、處理、共享等方面的要求。（2）信息最小化原則：隱私保護計算應該遵循信息最小化原則，只收集和使用必要的數據，避免收集不必要的個人信息。數據處理應當以實現特定目的為基礎，並且僅限於必要的範圍。（3）可追溯性和責任追究：在隱私保護計算的應用過程中，應建立相應的審計機制和數據追溯能力，以確保數據處理活動可以被有效監測和審查。同時，對於數據處理過程中的違規行為，應追究相應的責任。通過遵循上述原則和要求，隱私保護計算可以在合規的前提下實現數據的有效利用和共享，也將可能實現金融數據流動共享的全流程可追溯、可計量。[19]

3．建立金融數據流動共享前置風險評估制度

歐美的經驗表明，風險評估制度能夠有效檢測各方金融數據主體的安全保障能力。但該制度難以得到真正地貫徹實施，因為風險評估規範作為行業標準對金融機構往往並不具備強制效力。為此，應當引入風險評價機制，用行政強制力來保障風險評估的執行。此外，對金融機構的合規措施進行內外部評估，可以在一定程度上減輕金融機構的合規成本。

大灣區金融機構共享個人金融數據環節中建立風險評估體系，需要從內部與外部兩個方面進行部署。在內部風險評估方面，可以參考歐盟所實施的數據保護官制度。當進行大量的金融數據處理時，金融機構應設置專門的數據保護官，對個人數據權益的影響進行評估。在外部風險評估方面，監管部門也應對金融機構的安全措施進行外部評估。大灣區金融監管部門對金融數據外部安全評估應從以下幾點考慮：其一，評估金融機構的數據安全防控能力，包括金融機構在數據共享前已實施的安全措施，例如身份驗證、加密、存取控制、備份，也包括數據共享中使用匿名化和去標識化技術處理敏感性數據的能力等；其二，評估金融機構事後的應對措施，金融數據流動共享後對個人數據權益產生不良的影響的事後補救措施，是否採取有效措施控制事態的惡性發展。

（二）構建金融數據流動共享法律規則

1．優化“知情-同意”授權規則

首先，應遵循“三重授權”的規則。“三重授權”方法要求在進行個人數據共享時，需要獲取三次授權，即共享個人數據需取得三次授權，分別對應數據權利人對數據控制者收集個人數據的授權，

[18] 張曄：《隱私計算：讓數據“可用不可見”》，載《科技日報》2023年04月10日，第2版。

[19] 參見溫泉、劉霽雯：《進軍超級場景：隱私計算金融風控應用報告（2022）》，載《零壹財經》2022年1月28日。

數據控制者對其他控制者的授權以及數據權利人對數據控制者共享個人數據的授權。[20] 因此，金融機構在共享金融消費者個人數據前應當在收集環節與共享環節均須以合理的方式取得金融消費者的同意並授權。

其次，應當優化知情同意授權模式。金融機構可以採用簡化的流程和介面，減少授權的步驟和介面的複雜性，向金融消費者披露數據的實際使用情況；同時，可以提供更加多樣化的知情同意授權方式，如單項選擇、分級授權等。在實踐中，例如穀歌為註冊用戶提供Dashboard工具，[21] 使其能夠自主管理個人數據：使用者可以通過Dashboard頁面瞭解其數據在各項服務和應用程序中的使用情況，包括誰能夠訪問這些數據、以何種方式使用這些數據等；使用者可以選擇管理個人數據，包括增加、刪除和修改個人數據。Dashboard還提供了個性化的隱私設置，用戶可以通過這些設置控制個人數據的使用和共享。例如，用戶可以選擇是否允許穀歌跟蹤其位置信息，或者是否允許穀歌將其搜索記錄與其他數據進行關聯。這種模式可以為金融機構提供借鑒參考，以實現金融數據主體對其授權的自主管理。同時金融機構也應當細化同意權行使的規則。現有的金融數據的授權協定存在著普遍較長、內容模糊等問題，而該數據授權協定是一種格式條款。因此，第一，應當簡潔，要把條款的內容用通俗的文字表述出來，並重點突出“金融機構免責以及加重金融數據主體責任”的格式條款，讓消費者能夠迅速地辨認出來，從而更好地瞭解相關條款的內容。第二，應當遵循必要最小化原則。即在提供金融服務時，只能在必要的範圍內共享金融數據，而不允許以概括授權的方式超出必要範圍。

最後，適當使用“即時同意”規則。大灣區金融機構對數據的利用並不會僅僅滿足於收集個人數據，大數據時代數據的價值正是對數據的二次利用。金融機構在超出原始數據收集的目的和權限的前提下，運用原有金融數據，結合深度挖掘和分析技術，發掘數據之間的關聯性和規律性，以獲取新的價值。此時，金融機構應該獲得金融消費者的“即時同意”才能進行二次利用包括共享行為。儘管“即時同意”規則的引入可能會給金融消費者帶來諸多不便，也會給金融機構帶來較大的成本負擔，但對於重要的金融數據跨境流動或共享而言，採取“即時同意”規則是必要的。為了平衡金融數據流動共享需求和個人數據保護之間的矛盾，可以採取措施控制“即時同意”規則的使用頻率，並將“即時同意”規則與“選擇-退出”模式相結合，這種方法具有可行性。

2．釐清個人金融數據流動共享者的義務與責任

針對金融數據流動共享者的義務，具體要求如下：（1）數據共享前：應當簽訂數據共享協定，告知數據主體共享目的及第三方機構類型並取得授權，確保數據主體的知情權；還應當加強對數據接收方的盡職調查，確保其具備合法的資質。（2）數據共享中：應對數據的共享情況進行精確的記載，包括共享的日期、規模、目的，以及數據接收方的基本情況等；採取必要的安全措施，確保金融數據在共享過程中的安全性和保密性，防範數據洩露、篡改和丟失等風險。（3）數據共享後：應按照《網絡安全法》的要求保存共享記錄不少於6個月。

金融數據流動共享涉及的主體多元，在金融消費者個人數據權利受到侵害時，應當確定侵權責任主體，並對不同責任主體的責任承擔方式進行判斷。因此，需要根據不同的糾紛類型進行分析。從是否有金融消費者授權來看，金融數據跨境流動可能引發兩種類型的糾紛：第一種是金融機構或第三

［20］ 參見王利明：《數據共享與個人信息保護》，載《現代法學》2019年第1期，第45-57頁。

［21］ dashboard是商業智能儀錶盤的簡稱，它是一般商業智能都擁有的實現數據視覺化的模組，是向企業展示度量信息和關鍵業務指標現狀的數據虛擬化工具。dashboard關鍵的特徵是從多種數據來源獲取即時數據，並且是定制化的互動式介面。

方未經金融消費者授權，故意或者重大過失地向他人共享金融數據。金融消費者若提起違約之訴，則可依據合同條款有權要求金融機構承擔違約責任。金融消費者若提起侵權之訴，則可以依據侵權責任原理要求金融機構和第三方機構承擔對外連帶責任。第二種是在經過金融消費者授權下，金融機構或第三方機構故意或者重大過失地超出授權範圍內共享數據。金融消費者有權根據合同條款提起違約之訴，也可以在規定時期內對共享行為進行合法性追認，但這種約定不能對抗法律法規的強制性規定。此外，如果金融消費者在財產或者人格方面受到侵害，金融機構和第三方機構存在共同侵權，金融消費者有權要求其承擔連帶責任。

3．制定第三方機構審核與認證規則

為從源頭上防控風險，對於數據的共享物件是第三方機構的情況。首先，應要求第三方機構取得相關的牌照或者具有合格資質。在審核第三方機構提交的申請材料時，金融機構需要核查其營業執照是否寫明確定的營業範圍，並檢查其內部控制水準和技術能力等方面的資質，同時加強對金融消費者的數據授權安全保護。[22] 大灣區金融機構可以參考歐盟PSD2相關規定，在准入管理方面，加強對第三方機構的指導和制定規範，包括但不限於以下措施：對第三方機構實施資質管理，如設定帳戶存取權限；並制定由金融機構和第三方機構承擔因消費者帳戶缺陷或欺詐行為造成的損失的責任分配方案；[23] 其次，應當設立“黑名單”機制。將有數據運營異常記錄的第三方機構列入在金融機構的黑名單，如果第三方機構採取補救措施消除負面影響，則可以請求從黑名單中刪除。同時，“黑名單”應由各類金融機構共享，以消除由於信息不對稱帶來的損害。再次，應引進第三方機構的驗證制度。在第三方機構發起的數據轉移請求時，可以通過“用戶名和密碼”進行“單一驗證”，針對隱私風險較高的數據，應實施“用戶名和密碼+電子郵件複驗”的“雙重驗證”，例如先使用用戶名和密碼登錄，再以電子郵件或文本消息進行重複驗證。若驗證信息不真實或不符合，則應拒絕共享數據。

（三）協調金融數據流動共享監管機制

1．推進機構監管與功能監管相結合

在金融數據流動共享的有關金融創新活動中，金融科技公司等非持牌機構實際上參與金融活動，但又被排除在金融監管框架之外，這種不需要承擔監管成本的非持牌金融機構可以與需要承擔監管成本的持牌金融機構競爭的情況，也違背了市場公平競爭的原則。同時這種忽視金融本質、風險屬性和必要監管約束的現象，也會引發金融數據監管套利風險。儘管“金融科技”在詞義上強調了“科技”，但從其特點來看，其也具有明顯的金融屬性，其在從事金融數據業務時，需要遵循金融監管的邏輯和規定。然而，如果阻止大型互聯網公司開展金融業務，或者要求大量的中小型金融科技公司將必須選擇和持牌金融機構合作，這雖然有助於防範金融風險，但是可能會造成持牌金融機構對從事金融數據類業務的金融科技公司的控制，從而導致金融市場活力下降。

因此，隨著金融新業態的蓬勃發展，大灣區金融數據監管需要考慮兩個方面：一是要考慮到對金融數據的共享行為進行監管不會過分抑制金融的發展與創新；二是功能監管和機構監管兩種模式的結合過程中，應考慮取捨什麼，如何取捨，取捨到什麼程度的問題。我國金融控股公司的出現也更多地

［22］ 參見陳振雲：《我國金融數據治理法律構建的三個維度》，載《貴州大學學報（社會科學版）》2022年第5期，第80-92頁。

［23］ 參見趙吟：《開放銀行模式下個人數據共享的法律規制》，載《現代法學》2020年第3期，第138-150頁。

參照了美國模式，在功能監管建立的初期採取美國傘式功能監管。[24] 待監管水準達到一定程度後，再向功能監管中的雙峰模式[25] 或歐盟統一監管模式逐漸轉變，應該是比較合理的路徑。

2．細化金融數據反壟斷監管規則

因此，大灣區應將金融數據納入反壟斷監管。首先，要制定金融數據壟斷的具體判定標準，[26] 可以從以下考慮：一方面，針對特定金融市場，明確參與市場的主體及其所擁有的數據。例如，對於互聯網金融市場，應當明確不同互聯網金融平台所擁有的數據，包括但不限於金融消費者個人交易數據等。另一方面，需要考慮金融數據壟斷行為對金融市場和金融消費者的影響，包括價格、品質、創新等方面。只有綜合考慮以上因素，才能夠對金融數據壟斷進行準確判定。其次，完善對金融數據的反壟斷監管的法律。為此，可以從以下幾個方面入手。一是建立金融數據的反壟斷法律框架，包括法律法規、監管規則和執法機構等。二是明確金融數據反壟斷監管的物件和範圍。針對金融數據壟斷行為，需要明確監管物件為金融機構和互聯網金融平台等經營者，並且監管範圍需要覆蓋金融數據的收集、共享、使用、銷售等環節。三是加強金融數據反壟斷執法力度，制定有力的懲罰規則。

四、大灣區金融數據跨境流動規則構建與協調的基本路徑

根據大灣區內地九市與香港、澳門兩個特別行政區金融數據跨境流動實踐中存在的問題，結合前文對歐美經驗的考察，推進大灣區金融數據流動共享和順暢流動，就必須消弭數據跨境流動中因地方制度不一或操作規範分歧造成的障礙，解決個人信息保護和出境制度、法律規範接軌以及司法實踐的銜接問題。

（一）建立大灣區金融數據跨境流動制度的協調對接機制

金融數據多為敏感性數據，不僅涉及個人隱私權保護，還可能涉及國家安全。大灣區有必要建立相互協調的金融數據分類、分級保護制度，並對重要金融數據建立聯合認定和識別機制，加強保護。首先，建立粵港澳大灣區協調互認的金融數據分類分級制度，明確一般金融數據和重要金融數據的識別標準，並能在大灣區內互認，為大灣區內金融數據跨境流動奠定制度和標準基礎。其次，建立粵港澳聯合金融數據跨境流動評估機制，並適當簡化大灣區內金融數據跨境流動評估程序，對於一般金融數據，在嚴格保護個人隱私權的基礎上，制定相對寬鬆的跨境流動評估程序；對於重要金融數據，僅在大灣區範圍內流動的，除涉及國家安全事項需要單獨評估外，也盡可能簡化評估程序。再次，鼓勵大灣區金融機構在處理數據跨境流動時，採用數據脫敏技術，在技術層面降低金融數據的敏感性和跨境流動的安全風險。

（二）提升大灣區金融數據跨境流動的法治保護水準

大灣區在數據跨境流動的法律保護方面，均已初步出台了一些法律規定，已經有一定的法律基礎，但對於金融數據的跨境流動，法律保護水準尚不高。內地有關金融數據法律保護的立法和實踐，目前尚處於摸索階段，澳門由於金融市場不夠發達，在此領域的立法和司法實踐，稍顯滯後，而香港

［24］ 傘式功能監管是指金融控股公司的各個子公司根據業務不同接受不同行業監管機構的監管。

［25］ 雙峰監管（Twin　Peaks）是依目標進行監管。按照監管職能設立兩個監管機構，將審慎監管和行為監管分開。審慎監管負責維護金融體系和機構安全和穩健運行，行為監管負責公平交易，以保護金融消費者合法利益。

［26］ 參見鐘紅、馬天嬌：《金融數據安全風險及監管研究》，載《清華金融評論》2021年第10期，第96-98頁。

在普通法體系下，對個人隱私有著較高的法律保護標準，同時在司法層面，根據《香港特別行政區基本法》，香港的判例法體系可以援引整個普通法司法區的先例，對新的法律及司法問題有較好的調適性和靈活應對性，能夠快速適應數位金融的發展。香港這一司法優勢，不僅全球少有，就是在普通法地區，也獨具特色，需要我國尤其是大灣區善加利用。因此，提升大灣區金融數據跨境流動的法律保護水準，大灣區內地九市和澳門均應該以香港的規則、制度和司法實踐為基準，在立法和司法上，不僅要儘快消除三地的法律保護水準差，更要對標歐洲、美國等先進地區，提升法治保護水準。

（三）加強大灣區金融數據跨境流動監管和執法合作

由於“一國兩制、三法域”，大灣區還存在大量的監管和執法協作問題，這也為大灣區金融數據跨境流動帶來了困難。大灣區需要強化金融數據跨境流動安全和個人信息保護的聯合監管及執法協作。在聯合監管層面，大灣區金融監管部門要建立數據跨境流動的聯合監管機制，加強監管標準和流程的對接協調、監管信息的共享、監管措施的協助，必要時應建立跨境聯合監管機制。在執法協作層面，大灣區金融執法部門要建立數據跨境流動的信息共享與聯合調查機制，在執法證據搜集、執法信息共享、處罰措施協助等方面，進行充分的合作。這種聯合監管和執法，本身可能也涉及金融數據的跨境流動。但此時的金融數據跨境流動，應更多受到公法、行政法層面的規制，需要三地監管和執法部門在嚴格保護相關主體數據權利的基礎上尋求公法、行政法上的解決方案。

五、結語

針對大灣區金融數據流動面臨的數據風險，在金融消費者層面，應充分保障金融消費者的知情選擇權；在金融機構層面，從內部和外部對金融機構進行數據共享前的前置風險評估以及規範隱私保護計算的適用以防範金融數據洩露的風險。在大灣區建立協調金融數據跨境流動的具體法律規範方面，針對“知情-同意”規則在金融領域實效性減弱的問題，要通過“三重授權”同意規則、細化同意授權規則以及適當運用“即時同意”規則加以解決，同時須釐清金融數據共享者的義務與責任，並制定第三方機構審核與認證規則。針對大灣區金融數據跨境流動監管機制的不足，建議從監管模式上推進機構監管與功能監管相結合，並提出在銜接行政監管與司法救濟的過程中，還可以建立金融數據權益受侵害的公益訴訟制度，以緩解金融數據主體維權成本與金融機構違法成本之間不平衡的問題。

Abstract: The Guangdong-Hong Kong-Macao Greater Bay Area has unique advantages in exploring cross-border financial data flow rules in China, but currently there are still legal challenges such as different compliance systems, significant differences in standards, and poor institutional connections. The European Union involves multiple borders and jurisdictions, while the United States, although a single border, is a federal country with a highly developed market economy. The cross-border flow or sharing rules of financial data between the two have reference value for the Guangdong-Hong Kong-Macao Greater Bay Area, which has "one country, two systems, and three jurisdictions". In the legislative concept of cross-border flow or sharing of financial data, the European Union emphasizes the strict protection of personal data based on cross-border flow, while the United States emphasizes the protection of personal data rights based on sharing; In the regulatory model of cross-border flow or sharing of financial data, the European Union adopts proactive regulation, while the United States adopts restrictive regulation. The common rules between the two are: the "informed consent" rule for sharing financial data flow; Clear legal obligations and responsibilities of financial data flow sharers; Efficient and coordinated regulatory mechanism for sharing financial data flow. The experiences of the European Union and the United States can provide insights for the Guangdong-Hong Kong-Macao Greater Bay Area in preventing legal risks related to personal financial data flow sharing, establishing legal rules for financial data flow sharing, and coordinating regulatory mechanisms for financial data flow sharing. Based on the current problems and drawing on the experiences of the European Union and the United States, the Guangdong-Hong Kong-Macao Greater Bay Area needs to strengthen the integration of financial data management systems, improve the legal protection level of cross-border financial data flow, and build a joint regulatory mechanism for financial data flow.

Key words: The Guangdong-Hong Kong-Macao Greater Bay Area; Financial Data; Cross-border Flow; Data Sharing

（責任編輯：勾健穎）