大灣區民生數據跨境的障礙、策略與技術研究——以醫療康養數據跨境為例*

金雨心　馬晨曉　應作斌

[摘　要] 由於粵港澳大灣區在政策、法律法規、文化等方面存在差異，三地居民的醫療康養資料並不互通，對居民生活以及大灣區的資料跨境造成了一定的障礙。本文以醫療康養數據為例，從境內外法律法規、使用倫理及技術難點三方面展開研究。針對醫療康養數據的跨境需求，本文提出相應的策略和建議條文，為打造大灣區一體化建設提供具有價值的參考依據，也為日後中國與國際的數據跨境流通帶來借鑑意義。

[關鍵詞] 民生數據　粵港澳大灣區　資料安全　數據跨境　醫療康養

一、背景及研究意義

（一）醫療發展的政策背景

2021年9月5日，中共中央、國務院印發了《橫琴粵澳深度合作區建設總體方案》（下稱《方案》）。《方案》提出，要“加強與澳門社會民生合作，加快推進‘澳門新街坊’建設，對接澳門教育、醫療、社會服務等民生公共服務和社會保障體系，有效拓展澳門居民優質生活空間”，並要“促進國際互聯網數據跨境安全有序流動。在國家數據跨境傳輸安全管理制度框架下，開展數據跨境傳輸安全管理試點，研究建設固網接入國際互聯網的綠色通道，探索形成既能便利數據流動又能保障安全的機制”。[①]由此可以看出，《方案》對大灣區民生醫療產業發展，民生數據跨境管理創新和數據跨境安全有序流動提出了新要求。

《粵港合作框架協議》、《粵港澳大灣區衛生與健康合作框架協議》、《粵港澳大灣區藥品醫療器械監管創新發展工作方案》等重要協議、方案的締結，為灣區醫療康養共同發展奠基。為促進醫療數據跨境，地方政府也推出了一系列政策，如深圳市政府《關於加快推動醫療服務跨境銜接的若干措施》用十一招疏通醫療康養跨境，《廣州南沙深化面向世界的粵港澳全面合作總體方案》在南沙公立醫院試點跨境轉診合作等。

*本文係澳門基金會項目（研究類）“大灣區民生數據跨境的障礙、策略與技術研究：以醫療康養數據跨境為例（2022.06.30 － 2023.06.30）”（編號 MF2102）的研究成果。

作者簡介：金雨心，馬來亞大學計算機科學與信息技術學院數據科學碩士生；馬晨曉，九州大學系統情報科學研究院研究生；應作斌，澳門城市大學數據科學學院副教授，博士生導師、研究生課程主任。

[①]中華人民共和國中央人民政府：《橫琴粵澳深度合作區建設總體方案》，2021 年 9 月 5 日，www.gov.cn/zhengce/2021-09/05/content_5635547.htm.，2023 年 1 月 26 日讀取。

（二） 醫療開放的新機遇

粵港澳大灣區的人口老齡化問題日趨嚴重，醫療康養數據的跨境有了新的機遇。三地醫療數據的互通，也是大環境下解決民生醫療問題的重要辦法。

粵港澳大灣區的發展過程中，建立了一體高效的交通運輸體系，形成了獨特的經濟優勢和醫療康養產業優勢，這些都可以加速跨境醫療康養的發展。在解決跨境養老合作的過程中，養老產業也會帶來引人注目的成效，將獨特的氣候、生態、環境發展成異地養老的獨特優勢，建設優勢互補、互利互贏、資源共享的優質城市群。[①]

（三） 研究意義

粵港澳大灣區醫療康養數據跨境需求強烈，但存在着倫理道德、法律法規及技術上的障礙。目前三地的醫療康養服務由於基礎設施的不足、專業人才短缺、機構發展滯後、法律規定不一致、行業監管欠缺等原因，導致了供需矛盾凸顯、服務水平較低、社會資本投入不足、制度保障銜接困難等問題。

本文對跨境醫療在倫理道德、法律法規及技術上的障礙進行分析研究，嘗試提出對改善粵港澳大灣區民生數據跨境流動有參考意義的方案及建議。

二、倫理道德問題分析

在數字化時代，健康醫療數據共享是社會發展的必然趨勢，數據共享和隱私保護之間的矛盾越來越明顯，由此而引發的倫理道德問題也吸引了廣泛的關注。總體而言，醫療數據跨境共享中面臨的倫理道德難題有下列幾個方面：

（一）保護數據安全和個人隱私

數據共享在不同的階段面臨着不同的安全風險：不當收集、過度利用、數據脫敏或匿名化之後被重新識別、數據泄露等。研究者使用數據平台搜集和剖析患者醫療信息是否侵犯個人隱私，政府或企業對患者醫療信息收集監控和分析是否符合隱私規則，個人隱私在數字化社會下無所遁形。

（二）防範數據失真和信任危機

健康醫療大數據的價值體現在對真實的健康數據的有效分析。[②]無用的、虛假的健康數據不僅浪費資源，而且還會給受眾帶來心理衝擊和認知錯覺。[③]患者更會因為數據安全和數據失真問題存在“不願”、“不敢”分享醫療康養數據的問題。防範醫療數據失真和醫患失信是數據跨境共享中需要攻克的重要倫理道德難題。

[①]白岩曦：〈粵港澳大灣區跨境養老服務現狀及政策應對研究〉，博士論文，吉林財經大學，2021 年，頁 50。
[②]田維琳：〈大數據倫理失範問題的成因與防範研究〉，《思想教育研究》（北京），第 8 期（2018），頁 107 － 111。
[③]侯雄等：〈健康醫療大數據建設中的倫理問題〉，《解放軍醫院管理雜誌》（上海），第 6 期（2020），頁 552 － 554。

（三）縮小數字鴻溝

數字鴻溝表現為不同群體或個人因在獲取技術、信息可及，以及自身價值觀方面的差異導致技術、應用、知識和價值鴻溝。大數據在醫療領域的應用使得在經濟更好的地區、受教育度更高的人群將會享受更加優質的醫療服務，落後地區的一部分人則可能會被邊緣化。隨着互聯網的普及，不同地區、階級之間數字鴻溝正在縮小，但仍將長期存在。如何縮小“數字鴻溝”會變成更加凸顯的倫理道德問題。

上述倫理道德問題在一切數據跨境活動中都存在，為了使得澳門特別行政區的居民對於數據跨境的安全產生信任，可以使用一些策略使這些倫理道德問題得到一定程度的解決。如探索法律法規、通過數據文化培訓產生倫理規約、創新研發數據安全技術以及培養更加專業的醫療服務團隊等。

三、法律法規障礙及借鑑意義

（一） 粵港澳大灣區數據跨境法律對比

（1） 中國《個人信息保護法》

中國對於數據跨境的治理雖然相對於歐美國家來說較晚，但規則的嚴厲程度上基本對標歐盟《通用數據保護條例》（General Data Protection Regulation，GDPR），《網絡安全法》、[①]《數據安全法》、[②]《個人信息保護法》都對數據的跨境傳輸作出了規定。

《個人信息保護法》作為中國數據跨境傳輸的主要法律依據，主要從網絡安全和數據主權出發，規定了可以向境外提供個人信息的四種條件，以及特定情況下的數據本地化要求。即關鍵信息基礎設施運營者和處理個人信息達到國家網信部門規定數量的個人信息處理者，應當將在中華人民共和國境內收集和產生的個人信息存儲在境內。[③]此外，《個人信息保護法》也要求境外個人信息處理者在我國境內設立專門機構或者指定代表，負責個人信息保護相關事務；[④]明確表示個人信息處理者須採取必要措施保障境外接收方的處理活動達到規定的保護標準，[⑤]在最大程度上保障個人的知情權、決定權等權力。

《個人信息保護法》就個人信息的收集、存儲、使用、加工、傳輸、提供、公開、刪除等確立了保護規則，[⑥]也適應了個人信息跨境流動、個人信息國際合作保護的需要。除此之外，2016 年 11 月，全國人大常委會正式通過了《網絡安全法》，規定了關鍵信息基

[①]中華人民共和國中央人民政府：《中華人民共和國網絡安全法》，2016 年 11 月 7 日，https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm，2022 年 9 月 20 日讀取。
[②]中華人民共和國中央人民政府：《中華人民共和國數據安全法》，2021 年 6 月 11 日，https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm，2022 年 9 月 20 日讀取。
[③]中華人民共和國中央人民政府：《中華人民共和國個人信息保護法》，2021 年 8 月 20 日，https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm，2022 年 9 月 20 日讀取。
[④]王佳宜、王子岩：〈個人數據跨境流動規則的歐美博弈及中國因應 —— 基於雙重外部性視角〉，《電子政務》（北京），第 5 期（2022），頁 99 － 111。
[⑤]張睿、舒瑤芝：〈個人信息保護公益訴訟條款的語義分析〉，《浙江海洋大學學報（人文科學版）》（舟山）第 3 期（2022），頁 43 － 49。
[⑥]宋爍：〈論政府數據開放的基本原則〉，《浙江工商大學學報》（杭州），第 5 期（2021），頁 107 － 116。

礎設施個人信息和重要數據跨境流動的一般規則。2021 年出台的《數據安全法》又再次聚焦數據安全領域，完善了相關細節。總體來說，中國一直以來傾向於嚴格的數據跨境傳輸治理方式。跨境數據的安全、可控的確是需要重視的必要課題。在保障安全的基礎上，靈活的採取措施使中國的數據流動更加便利、有序，進一步推動數字經濟的發展是中國一直以來的目標。

（2）澳門特別行政區《個人資料保護法》及香港特別行政區《個人資料（隱私）條例》

中國香港特別行政區和澳門特別行政區將信息稱作資料，以多元化服務業經濟為主的澳門於 2002 年開始啟動關於個人資料保護的立法工作。以葡萄牙《個人資料保護法》為藍本，結合澳門特別行政區本土實際情況，形成第 8/2005 號法律《個人資料保護法》。該法對個人資料的自動化處理（電腦處理）和非自動化處理（人工處理）作出了規定。《個人資料保護法》的第五章對於個人數據的跨境提供了一系列的規則，依據該法，個人資料原則上僅在遵守法律規定且數據接收方達到適當保護程度的情況下方可轉移到特區以外的地方。是否達到“適當保護程度”則由澳門公共當局決定，這種途徑與歐盟的“充分性保護認定”相似，通常採用的方法是設立“白名單”：將滿足保護水平的國家或地區列入“白名單”。而到目前為止“白名單”中沒有任何國家或地區。

若資料轉移的目的地對個人資料沒有適當保護程度，在符合法律規定的前提下，實體仍可以將個人資料轉移，但須通知公共當局。若實體在確保可以保障他人的私人生活、基本權利和自由的情況下，特別是通過合同條款保障這些權利能夠行使的情況下，可向公共當局申請許可，在獲得許可後方可將個人資料轉移。若是個人資料的轉移是維護公共安全、制止刑事犯法行為等的必要措施，可在無需申請的許可的情況下進行。[①]

香港特別行政區有獨立的立法、執法和司法機關，並且從 1996 年起就開始實施《個人資料（私隱）條例》，[②]保障信息數據的自由流動，具備較完整的法治體系和數據流通保障體系。《個人資料（私隱）條例》第 33 條對於個人資料轉移至香港以外的地方有和澳門特別行政區相似的規定，但由於種種原因這條法規至今尚未實施，對於數據的跨境流動僅具有參考意義而不具有約束性。

總體而言，港澳特區對於跨境數據的要求亦十分重視，但在一些定義的界定上相較於《中華人民共和國個人信息保護法》比較模糊。香港地區的《個人資料（私隱）條例》，澳門地區的《個人資料保護法》與中國大陸地區《網絡安全法》、《個人信息保護法》，在對個人信息監督管理機構、數據和隱私的範圍定義上都存在不同。[③]不同地區法律法規的適用範圍不同，下表綜合對比中國內地和港澳三地的法律法規（表 1）。

[①] 澳門特別行政區政府第 8/2005 號法律《個人資料保護法》，2005 年 8 月 10 日，https://bo.io.gov.mo/bo/i/2005/34/lei08_cn.asp，2022 年 10 月 3 日讀取。
[②] 香港特別行政區政府香港法例第 486 章《個人資料（私隱）條例》，2022 年 10 月 1 日，www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y，2022 年 10 月 3 日讀取。
[③] 京東數字科技研究院：〈粵港澳大灣區數據跨境合規流通研究〉，2019 年 9 月 11 日，www.secrss.com/articles/13625，2022 年 10 月 03 日讀取。

表 1　中國內地、香港、澳門的法律法規對比

	中國大陸		中國澳門		中國香港	
法律法規	《網絡安全法》 《數據安全法》 《個人信息保護法》	強調技術加密和數據分類管理制度；安全、自由的原則；保障個人信息的“告知—同意”。	《個人資料保護法》	“嚴格限制”；確保信息接收地的信息有法律保護；同時遵守其他規定。	《個人資料（私隱）條例》	確保信息接收地的信息有法律保護； 數據傳輸在數據主體同意下進行； 符合“數據主體同意”的例外情形。
域外管轄界定	基於信息處理行為	凡是涉及的信息涉及境內自然人即在管轄範圍。	個人資料	兩種情形：一是信息處理主體在境內；二是通過境內服務器或服務供應商。[①]	個人資料	其收集、持有、處理或使用是在境內進行的； 其收集、持有、處理或使用是由主要業務地點是在境內的人所控制的。
問責機制	行為與安全風險為中心的問責制	規定應當在中華人民共和國境內存儲；向境外應進行安全評估、個人信息保護認證、與境外接收方訂立合同且個人信息處理活動合規，符合法律法規規定的其他條件。	處理行為問責	個人信息處理主體是否採取足夠的技術和組織措施來保護個人信息。	條例規定問責	個人信息處理主體是否違反《個人資料（私隱）條例》下的一系列規定，是否違反實務守則。

資料來源：中華人民共和國《網絡安全法》、《數據安全法》、《個人信息保護法》；澳門特別行政區《個人資料保護法》；香港特別行政區《個人資料（私隱）條例》。

（二）各國數據跨境法律對比及在數據跨境上的做法

（1）新加坡

新加坡跨境數據最主要的法律依據是《個人資料保護法令》（Personal Data Protection Act，PDPA），[②]同時成立個人資料保護委員會來承擔 PDPA 的制定和實施工作。

PDPA 中第 26 條及《個人資料保護條例》（Personal Data Protection Regulations，

[①]葉湘：〈阿里雲在大灣區的個人信息跨境合規：管轄權競合視角〉，《中國流通經濟》（北京），第 7 期（2021），頁 106 － 118。

[②]Personal Data Protection Act 2012, 31 Oct 2021, Singapore Statutes Online, sso.agc.gov.sg/Act/PDPA2012, accessed on 8 Oct 2022.

PDPR）中第 9 條確立了新加坡的數據跨境制度：只有在符合 PDPA 要求，轉移組織採取了適當的措施確保數據接收方受到和新加坡至少相等的“可依法執行的義務（legally enforceable obligations）”約束的情況下方可進行數據的跨境傳輸。[①]此外，在一些明確的例外情況下，可以視為滿足了“可依法執行的義務”，實踐中參考 PDPR 中一系列更具體的補充情形。新加坡希望在跨境數據在被高度保護的情況下能夠盡可能自由的流動。[②]

為了創造更加安全的數據跨境環境，新加坡作出了一系列重要舉措。如簽署並加入其他數據跨境相關的協議或體系，發佈《可信任資料共享框架》，[③]強調數據共享中的可信第三方認證制度、數據標準化、數據共享協議制度等。[④]

在醫療數據的流動中，新加坡經歷過多次數據泄露事件後，為了應對一系列的數據安全問題，對數據泄露和問責細節進行了補充，在提升數字科技水平方面作出了努力，爭取構建政府與民衆間的信任。在數字政府、智慧國家的建設中，新加坡也基於醫療數據的流動開發了綜合醫療信息平台，包括全國電子健康病歷系統、綜合臨床管理系統、個人健康記錄計劃以及遠程合作徵求計劃。[⑤]新加坡還着重孵化掌握多維度知識的高端複合型人才，讓他們為新加坡包括醫療在內的數據流動安全保駕護航。

（2）日本

《個人信息保護法》（Amended Act on the Protection of Personal Information ， APPI）與《個人信息保護法實施條例》、《個人信息保護法指南（向外國第三方提供）》共同構成了日本個人數據跨境傳輸制度，可概括為“一個原則，三個例外”。“一個原則”是指個人數據處理者在將個人信息傳遞給境外第三方時，原則上要經過數據主體的同意。但是在出現“三個例外”中的情況時，可以直接採取“opt-out”模式，即個人數據跨境傳輸可以不經數據主體的同意，直接傳送給境外第三方。[⑥]

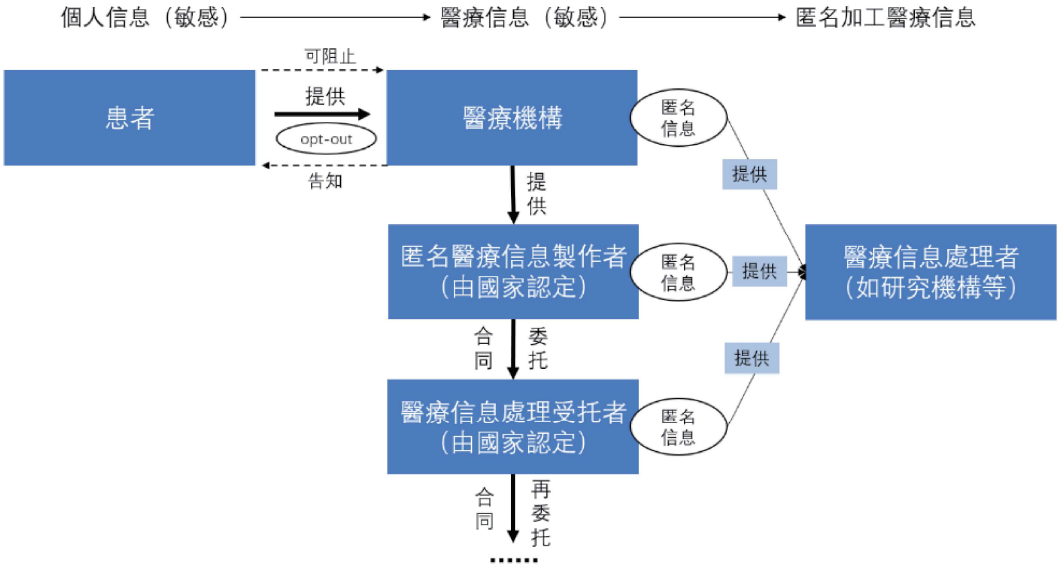
而對於個人敏感信息的流通，在《個人信息保護法實施條例》第 2 條中指出，除非存在特殊情況，都必須取得本人同意。

由於大部分醫療方面的數據都是敏感的個人隱私數據，按照 APPI 系列中的規定，受到非常嚴格的傳輸使用限制，不利於醫療數據的開發和使用。於是日本擬定了“專門法”——《次世代醫療基礎法》作為補充。該法的主要框架如下（圖 1）：

---

① Personal Data Protection Regulations 2021, 29 Jan 2021, Singapore Statutes Online, sso.agc.gov.sg/SL-Supp/S63-2021/Published/20210129?DocDate=20210129, accessed on 8 Oct 2022.
② 李晶、張靖辰：〈“雙循環”格局下中國數據跨境制度創新研究〉，《中國發展》（北京），第 1 期（2021），頁 41 － 47。
③ IMDA. *Trusted Data Sharing Framework*. 4 Jan 2020, www.imda.gov.sg /programme-listing /data-collaborative-programme, accessed on 12 Nov 2022.
④ 徐明月、安小米：〈協同理論視角下新加坡可信數據共享框架的案例分析〉，《情報理論與實踐》（北京），第 10 期（2020），頁 177 － 182。
⑤ 京東科技集團：〈新加坡，全球智慧城市之首，憑甚麼？（京東數科觀察）〉，2022 年 10 月 21 日，https://zhuanlan.zhihu.com/p/267115519，2022 年 11 月 12 日讀取。
⑥ 日本個人信息保護委員會：〈個人情報の保護に関する法律〉，2020 年 6 月，www.ppc.go.jp/files/pdf/APPI_english.pdf，2022 年 10 月 24 日讀取。

圖 1　《次世代醫療基礎法》規制框架



該法律開創了匿名加工制度，通過匿名加工，本來敏感的醫療信息將失去個人隱私屬性，變為普通信息，從而允許以特定目的在特定主體之間實現跨境流通。

它還開創了國家認定制度，規範了匿名醫療信息的製作者和使用者的資質標準。醫療機構可以選擇自行加工醫療信息，或者委託由國家認定的製作者進行匿名加工，同時，製作者也可以繼續委託其他由國家認定的法人進行信息加工。

《次世代醫療基礎法》允許認定製作者採取“opt-out”方式獲取敏感的醫療數據，目的是為了提高醫療信息匿名加工的效率。但是醫療機構必須在獲取信息之前，事先向患者詳細解釋使用目的、被使用的信息詳情、拒絕的方法等事項，並留出 30 天的時間，讓患者有充足的時間做出拒絕選擇。[①]

（3）美國

美國雖然沒有一套完整的立法體系，但它是世界上在國際貿易中最早考慮數據跨境流動的國家。早在 1983 年美國就為推動跨境投資流動發佈重要聲明。如今美國在數據傳輸中利用自身在全球通信產業和科技上的優勢，主導全球跨境數據的流向並對相關國家進行“長臂管轄”。

美國《澄清海外合法使用數據法案》（Clarify Lawful Overseas Use of Data Act，CLOUD）103 例 b 條中提到只要網絡服務提供者擁有、保管或控制通訊內容或記錄信息等，無論此信息是否存儲在美國國內，網絡服務提供者必須提供此項數據。

[①]李慧敏、陳光：〈論數據驅動創新與個人信息保護的衝突與平衡——基於對日本醫療數據規制經驗的考察〉，《中國科學院院刊》（北京），第 9 期（2020），頁 1143 － 1151。

（4）歐盟

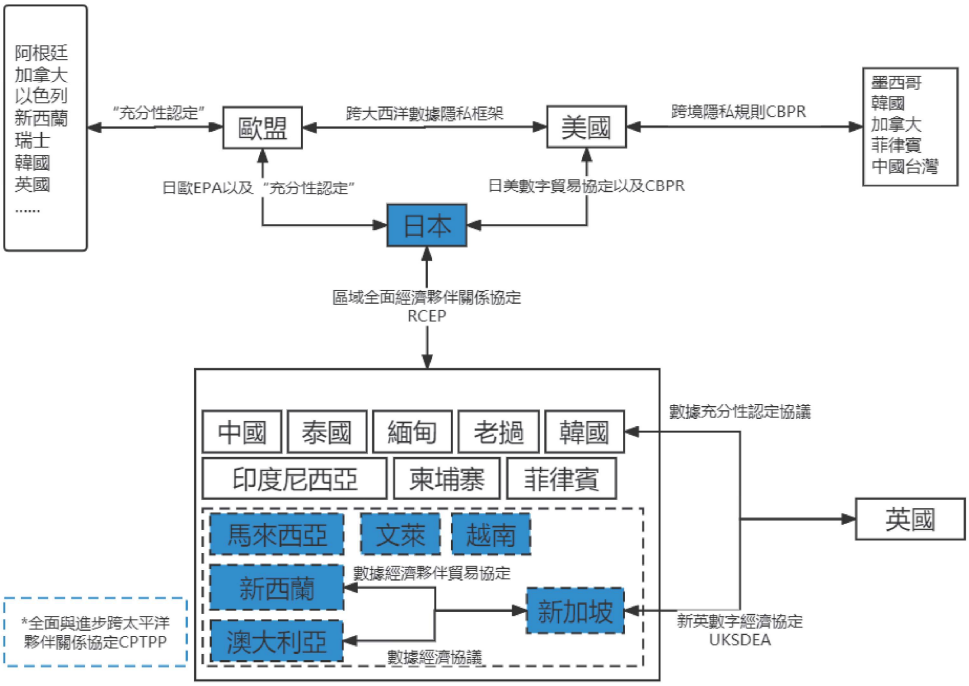
歐盟的《通用數據保護條例》（General Data Protection Regulation，GDPR）被認為是當今世界對個人數據保護水平最高的條例，出台後多次被其他國家借鑑。GDPR 對於“個人數據”的定義不僅包括姓名、住址、身份證明文件等常規信息，還包括指紋、虹膜、宗教信仰等信息。除此之外，條例中還嚴格限定企業對個人用戶數據的使用。

對於個人數據，數據主體在被告知相關風險後仍同意的情況下，可允許跨境傳輸。歐盟還為企業提供了遵守適當保障措施條件下的轉移機制，包括公共當局或機構間具有法律約束力和執行力的文件、企業約束規則、標準數據保護條款、批准的行為準則、批准的認證機制等。[①]

（5）俄羅斯

《聯邦個人數據法》要求收集和處理俄羅斯公民個人數據的所有運營者使用位於俄羅斯境內的數據中心。法令雖然不對個人數據出境做限制，但是要求數據首次存儲必須在俄羅斯境內的服務器上。俄羅斯同時希望通過數據本地化存儲加強政府執法權和對數據的控制力，這一點也在其反恐法修正案《亞羅娃亞法》（Yarovaya Law）上得以體現。該法要求在互聯網上傳播信息的組織者保留俄羅斯用戶的互聯網通信數據、用戶本身的數據和某些用戶活動的數據。[②]

圖 2　全球多個國家或組織跨境資料流動合作



[①]阿里研究院：〈重磅發佈：全球數據跨境流動政策與中國戰略研究報告〉，2019 年 9 月 19 日，www.sohu.com/a/342053712_384789，2022 年 12 月 26 日讀取。
[②]董京波：〈跨境數據流動安全治理〉，《科技導報》（北京），第 21 期（2021），頁 9 — 17。

（6）各國數據本地化

數據本地化是將數據保存在數據來源處的一種數據跨境管理措施，主要表現為某一主權國家通過制定的法律條例或規制限制本國的數據流向境外。各國對其管理的寬嚴程度如下（表 2）。

表 2　各地或組織數據本地化要求對比

國家／地區	程度	信息本地化儲存具體要求	備註
中國內地	強	《個人信息保護法》要求某幾項個人信息應當存儲在境內。	/
新加坡	強	PDPA 無強制性本地化要求。	嚴格限制數據跨境傳輸。
印度	強	《個人數據保護法案》要求數據在印度處理或存儲在印度境內。	針對不同信息類型有不同管理與限制。
韓國	強	《個人資料管理條例》第十七條要求個人資料轉移到國外必須徵得數據主體同意。	還需通過“對等原則”。
歐盟	一般	GDPR 無強制性要求。	約束數據跨境傳輸，要求高。
日本	一般	/	《全面與進步跨太平洋夥伴關係協定》要求成員國限制數據本地化存儲。
澳大利亞	一般	《個人控制電子健康記錄法》規定特殊數據經匿名化處理可境外傳輸、加工和處理。[①]	亞太的跨境隱私規則體系要求成員國限制數據本地化存儲。[②]
俄羅斯	一般	數據滿足出境合規條件即可向境外傳輸數據且可處理。	不限制個人數據的跨境傳輸，但要求數據首次存儲必須在俄羅斯境內的數據中心。
中國澳門	一般	無本地化要求，《個人資料保護法》中規定了多樣化的資料出境條件。	資料審核出境的同時大程度保證了跨境自由。
中國香港	較輕	無本地化要求，《個人資料（私隱）條例》第 33 條規定了個人資料跨境的審核條件。	至今尚未實施，不具備法律約束力。
美國	較輕	為國防部服務的雲計算服務提供商必須在境內儲存數據。	主導數據流向，維護產業競爭優勢為主，看重自由跨境流動。

（三）各國數據跨境流動對粵港澳大灣區的啓示

（1）完善法律體系與分級標準

在粵港澳大灣區，由於特殊的國情，跨境養老、醫療、金融服務等已經開始發展起

[①]馬其家、李曉楠：〈論我國數據跨境流動監管規則的構建〉，《法治研究》（杭州），第 1 期（2021），頁 91 － 101。

[②]王娜等：〈跨境數據流動的現狀、分析與展望〉，《信息安全研究》（北京），第 6 期（2021），頁 488 － 495。

來，個人敏感數據跨境必然存在很大需求。然而，三地並沒有形成統一的司法體系，現存法律中對數據分級與使用的規制上存在着細微的差別。面對在數據跨境議題下的這一新的場景，特別需要根據實際情況作出規範和細則。

在個人隱私數據方面，澳門《個人資料保護法》主要將宗教信仰，私人生活，世界觀及政治信仰等六類數據劃分為“敏感資料”（第 7 條），而在大陸《個人信息保護法》中，“敏感個人信息”又額外包括了金融賬戶、行踪軌迹、未滿十四周歲未成年人信息等（第 28 條），比澳門保護範圍更廣、更嚴格。不統一的標準在數據跨境流通時容易造成混亂，澳門特別行政區可以進一步的修改和完善其法律，爭取與內地的相關法律接軌。

（2）加強國際合作

在歐盟與美國數據跨境制度已被大多數國家接受的情況下，新加坡、日本等國為了能搶佔全球數據跨境傳輸規則制定的話語權，一直在積極參與國際合作，簽訂雙／多邊貿易協議。中國及港澳特別行政區應當適當借鑑，積極參加國際性跨境數據合作機制。例如，中國現在參與的《區域全面經濟夥伴關係協定》，對數據跨境方面沒有太多規定性的條例，可以先協商制定“指南”、“倡議”等軟法，降低條約制定的時間成本與協調成本。也可以利用金磚國家或者“一帶一路”等展開規則談判。同時，中國也需要發展和推行自己的數據跨境流動規則，可以以大灣區為試點，逐步擴大國際影響力。

澳門一直以來積極參與國際性事務，主辦了澳門國際環保合作發展論壇及展覽、澳門國際貿易投資展覽會等促進澳門與國際合作的盛事。在數據跨境方面，也可以參照這些領域與國際走過的步伐，開展論壇等加強澳門與國際之間的合作。

（3）平衡數據流通與安全

日本 APPI 雖名為“保護法”，但並沒有執着與強調數據保護，而注重在開發利用個人信息的前提下，保護個人的權利，即使對於敏感的醫療數據也是如此。

對於數據出境安全，澳門目前已經存在《個人資料保護法》，其在個人信息跨境轉移事宜上遵循“嚴格限制”的立場，將個人信息轉移到澳門以外的地方需要同時滿足兩個條件；在數據跨境白名單中，澳門個人資料保護局也未宣告任何一個國家或地區具有適當保護程度。因此，澳門在數據跨境上較為不靈活，過於注重數據安全，不利於數據流通。

新加坡《可信任資料共享框架》為數據出境安全評估體系提供了新的思路。澳門可借鑑新加坡的數據保護信任標識認證制度，對於涉及敏感個人信息跨境的企業進行類似的評估，促進粵港澳大灣區企業間數據的共享和高效利用。

（4）強化網絡安全

數據的流動必定存在潛在的風險，粵港澳大灣區的數據跨境傳輸也不例外。為了將這種風險降到最小化，三地政府除了要不斷更新和優化有關的法律政策，還需要從已經發生的國內外數據泄露事件中吸取教訓，進一步強化網絡安全，促進數據的跨境流通。

保障數據的完整性、保密性及可用性，防範網絡數據等受到意外事故和未經許可的行

為，可以有效保障澳門特別行政區的網絡安全。具體來説，首先，大灣區尤其是澳門地區應該發揮自身獨特的政治及地理優勢，開展對數據跨境安全技術體系的研究，與國際進行聯合實驗，形成國際通用的數據跨境安全平台，研究數據跨境安全技術防護手段，加強基礎設施建設；其次，對於跨境數據安全技術的最前沿成果，積極開展落地應用工作，加速成果轉化與落地應用，從而完善和增強數據跨境安全保障能力。[①]

（5）加強數據精細化監管

在中國內地，網信部門為核心，發揮着統籌協調作用，並與其他多個部門如公安部、教育部、人力資源和社會保障部等一起保護個人信息，多頭監管和分散的職權使得協作更加費時費力。而其他發達國家，幾乎都擁有自己的專門機構來進行數據跨境中的監管工作，例如歐盟的歐洲數據保護監管機構、日本的個人信息保護委員會。由此看出，內地的數據監管體系還需完善。

而對於澳門來說，雖然有了個人資料保護局作為獨立的數據保護機構，其在數據管理精細化、業務透明化方面仍有不足之處，可以進一步加強投訴受理的效率，切實做到事事有落實、件件有回音，同時，需扎實做好網絡宣傳工作，強化網站功能，準確及時地發佈相關消息。

（6）發揮治理主體能動性

對於日本目前政府主導，民間團體協作的數據跨境治理模式，粵港澳大灣區也可以進行適當借鑑。中國現階段的數據治理和美國一樣，主要依靠政府的單一治理模式。而在實踐中，企業面對數據跨境問題更具有相關經驗，高校以及科研院等掌握技術前沿，在數據跨境相關法律制度中或者政策執行中應當吸納民間團體與社會部門。

粵港澳地區的多元文化是一項優勢，應該共同建設數據跨境民間團體。這樣公開透明化的制度也能極大地增加公民對政府的信任，增強公民對數據跨境法律的認知，利於政策的推廣和實施。

對於澳門而言，自回歸之後，數據研究隊伍日益壯大，以澳門大學為首的各高校陸續開展了一系列與大數據有關的課程和活動。鼓勵更多碩博士研究生參與到數據跨境的專業研究中來，可以使得高校及科研院的主體能動性更加年輕化、專業化。高校開展的數據跨境知識普及也更能使澳門居民信服。

（7）靈活法律分層

日本根據不同行業的發展特點，為不同領域特定數據的傳輸制定出可變通的規則，“基本法”規定大多數適用情況，“專門法”規定特例。例如《次世代醫療基礎法》緩和了 APPI 中對敏感數據流通過於嚴格的做法。

從國情上看，港澳特別行政區也屬特殊地區，大陸可以針對此區域的特殊情況制定數據跨境 “專門法”，同時，港澳特別行政區也應該推行自己的“專門法”來應對粵港澳大

[①]王娜等：〈跨境數據流動的現狀、分析與展望〉，《信息安全研究》（北京），第 6 期（2021），頁 488 — 495。

灣區的信息交流，以順應粵港澳大灣區在數字金融、醫療健康等方面越來越大的個人敏感信息流動需求。

四、康養數據技術上的難點及解決方案

（一）現存平台及技術

（1）現存平台

（1.1）粵澳兩地健康碼平台

粵澳的健康碼互認，旨在解決疫情期間兩地用戶之間的個人數據交互問題，確保健康碼數據及核酸數據能夠互通及認可。為此，該平台專門採用了 FISCO BCOS 與 WeIdentity 方案。這既解決了數據溯源和不可篡改的問題，又可擴展到其他國家和地區。

（1.2）粵澳跨境數據驗證平台

粵澳跨境數據驗證平台旨在為粵澳兩地機構提供高效的跨境數據驗證設施，以方便兩地居民和企業享有便捷的跨境服務體驗，它沿襲了粵澳健康碼跨境技術方案。澳門金融機構發出可信的證明原件後，用戶自主線上提交，然後進行驗證，以確保數據真實可靠及隱私安全。

（2）平台中使用的技術

（2.1）FISCO BCOS

FISCO BCOS 是一個強大的分佈式區塊鏈應用平台，由金鏈盟開發，是在 BCOS 的基礎上改進而來的。它具有群組架構、分佈式存儲以及預編譯合約框架等功能，可以更好地實現平行擴展，以滿足高頻交易場景的需求。[①]

（2.2）WeIdentity

WeIdentity 是一套微眾銀行自主研發並完全開源的實體身份標識與可信數據解決方案，可承載實體對象（人或者物）的現實身份與鏈上身份的可信映射，以及實體對象之間安全的訪問授權與數據交換。[②]

（2.3）新型分佈式數據傳輸協議

新型分佈式數據傳輸協議（Distributed Data Transfer Protocol， DDTP），旨在讓用戶成為關鍵參與者，由用戶主動發起個人信息數據傳輸並自行上傳。協議方案基於區塊鏈技術，引入權威機構的參與，助力更安全、可信、易協作的個人信息攜帶應用。[③]與其他模式不同的是，該協議強調以用戶個人為主導，遵循分佈式理念，不依賴於數據提供者和接

[①] FISCO BCOS 區塊鏈：〈FISCO BCOS v2.9.0 技術文檔〉，2019 年，fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/introduction.html，2022 年 11 月 20 日讀取。
[②] WeIdentity：〈WeIdentity 文檔〉，2021 年，weidentity.readthedocs.io/zh_CN/latest/README.html，2022 年 11 月 12 日讀取。
[③] FISCO 金鏈盟：〈DDTP：分佈式數據傳輸協議〉白皮書 V1.0，2021 年 10 月，max.book118.com/html/2021/1026/7134005110004030.shtm，2022 年 12 月 26 日讀取。

收者雙方合作，也不依賴中心化機構推動。

（二）方案架構

（1）數據溯源關鍵技術

（1.1）實用拜占庭容錯算法

實用拜占庭容錯算法（Practical Byzantine Fault Tolerance，PBFT）主要是為了應用於不需要大交易量但需要處理許多事件的數字資產平台，每個節點都可以發佈公鑰。節點簽名全部通過的消息，以驗證其準確性。當獲得一定數量的簽名響應，交易被認定為有效。

此算法在醫療數據跨境平台上的優勢在於它可以提供可靠的系統。算法共識各節點由業務的參與方或監管方組成，安全性與穩定性由醫療業務相關方保證；其次，共識的時間延遲最短，基本可以達到醫療數據實時處理的要求；再次，共識效率高，可以滿足高頻交易量的需求。

雖然實用拜占庭算法存在一些不足，但不會影響基於聯盟鏈的醫療數據跨境平台的應用需求。以大灣區醫療康養數據組成聯盟鏈，節點數量有限，即便存在節點的擴展，也不會無限增長。實用拜占庭容錯算法不對存貯記錄的交易信息進行匿名保護，但是實際上接入聯盟鏈的交易數據也只涉及與其他節點達成交易的相關部分，且交易數據的透明化可以推動聯盟鏈各節點整體效率的提升。

（1.2）哈希時間鎖定合約

哈希鎖定，全稱哈希時間鎖定合約（Hash TimeLock Contract，HTLC），是閃電網絡中提出的一種新的技術實現形式。它可以在兩個節點之間提供安全的交易通道。在智能合約的基礎上，使用哈希加密技術，使支付者和接收者都可以確保只有在條件被滿足的情況下才能完成交易。在這樣的機制下可以實現小額支付的快速安全確認，並可以更有效的避免欺詐行為。

（1.3）簡單支付認證

簡單支付認證（Simplified Payment Verification，SPV）模式是最初的側鏈白皮書（*Enabling Blockchain Innovations with Pegged Sidechains*）中去中心化雙向錨定技術的最初設想。[①] SPV 是一種用於證明交易存在的方法，通過少量數據就可以驗證某個特定區塊中交易是否存在，非常簡便且高效。

（2）數據存儲關鍵技術

（2.1）雲計算

雲計算可以幫助使用者在共享計算資源上實現任務。它通過在網絡中連接各種計算節點來提供動態資源分配、負載均衡和自動化服務。它的優勢在於使用簡單，可以提供更高的可擴展性，節省計算成本，有較高的安全性。

[①] Back, Adam, Matt Corallo, et al. “Enabling Blockchain Innovations with Pegged Sidechains,” 2014, www.semanticscholar.org/paper/Enabling-Blockchain-Innovations-with-Pegged-Back-Corallo/348b131254a0a84083e12a4abd092114b2662bc4, accessed on 26 Dec 2022.

對於跨境醫療數據平台，因為本身數量龐大，敏感度高，並且需要進行頻繁的操作與處理，可以運用雲計算技術，在雲平台上進行平台的搭建部署，有利於提高資源利用率，節省成本和提高效率。

（2.2）基於屬性的訪問控制

基於屬性的訪問控制（Attribute-Based Access Control，ABAC），是一種靈活的授權模型，它允許使用者通過攜帶特定的屬性值，包括主題屬性和環境屬性，來發送訪問資源的請求，授權引擎會根據使用者以及相關資源的屬性，判斷使用者是否可以訪問指定資源，並給出授權結果，允許或拒絕。

在醫療康養數據的情況下，可以使醫護人員的資料訪問更加靈活。它可以精確到哪一個醫生能看到哪一個患者的資料，當這個患者出院後，對醫生的訪問權限進行快速變更等等。

（2.3）基於密文策略的屬性加密

基於密文策略的屬性加密（Ciphertext-Policy ABE，CP-ABE）是一種新型的加密技術，它可以根據指定的屬性來加密和解密數據，從而提高數據的安全性。它通過使用不同的密鑰來對不同的屬性進行加密，並將這些屬性和公鑰綁，也就相當於對這份數據進行了一個粒度可以細化到屬性級別的加密訪問控制。

密文對應於一個訪問結構而密鑰對應於一個屬性集合，僅當屬性集合中的屬性能夠滿足此訪問結構的時候才可以進行解密。

五、結束語

粵港澳大灣區作為我國數據流動的重點地區，數據跨境相關的需求日益增長，尤其是醫療康養數據方面，而在醫療數據的跨境傳輸和跨境康養上仍有不健全的地方。在法律法規方面，存在具體概念內涵不明確、數據流動監管單一混亂等問題；在倫理道德方面，隱私數據泄露與數字鴻溝是不可忽略的隱患；在安全技術方面，粵港澳大灣區也尚未擁有已落地的跨境醫療數據平台。本文對存在的問題進行梳理，並提出解決方案。在法律方面，可以借鑑其他國家，如新加坡、日本、美國等地的數據跨境流動規則，形成符合國情的數據跨境體系；在倫理道德方面，可以通過宣傳培訓，產生數據使用倫理規約，培養更加專業的醫療服務團隊；在安全技術方面，本文則研究了粵港澳等地現存的數據跨境平台，給出能夠用於醫療數據跨境平台建設的存儲及溯源技術。粵港澳大灣區的醫療數據擁有廣闊的應用發展空間，在保證數據資源能夠安全跨境傳輸的基礎上，繼續探索城市治理模式和服務模式創新，將能為三地民眾帶來實實在在的紅利。

〔責任編輯　陳超敏〕
〔校對　　倫國基〕