三、中共數據安全立法對臺之影響

臺北大學法律學院王震宇副院長主稿

- **中共數據安全法為中國大陸第一部「數據安全」立法，對外宣告北京對「數據主權」的高度重視。**
- **該法規定細節繁多且具法律懲罰之效果，對涉及陸數據的臺商與外資而言，不可不慎。**

（一）數據安全法之立法背景

2021 年 6 月 10 日中共於第十三屆全國人民代表大會常務委員會第二十九次會議通過「中華人民共和國數據安全法」（以下簡稱「數據安全法」），自同年 9 月 1 日起施行，為中國大陸第一部「數據安全」立法，該法開宗明義說明其目的係為「規範數據處理活動，保障數據安全，促進數據開發利用，保護個人、組織的合法權益，維護國家主權、安全和發展利益」（第 1 條）。「數據安全法」共計有 7 章 55 條，包括數據安全與發展、數據安全制度、數據安全保護義務、政務數據安全與開放以及相關法律責任等內容。

值得注意者，雖然本法並沒有特別排除個人資料保護，但陸另有制定「個人信息保護法」作為特別法之適用；且涉及國家秘密之數據處理，則適用「中華人民共和國保守國家秘密法」（第 53 條）；並排除軍事數據安全保護適用本法的空間，由中共中央軍事委員會另行制定之（第 54 條）。陸在制定「數據安全法」之法律體系架構，很大一部分參考了歐盟之立法體制，將「個人」與「非個人」之數據進行區別，而形成「一般資料保護規範」（General Data Protection Regulation, GDPR）與「非屬個資之資料流通規則」（Regulation on the Free Flow of Non-personal Data）之法規範。

「數位主權」（Digital sovereignty）與「資料在地化」（Data Localization）是二十一世紀以來，歐盟、美國、中國等大國不斷競逐的場域，隨著巨型跨國企業的大數據資料掌握，讓國家政府提高管制層級，並提升為「國家安全」的位階。數位安全法中明確規定，「維護數據安全，

應當堅持總體國家安全觀，建立健全數據安全治理體系，提高數據安全保障能力」（第 4 條）。基於國家總體安全觀，網路與數據安全屬於政治、軍事、領土主權等之外的「非傳統安全」範疇，數據的掌握與取得，在當代國家安全戰略體系中的地位十分關鍵。無論是出於中國對於與美國各領域競爭的白熱化、或者對於中國境內或境外各種數據資料的蒐集與跨境傳輸之警覺與管制，都象徵著「數據安全法」已被中共視為具有高度戰略意義的國家安全層次立法。

（二）數據安全法規範之重要基本定義與原則

本文以下簡要介紹「數據安全法」中的基本定義與原則，作為後續進行法律分析的基礎：

首先，「數據」（Data）在臺灣亦稱為「資料」，依該法之定義：「數據係指任何以電子或者其他方式對資訊的記錄」（第 2 條第 1 項）；而由上述定義所延伸之「數據處理」，則包括對於數據的「收集、存儲、使用、加工、傳輸、提供、公開等」（第 2 條第 2 項）；至於對「數據安全」所隱含的風險及其預防措施，則有謂「通過採取必要措施，確保數據處於有效保護和合法利用的狀態，以及具備保障持續安全狀態的能力」（第 2 條第 3 項）。就第 2 條定義而言，「數據」未免涵蓋一切「資訊」（information）而太過廣泛；因此，本法在草案時期，即要求對於數據建立分類分級保護制度，概分為「核心數據」、「重要數據」及「一般數據」等不同級別，以茲遵循。

其次，本法最至關重要的條文乃為其「適用範圍」之規定，「在中華人民共和國境內開展數據處理活動及其安全監管，適用本法（第 2 條第 1 項）。在中華人民共和國境外開展數據處理活動，損害中華人民共和國國家安全、公共利益或者公民、組織合法權益的，依法追究法律責任 （第 2 條第 2 項）」。就國際法上之管轄權（jurisdiction）觀之，第 2 條第 1 項屬於屬地主義的「領域管轄」（territorial jurisdiction），凡在中共廣義領土主權範圍內所開展的數據處理活動皆受其管轄概無疑問，畢竟領域管轄乃屬於國內司法管轄範疇，各國皆然；比較值得關注的是同條第 2 項將「數據處理活動」視為「保護管轄」（protective

jurisdiction）的一部分，也可稱為是「域外管轄」（extraterritorial jurisdiction）或「長臂管轄」（long-arm jurisdiction），由於將一國國內管轄權延伸至領域外的任何地區，此立法技術在比較法上多半是為了保護攸關國家的重大政治或經濟利益。[1]在本條規範下，中國大陸監管境內外所有涉及數據處理公司的權力，意味網絡安全審查對象是針對所有企業，無論是中資、臺商、或外資，無論數據處理地點在中國境內或境外。

再其次，數據安全法訂出對於中央、地方與各特殊部門間的數據安全分層負責機制。在中央層級，「中央國家安全領導機構負責國家數據安全工作的決策和議事協調，研究制定、指導實施國家數據安全戰略和有關重大方針政策，統籌協調國家數據安全的重大事項和重要工作，建立國家數據安全工作協調機制」（第 5 條）；在地方層級，「各地區、各部門對本地區、本部門工作中收集和產生的數據及數據安全負責」（第 6 條第 1 項）；在個別部門中，「工業、電信、交通、金融、自然資源、衛生健康、教育、科技等主管部門承擔本行業、本領域數據安全監管職責」（第 6 條第 2 項）、「公安機關、國家安全機關等依照本法和有關法律、行政法規的規定，在各自職責範圍內承擔數據安全監管職責」（第 6 條第 3 項）、「國家網信部門依照本法和有關法律、行政法規的規定，負責統籌協調網路數據安全和相關監管工作」（第 6 條第 4 項）。除監管單位的分層分級外，對於「數據使用」之原則，該法強調必須「依法、合理、有效」（第 7 條），甚至在法條中有許多連結「尊重社會公德和倫理，遵守商業道德和職業道德，誠實守信，履行數據安全保護義務，承擔社會責任，不得危害國家安全、公共利益，不得損害個人、組織的合法權益」（第 8 條）等上位概念，是否會形成不確定之法律概念，仍需觀察其後的實踐。

最後，「數據安全法」賦予「吹哨者」（Whistleblower）之地位，「任何個人、組織都有權對違反本法規定的行為向有關主管部門投訴、舉報」（第 12 條第 1 項），而收到投訴或舉報的部門應當及時依法處理，並「應當對投訴、舉報人的相關資訊予以保密，保護投訴、舉報人的

[1]美國的「域外管轄」最為著名的有關於反托拉斯法(anti-trust law)的域外適用，美國 1982 年修訂了「外國貿易反托拉斯促進法」（Foreign Trade Antitrust Improvement Act）即規範了對於領域外行為之適用。

合法權益」(第 12 條第 2 項)。至於如何認定是否違法則初步係由主管部門進行行政裁量，而非進入司法程序，此部分是否有可能因為商業上的敵意競爭而惡意投訴、濫訴、舉報，則仍是考驗該法實施後，中共各主管部門對於數據安全的處理與辨識能力，否則將成為企業在數據管理上存在不確定之法律風險。

（三）數據安全法數據「開發利用」與「安全保障」之關係

數據安全法之宗旨係平衡「數據開發利用」與「數據安全保障」間之關係（第 13 條），且首次於法規中提出「數據基礎設施建設」的概念，支援數據在各行業、各領域的創新應用（第 14 條），顯見中國大陸除對於數據安全之監管外，亦開始將「數據」視為與高鐵、公路、公共衛生、教育等等量齊觀之「基礎建設措施」。

值得注意者，「數據安全法」欲建立一套「數據安全標準體系」之建立，該法要求中共國務院應「標準化行政主管部門和國務院有關部門根據各自的職責，組織制定並適時修訂有關數據開發利用技術、產品和數據安全相關標準。國家支援企業、社會團體和教育、科研機構等參與標準制定」(第 17 條)。在數據使用技術高速發展的情況下，立法往往滯後於行業發展，透過「數據安全法」之統一立法形式，並將行業組織的行為規範、團體最佳實踐標準等實踐經驗加以彙總，逐漸構成數據安全標準體系的重要部分。除「數據安全標準體系」外，法條中亦強調「安全檢測評估、風險評估、認證專業機構、交易管理制度、數據交易市場」等具體作法（第 18 條、第 19 條)。顯見陸極力尋求在「與數據有關之技術性標準」(Data-Related Aspects of Technical Standard）中的話語權，甚至未來於國際組織或協定中形成由中國所建構「數據安全國際標準」之企圖心。

數據安全法將「公共數據」之定性明確規範為「新型國有資產」，其「數據所有權與使用權」歸國家所有，也象徵「數位主權」之法律上主張，這是在理解中共對於數據安全保護的重要脈絡。在該法中，具體規範涉及「數據全生命週期」(Life Circle of Data） 的數據安全基本方針、原則和制度要求，簡要說明如下：

1. 數據分類分級保護制度（第 21 條）：國家建立數據分類分級保護制度，根據數據在經濟社會發展中的重要程度，以及一旦遭到篡改、破壞、洩露或者非法獲取、非法利用，對國家安全、公共利益或者個人、組織合法權益造成的危害程度，對數據實行分類分級保護。國家數據安全工作協調機制統籌協調有關部門制定重要數據目錄，加強對「重要數據」的保護（第 1 項）。關係國家安全、國民經濟命脈、重要民生、重大公共利益等數據屬於國家核心數據，實行更加嚴格的管理制度（第 2 項）。各地區、各部門應當按照數據分類分級保護制度，確定本地區、本部門以及相關行業、領域的重要數據具體目錄，對列入目錄的數據進行重點保護 （第 3 項）。

2. 數據安全風險評估機制（第 22 條）：由國家建立集中統一、高效權威的數據安全風險評估、報告、資訊共用、監測預警機制。國家數據安全工作協調機制統籌協調有關部門加強數據安全風險資訊的獲取、分析、研判、預警工作。

3. 數據安全應急處置機制（第 23 條）：國家建立數據安全應急處置機制。發生數據安全事件，有關主管部門應當依法啟動應急預案，採取相應的應急處置措施，防止危害擴大，消除安全隱患，並及時向社會發佈與公眾有關的警示資訊。

4. 數據安全審查制度（第 24 條）：國家建立數據安全審查制度，對影響或者可能影響國家安全的數據處理活動進行國家安全審查。依法作出的安全審查決定為最終決定。

5. 數據的出口管制制度（第 25 條）：國家對與維護國家安全和利益、履行國際義務相關的屬於管制物項的數據依法實施出口管制。

6. 對境外歧視措施的對等措施（第 26 條）：任何國家或者地區在與數據和數據開發利用技術等有關的投資、貿易等方面對中華人民共和國採取歧視性的禁止、限制或者其他類似措施的，中華人民共和國可以根據實際情況對該國家或者地區對等採取措施。此條針對境外歧視行為的反制措施條款（provision of counter-measures）很明顯係針對歐美國家近期對於中國在「數位貿易或投資規範」等具歧視性之限

制或禁止措施而來。

7. 政務數據安全與開放：在數據安全法第 37 條至 43 條中規範關於中共的政務數據安全以及公開原則，此章的條文類似於各國的「政府資訊公開法」，只是將此「資訊」定義在「數據」資料的揭露，其法律責任與義務與中共的中央與地方政府關聯性較大，與一般企業或私人較無關聯性。

（四）數據安全保護義務及其法律責任

「數據安全法」對於各種可能衍生法律責任之條文及其對應之罰則規定做詳細的規範，由於涉及之行為態樣較多，以下僅就「數據安全保護義務及其法律責任」之重要條文進行彙整，相關內容攸關臺商或外資之權利及義務，在涉及違反該法，或有違反該法之虞時，不得不提早進行法律風險預防之偵測。

1. 開展數據處理活動的組織、個人不履行數據安全保護義務之法律責任：

（1）開展數據處理活動應當依照法律、法規的規定，建立健全全流程數據安全管理制度，組織開展數據安全教育培訓，採取相應的技術措施和其他必要措施，保障數據安全。利用互聯網等資訊網路開展數據處理活動，應當在網路安全等級保護制度的基礎上，履行上述數據安全保護義務。重要數據的處理者應當明確數據安全負責人和管理機構，落實數據安全保護責任。（第 27 條）

（2）開展數據處理活動應當加強風險監測，發現數據安全缺陷、漏洞等風險時，應當立即採取補救措施；發生數據安全事件時，應當立即採取處置措施，按照規定及時告知用戶並向有關主管部門報告。（第 29 條）

（3）重要數據的處理者應當按照規定對其數據處理活動定期開展風險評估，並向有關主管部門報送風險評估報告。風險評估報告應當包括處理的重要數據的種類、數量，開展數據處理活動的情況，

面臨的數據安全風險及其應對措施等。（第 30 條）

（4）法律責任：開展數據處理活動的組織、個人不履行本法第 27 條、第 29 條、第 30 條規定的數據安全保護義務的，由有關主管部門責令改正，給予警告，可以併處 5 萬元以上 50 萬元以下罰款，對直接負責的主管人員和其他直接責任人員可以處 1 萬元以上 10 萬元以下罰款；拒不改正或者造成大量數據洩露等嚴重後果的，處 50 萬元以上 200 萬元以下罰款，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處 5 萬元以上 20 萬元以下罰款。違反國家核心數據管理制度，危害國家主權、安全和發展利益的，由有關主管部門處 200 萬元以上 1000 萬元以下罰款，並根據情況責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照；構成犯罪的，依法追究刑事責任。（第 45 條）

2. 向境外提供重要數據的之法律責任：

（1）關鍵資訊基礎設施的運營者在中華人民共和國境內運營中收集和產生的重要數據的出境安全管理，適用「中華人民共和國網路安全法」的規定；其他數據處理者在中華人民共和國境內運營中收集和產生的重要數據的出境安全管理辦法，由國家網信部門會同國務院有關部門制定。（第 31 條）

（2）違反本法第 31 條規定，向境外提供重要數據的，由有關主管部門責令改正，給予警告，可以併處 10 萬元以上 100 萬元以下罰款，對直接負責的主管人員和其他直接責任人員可以處 1 萬元以上 10 萬元以下罰款；情節嚴重的，處 100 萬元以上 1000 萬元以下罰款，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處 10 萬元以上 100 萬元以下罰款。（第 46 條）

3. 從事數據交易仲介服務的機構之法律責任：

（1）從事數據交易仲介服務的機構提供服務，應當要求數據提供方說明數據來源，審核交易雙方的身份，並留存審核、交易記錄。（第

33 條）

（2）從事數據交易仲介服務的機構未履行本法第 33 條規定的義務的，由有關主管部門責令改正，沒收違法所得，處違法所得 1 倍以上 10 倍以下罰款，沒有違法所得或者違法所得不足 10 萬元的，處 10 萬元以上 100 萬元以下罰款，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照；對直接負責的主管人員和其他直接責任人員處 1 萬元以上 10 萬元以下罰款。（第 47 條）

4. 拒不配合公安機關、國家安全機關調取數據之法律責任：

（1）公安機關、國家安全機關因依法維護國家安全或者偵查犯罪的需要調取數據，應當按照國家有關規定，經過嚴格的批准手續，依法進行，有關組織、個人應當予以配合。（第 35 條）

（2）違反本法第 35 條規定，拒不配合數據調取的，由有關主管部門責令改正，給予警告，並處 5 萬元以上 50 萬元以下罰款，對直接負責的主管人員和其他直接責任人員處 1 萬元以上 10 萬元以下罰款。（第 48 條第 1 項）

5. 未經主管機關批准向外國司法或者執法機構提供數據之法律責任：

（1）中華人民共和國主管機關根據有關法律和中華人民共和國締結或者參加的國際條約、協定，或者按照平等互惠原則，處理外國司法或者執法機構關於提供數據的請求。非經中華人民共和國主管機關批准，境內的組織、個人不得向外國司法或者執法機構提供存儲於中華人民共和國境內的數據。（第 36 條）

（2）違反本法第 36 條規定，未經主管機關批准向外國司法或者執法機構提供數據的，由有關主管部門給予警告，可以併處 10 萬元以上 100 萬元以下罰款，對直接負責的主管人員和其他直接責任人員可以處 1 萬元以上 10 萬元以下罰款；造成嚴重後果的，處 100 萬元以上 500 萬元以下罰款，並可以責令暫停相關業務、停

業整頓、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處 5 萬元以上 50 萬元以下罰款。（第 48 條第 2 項）

（五）數據安全法對臺灣之影響

中共在 2021 年 9 月實施「數據安全法」前，已經針對中國境內擁有大量重要關鍵數據的電商平臺，如：滴滴出行、阿里巴巴及外資特斯拉、蘋果、臉書等大型企業，進行數據安全審查及相關監管措施。而在該法實施後，則更有法律上依據來行使「數位主權」，並將領域管轄及保護管轄交互運用，不分中國境內外的企業，只要涉及收集、處理、使用、公開關於「數據安全法」之界定範圍，都可能受到該法的規範。由於該法為中共第 1 部對於數據安全之重要立法，對於未來臺灣的影響不可小覷，而臺商在全球甚至中國大陸市場布局時，尤其應該注意法律的責任與效果，以免引發不必要的法律風險及受到調查。以下為本文的幾項觀察與建議：

1. 政府應隨時留意「數據安全」的國際標準及相關協定談判：由於美國與中國在高科技場域的競爭日趨緊張，再加上歐盟對於數位規則又早有相關的立場，國際間形成大國間競逐話語權的局面。「國際標準」的制定往往都是在大國角力與妥協下的產物，「數據安全」的爭鋒相對於不久的未來是否會有預料之外的發展，目前無論是 APEC、WTO 或其他區域架構中都尚無形成多邊協定的可能性，我國政府更應該針對中國、美國、歐盟等對於數據安全之相關立法進行研析，以制定未來的因應對策。

2. 在可見的未來，臺商無論是在中國大陸境內投資、或籌資到美國、歐盟、或第三地上市等，只要其營運範圍內涉及「與中國有關的數據」，都必須注意「數據安全法」之適用及其法律責任，尤其在建立「數據中心」或關於「數據資料在地化」考量時，可能都必須「分流處理」。亦即將美國、歐盟、中國等有建立「數據安全規則」之市場加以區隔，避免在大國角力的過程中，成為法律制裁的犧牲品。

3. 臺商在處理關於「數據跨境移動」之業務時，應特別留意在「數據安全法」下的數據安全級別，尤其在大陸境內營運中涉及收集和產生重要數據的「出境」時，更必須了解該法與其他監管法規的限制；且今後將難以拒絕監管機構、公安機關或國家安全機關關於調取數據的要求。