再訪資料跨境流通政策與法制

再訪資料跨境流通政策與法制

資訊工業策進會科技法律研究所
2022年03月25日

壹、事件摘要

資訊科技與創新基金會[1]（Information Technology and Innovation Foundation, ITIF）於2021年7月發布「跨境資料流通障礙如何在全球層次擴散」（How Barriers to Cross-Border Data Flows Are Spreading Globally）報告，指出近四年內國際間個別國家生效的資料在地化措施增加一倍以上。惟設置資料流通障礙對於一國經濟會產生重大影響，將嚴重削減其貿易總量，依ITIF根據經合組織（Organisation for Economic Cooperation and Development, OECD）市場監控數據計算，一國對資料流通之限制每增加一項，將影響總體貿易輸出達七個百分點，連帶使生產力下降，下游供應鏈的成本亦將上漲[2]。

在2020年後，因疫情造成之實體阻隔的影響，加深各方運用數位與資訊科技之力道，資料更被視為戰略性資源，各國如何對資料加以運用與掌握，不僅對數位經濟發展有正相關，更可能與國家整體安全其他面向相互連結（如國防、財務與資訊安全等）。追蹤研析各國程度與類別不同的資料在地化政策法制，資料流通限制之方式或可區分為三種模式：（1）由國家規範或限制特定類型資料傳輸境外的條件。各國常見的限制類型包括個人資料、財務／稅務／金融資料、交易支付資料（payment data）、地圖地理空間資料、健康與基因資料、政府紀錄與雲端服務（government records & cloud services）、傳統電信與網際網路通訊服務的用戶資料與內容、資通訊技術與電信資料、公共部門在地雲端（public local cloud）資料、非個人資料（non personal data framework）等。（2）以不確定法律概念限制資料傳輸標的與範圍。各國對資料流通限制越來越寬泛和模糊，動輒以「敏感」（sensitive）、「重要」（important）、「核心」（core）或與國家安全（national security）等不確定法律概念框定所欲限制的資料範圍，但這些限制往往對商業性資料流通造成重大影響。（3）以事實上資料在地化手段替代法制規範。此因個別國家或組織政策使資料傳輸因過程變得複雜、昂貴和不確定，導致企業基本上已無其他選擇，事實上僅能將資料儲存在本地，否則將面對巨額罰款，其他事例尚有對個人資料傳輸要求須得當事人明確之同意，以及要求資料傳輸前須有特別之授權[3]等。

歸納上述資料流通限制型態後，本文進一步探討各國對資料跨境流通與資料落地議題之處理態度，更新近期中國大陸、俄、美、歐盟、印度及其他重要國家所採取之政策與立法，期為我國未來掌握資料流向及規劃在地化措施預做準備。

貳、重點說明

目前國際間對於資料在地化之立場不一，除少數國家對於資料在地化採取較全面性之要求、較高強度之立法外，大部分國家僅針對特定種類資料要求資料在地化，以下依國別與要求強度進行歸類與評析。

（一）高強度資料在地化要求：中國大陸與俄羅斯

1.中國大陸

觀測國家中，資料在地化措施管理強度最高者應屬中國大陸與俄羅斯。就中國大陸而言，其直接明確在地化的法律規定如2017年《網路安全法》第37條，要求關鍵資訊基礎設施的營運者應將其在中國大陸境內蒐集和產生的個人資料與重要數據儲存於中國大陸境內。近二年中國大陸採行資料在地化之範圍逐漸擴大，其涵蓋範圍除早期係以個人資料為範圍[4]，後續則涉及如金融稅務資料、支付資料、地理位置資料、健康與基因資料、政府紀錄與雲端服務資料、電信通訊資料等非僅限於個人資料之範圍，而依2021年之《數據安全法》第21條與31條，政府甚至有權定義何謂「重要數據」，並對境內營運中心蒐集和產生的重要數據制定其得否流出境外的安全管理機制，顯見中國大陸對於資

料在地化之考量多出於維護國家安全之目的，近年更高舉維繫其數位主權的旗幟以強化其法制措施背後的論述，並以強大的科技監控能力為擔保，確保該國國家法令的落實。

2.俄羅斯

俄羅斯近年對於資料在地化措施之要求有逐漸增強之趨勢，規範密度雖未如中國大陸嚴格，但亦屬於高強度之國家，規範要求之資料種類從個人資料擴及金融稅務、電子支付資料、政府紀錄與雲端資料，乃至電信網路資料等。除要求個人資料之營運商應將處理及儲存俄羅斯公民個人資料之伺服器設置於俄羅斯境內，並向俄羅斯政府報備該伺服器之位置外，另要求每日流量超過一定數量之IT營運商應在俄羅斯建立分支機構或代表處，代表其母公司接受主管機關的管制，並規定強制執行的措施，如禁止蒐集個資、跨境傳輸個料與限制資訊使用等[5]。

中國大陸與俄羅斯因其國家體制屬性，其資料在地化法制規範與執行措施有其特定背景，往往出於國家安全整體性考量所為，但由於較不符民主憲政國家所施行之法治國原則（包括比例原則）等憲法核心要求，僅作為了解對象而較不具直接參考價值。

（二）中度資料在地化要求：美、歐、印、澳

1.美國：針對國防與稅務資料

美國因其對自由貿易的立場，加上對該國產業而言資料流通最符合該國的產業利益所在，故對於資料的限制與保護要求最為寬鬆，僅在涉及國防[6]與稅務[7]特定領域資料時，聯邦之行政規則層級有資料在地化之規定，要求資料存放於美國境內，除此之外則交由各州個別規範之。

2.歐盟：針對個人資料

歐盟利用強化網路基礎建設的政策措施，採取誘導性作法建立可信任架構，使企業更有意願使用歐盟自身的資料與服務，可認為是資料在地化的軟性誘因[8]。此外，基於其一貫維護基本價值、保護個人資料的立場，對於跨境傳輸規範較為謹慎。歐盟於2018年施行GDPR以來，對資料跨境傳輸之限制採取原則禁止、例外許可的立法模式，雖無資料在地化之名，卻已經造成事實上的資料在地化結果。加上Schrem II案判決[9]後的發展，適用新版「標準契約條款」（Standard Contractual Clauses, SCCs）對於個人資料之跨境傳輸採取高標準之適足性規範[10]，令歐盟GDPR有可能變為世界上最大的事實上（de facto）資料在地化框架[11]。另外，從歐盟近來主張數位主權的觀點，這樣的狀況似乎亦合乎歐盟的主張，但這樣的趨勢否有益於對經濟流通與發展，將是未來觀察重點。

3.印度：針對敏感性與關鍵性資料

就印度部分，印度國會於2021年12月16日通過新修正個人資料保護法（Data Protection Bill, 2021）[12] ，原2019年時法案修正內容曾要求將所有個人資料（或至少一份副本）儲存於印度境內，但通過之新法則未再做此要求。修法方向的改變推測受西方國家影響而對資料在地化的政策有所緩和，但在法律分類上的敏感性個人資料（類似我國個資法之特種資料）與關鍵性個人資料（由中央政府所指定之資料種類）方面，則運用法律中的不確定法律概念，讓主管機關掌握較大裁量空間，決定何種資料可予在地化限制，形同擴大資料管控的範圍，甚至可泛稱出於國家安全考量，即可限制資料的傳輸、在地。由此觀之，印度對於資料在地化政策，其限制措施在其個人資料保護法新近修正後也朝向擴大的趨勢[13]。

4.澳洲：針對個人醫療資料

就澳洲部份而言，因考量到健康資料的高度敏感性，其針對健康資料採在地化政策，，目前規範電子健康紀錄資料庫系統內的資料不得在境外持有及處理[14]。

（三）其他國家

而本研究觀察的其他國家目前仍採取較為謹慎保守之立場，且立法動機較為分歧，如加拿大針對國家公共機構資料採取流通限制強度較高之要求態度[15]，但因受COVID-19影響有暫緩實施的狀況[16]。德國出於課稅原因要求業者留存會計紀錄於境內，或於可線上下載情形下得放置於境外[17]；法國則對於中央與地方政府機關之資料要求應儲存於境內[18]。總體而言，各國的立法背後考量，大體係有明確並更亟欲保護之法益和目的，但亦觀察到較為特別的發展，即歐盟資料傳輸政策似乎有逐漸從自由流通走向事實上在地化的狀況，甚至有提升為主權層次議題的可能，值得再予關注。

（四）世界及區域貿易協定：傾向資料自由流通

就世界及區域貿易協定部分，檢視「跨太平洋夥伴全面進步協定」（Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP）[19]、「服務貿易協定」（Trade in Services Agreement, TiSA）[20]、「美加墨協定」（United States-Mexico-Canada Agreement）[21]以及「亞太經濟合作」（Asia-Pacific Economic Cooperation,下稱APEC）之《APEC隱私保護綱領》（APEC Privacy Framework）[22]，因貿易協定側重於國際貿易之發展，儘可能排除任何有礙貿易發展之障礙，故而其多強調資料之流通性，並以自由流通為原則。然近年因資安與隱私保護之觀念日益受到重視，故而轉為要求一定保護機制作為資料跨境傳輸之前提，雖然可能造成事實上的障礙，但整體而言國際間的貿易交流對於資料仍是採取自由流通之較開放立場，未見任何資料在地化之高強度要求。我國近期積極申請參與談判的CPTPP與TiSA，可看出參與談判的國家多半傾向不恣意限制資料的跨境流通，也傾向不任意規範外國服務者須在當地設置相關的電腦設備，CPTPP更是明訂除基於正當公共政策目標外，不得將資訊服務設施在地化列入於會員國境內執行業務之必要條件，我國將來如欲爭取加入，應確保這些國際義務的遵行。

參、事件評析

系統化觀察與分析上述國際間主要國家規範性主張之資料在地化法制政策，以及國際層級區域貿易協定與資料在地化相關之重要規定，可發現歐盟、澳、美、加針對特定類型資料，如個人醫療資料、稅務金融資料，或國家公共資料的跨境傳輸政策或資料在地化採取較強之要求，印度則出於國家安全考量亦有較強資料在地化之要求。至於相關國際與區域貿易協議雖傾向資料自由流通原則，各國談判則仍在進行中。

參考以上國際間相關法制或政策，建議我國在考量整體性資料跨境傳輸政策時：（一）可優先找出我國亟需保障的利益何在（如我國關鍵的半導體產業），並檢視其在整體產業鏈與供應鏈上的角色與定位，由此思考應採取何種模式（歐、美）的管制方式與強度。（二）確認要保護的核心利益後，可再檢視立法目的究為保護公民的隱私、確保執行機關執行公權或調查證據、保護國家安全、強化經濟成長跟競爭力、或建立公平的遊戲規則，以決定相應不同強度的資料控制手段（如單純禁止、有條件禁止到僅要求儲存副本於本地等態樣），建立起層級化規範架構。短期內建議我國或可再就資料傳輸原則予以檢視，例如現行個人資料保護法採取原則流通，例外禁止的方針是否需要變易。其次，資料傳輸與資料在地化政策法制相關規範，或可優先以金融支付資料、健康基因資料等高度敏感資料為主，基於特定部門產業之監理或數位國土、國家安全等原因，而針對性地要求採取在地化措施，並將資料類型化，針對不同屬性之資料採取不同規範標準。

[1] 資訊科技與創新基金會（ITIF）是美國非營利性公共政策智庫，總部位於華盛頓特區，研究主題專注於有關工業和技術的公共政策。美國賓州大學截至2019年為止都將ITIF列為世界上最權威的科學和技術政策智庫。ITIF， https://itif.org/（最後瀏覽日：2021/12/25）。

[2] 從該報告顯示中國大陸是對資料限制最多的國家，相關措施達29項，其次為印尼、俄羅斯與南非，其經濟均因而受影響，參考Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION[ITIF], Jul. 2021, at 4, https://itif.org/sites/default/files/2021-data-localization.pdf (last visited Dec. 25, 2021).

[3] *id.*

[4] 中國人大網，〈中華人民共和國個人信息保護法〉，2021/08/20，http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml（最後瀏覽日：2021/12/25）。

[5] Russian Federal Law No. 242-FZ, https://pd.rkn.gov.ru/authority/p146/p191/ (last visited Mar. 03, 2021).

[6] Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services(DFARS Case 2013– D018), 81 Fed. Reg. 72986, 72999(Oct. 21, 2016).(to be codified at 48 C.F.R. pt. 239).

[7] INTERNAL REVENUE SERVICE, Tax Information Security *Guidelines for Federal, State and Local Agencies* 95 (2016).

[8] Gaia-X, Gaia-X European, https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (last visited Mar. 03, 2021).

[9] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CA0311 (last visited Mar. 03, 2021).

[10] 歐盟法院（Court of Justice of the European Union）於2015年Schrems I案判決歐盟執委會「安全港隱私準則」（Safe Harbour Privacy Principles）失效後，歐盟執委會雖於2016年以第2016/1250號決定認可美國提出之「隱私盾架構」（EU-US Privacy Shield Framework），對於跨境傳輸有更嚴謹之規範，但其後的Schrems II案，經歐盟法院於2020年7月以判決宣告該隱私盾架構無效，其中理由除美國政府對外國人個資之監管與近用不符合比例原則外，美國法制架構亦無提供適當之救濟手段，令權利受侵害之人得以獲得賠償。惟歐盟法院對歐盟執委會通過第2010/87號決定之「標準契約條款」，則認為已納入有效之保障機制；倘資料傳輸方或接受方未能遵守SCCs或缺乏歐盟法律所要求之保護程度，歐盟主管機關可命令暫停或停止相關傳輸，因此仍肯認「標準契約條款」之有效性。但SCCs始終無法解決美國法欠缺法律救濟之爭議，故而歐盟法院採取較保留態度，另要求締約國之企業應確保資料接受方所在之各國法規可提供符合歐盟個資法保護相關規範之保護水準，並建議採取「補充措施」以保護跨境傳輸之資料，其後，歐盟執委會於2020年底以（EU）2021/914號執行決定（Implementing Decision）發布的新版SCCs取代舊版條款。*see Cross Border Transfer Master Class: Onward transfers from a US controller to a processor that is outside of the US and the EEA*, NATIONAL LAW REVIEW, Dec. 24, 2021, https://www.natlawreview.com/article/cross-border-transfer-master-class-onward-transfers-us-controller-to-processor (last visited Dec. 25, 2021).

[11] Nigel Cory, *How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION[ITIF], Jul. 8, 2021, https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data (last visited Dec. 25, 2021).

[12] *The Data Protection Bill*, TRILEGAL, Dec. 24, 2021, https://trilegal.com/knowledge_repository/the-data-protection-bill-2021/ (last visited Dec. 25, 2021).

[13] The Personal Data Protection Bill(2018), MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited Mar. 03, 2021).

[14] Stronger My Health Record privacy laws, AUSTRALIAN DIGITAL HEALTH AGENCY, Nov. 26, 2018, https://www.myhealthrecord.gov.au/about/legislation-and-governance/summary-privacy-protections (last visited Dec. 25, 2021).

[15] Freedom Of Information And Protection Of Privacy Act § 30(1)(1996), BRITISH COLUMBIA, https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00 (last visited Mar. 03, 2021).

[16] Ryan Berger & Cory Sully, *BC Government Relaxes "In Canada Only" Data Hosting Requirements for Public Bodies Due To COVID-19,* PRIVACY, Mar. 30, 2020, https://www.lawsonlundell.com/change-your-privacy-settings-here/bc-government-relaxes-in-canada-only-data-hosting-requirements (last visited Dec. 25, 2021).

[17] Handelsgesetzbuch (HGB) § 257(2020).

[18] Martina F Ferracane, *Restrictions on cross-border data flows*(2017), EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

(ECIPE), at 14, https://www.econstor.eu/bitstream/10419/174853/1/ecipe-wp-2017-01.pdf (last visited Dec. 25, 2021).

[19] 「跨太平洋夥伴全面進步協定」（CPTPP）簡介，中華民國外交部，https://www.mofa.gov.tw/cp.aspx?n=2613（最後瀏覽日：2021/12/15）。

[20] Trade in Services Agreement (TISA), FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND CLIMATE ACTION, https://www.bmwk.de/Redaktion/EN/Artikel/Foreign-Trade/tisa.html (last visited Mar. 03, 2021).

[21] United States-Mexico-Canada Agreement, OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE[USTR], https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement (last visited Mar. 03, 2021)

[22] APEC Privacy Framework (2015), APEC, https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) (last visited Mar. 03, 2021).

相關連結

- ITIF
- 中華人民共和國個人信息保護法
- Russian Federal Law No. 242-FZ
- Gaia-X European
- Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems
- see Cross Border Transfer Master Class: Onward transfers from a US controller to a processor that is outside of the US and the EEA
- How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime
- The Data Protection Bill
- Stronger My Health Record privacy laws
- Freedom Of Information And Protection Of Privacy Act § 30(1)(1996)
- BC Government Relaxes "In Canada Only" Data Hosting Requirements for Public Bodies Due To COVID-19
- 「跨太平洋夥伴全面進步協定」（CPTPP）簡介
- Trade in Service Agreement (TiSA)
- United States-Mexico-Canada Agreement
- APEC Privacy Framework (2015)

相關附件

- How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them [pdf]
- The Personal Data Protection Bill(2018) [pdf]
- Restrictions on cross-border data flows(2017) [pdf]

你可能會想參加

→ 數位海盜時代來臨─抵禦海上資安威脅的實踐與挑戰
→ 新創不容忽視的數位行銷「蝴蝶效應」 如何運用數位力為企業注入新生命
→ 零售業個資保護宣導暨座談會
→ 零售業個資保護及資訊安全教育講習
→ 零售業個資保護及資訊安全教育講習

洪政緯
法律研究員 編譯整理

上稿時間：2022年04月

文章標籤

個人資料 數位經濟 隱私保護 資料運用 APEC CBPR

推薦文章