2021 年中國大陸數據安全法新制及其對臺商的影響

文《行政院國家資通安全會報技術服務中心[1]》

7 月 29 日，2021 世界安防博覽會在廣州開幕，海康威視展覽區攝影鏡頭結合大數據平臺運用。

前言

中國大陸自從 2015 年 (民國 94 年) 公告國家安全戰略綱要後，已陸續制定《國家安全法》、《網絡安全法》、《密碼法》、《數據安全法》等法律且彼此互相呼應、補充的規範。這些法律的範圍與處理的主要議題雖然不同，但對網路與技術面向之控管與著墨，則是重要的共通點，對商務活動將產生一定影響。尤其是《密碼法》、《數據安全法》，這兩部法律的主要規範對象已從少數性質較特殊的運營者 (例如，經營涉及油、水、電等關鍵資訊基礎設施者)，轉變為包括一般企業，使得一般企業不再像從前僅是受到間接影響而已。本文將探討今 (2021) 年 6 月 10 日通過，自 9 月 1 日施行之《數據安全法》[2]。

依《數據安全法》定義，所謂數據即是對資訊 (該法稱之為信息) 所為的記錄，無論電子或非電子形式均包括在內。除了對數據的定義廣泛，該法規範之對象也幾乎包含了其境內各公、私部門組織，部分情形甚至包括境外組織，因此影響範圍甚大。在內容上，《數據安全法》有兩大主軸，其一

註 1、作者為李婉萍、陳宏志，本文為行政院國家資通安全會報技術服務中心「國際資安組織與法制政策研析」研究成果。

註 2、中國人大網，《中華人民共和國數據安全法》，載於：http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml（最後瀏覽日：2021 年 7 月 20 日）。

是對數據安全的維護，另一則是關於數據之發展與利用。

對中國大陸臺商來說，此法最直接的影響，首先是增加了許多須注意、配合之事項;另一方面，臺商也可能有機會評估中國大陸對數據發展、利用的政策，進行相關的投資規劃。此外，中國大陸即將透過《數據安全法》對其所稱「重要數據」進行出口管理 (第 31 條)，以及對他國採取關於數據或相關技術的同等措施 (第 26 條) 之情形下，臺商不得不立即重新思考其經營定位並調整全球布局的處境。《數據安全法》施行後，不管是不是臺商，像滴滴出行這樣 6 月赴他國上市，7 月 APP 旋即遭中國大陸官方下架，或其他商務經營受限的例子，在《數據安全法》施行後恐會增加。

中國大陸《數據安全法》內容簡介

一、關於數據安全之規定

(一) 包羅廣泛的「數據」及對數據內容的分類分級掌握

如前述，《數據安全法》所稱數據，範圍相當廣泛，依該法第 3 條，以電子或其他任何形式記錄的資訊，都被認定在數據的範圍。同法第 21 條指出：其將依據數據在經濟社會的重要程度，及其遭竄改或洩漏對國家安全、公共利益或其他合法權益造成的危害，對數據進行分類分級保護要求；從該法的內容脈絡看來，未來中國大陸之數據，至少會區分成關係其經濟命脈、國家安全或重大公益之「國家核心數據」、「重要數據」及「其他數據」等三級。

過去，中國大陸針對資訊、資訊技術或周邊之管制，常採取分級管制之方式，例如依其《計算機信息系統安全保護條例》而來的信息安全等級保護規定，因《網絡安全法》而來的網路安全等級保護規定等。上述多是針對系統等技術層面而為的規定，但《數據安全法》的分類分級規定則將直接針對數據本身，換言之，直接涉及數據的內容。

依《數據安全法》目前的規定看來，上述數據之內容，理論上似未排除組織的財務資訊、客戶資訊、研發資訊及其他與營業、競爭相關的任何資訊；而資訊一旦被認定為「重要數據」，就必須依《數據安全法》第 30 條，向主管機關提出數據的種類、數量、數據處理 (蒐集、存儲、加工、傳輸、提供、公開等皆屬處理) 的情形，及數據風險評估與應對措施。這是強度相當高的資訊掌握，對企業來說當然就必須考量有機密商業資料之概況被掌握的可能，必須與客戶就這部分進行溝通與應對調整。

此外，如數據經認定係「國家核心數據」，則可能會受到更嚴格的控管。當然，究竟企業的資訊有多少會被認定成「國家核心數據」或「重要數據」，以及被要求的程度如何，真正納管的數據內容到底對企業有多敏感，還是要看後續配套之「數據分類分級保護制度」細節內容，以及當局所要求提交之風險評估報告的細項而定。

(二) 數據處理者須建立數據安全管理制度

依據《數據安全法》第 27 條，進行數據處理活動之組織或個人，均須建立數據安全管理制度。該制度之重點，包括下一段所歸納該法第 28 條至第 36 條的要求；而未遵守相關要求者，依第 44 條至第 48 條，視違反條文及情節輕重，可能被處以最高 1,000 萬元之罰款，亦可能被停業、吊銷許可或執照，且違反者為組織時，組織之相關主管人員或直接負責業務之人員，也可能被處以最高至 100 萬元之罰款。

《數據安全法》第 28 條至第 36 條對組織處理數據之要求，歸納、摘要如下：

1、監測數據處理過程中之風險、修補漏洞，回應、處置，並向主管機關陳報與數據安全相關之事件。

2、對「重要數據」之處理活動進行風險評估並提交報告。

3、一般組織 (如關鍵資訊基礎設施運營者以外之一般企業) 的「重要數據」須符合中國大陸國家網信部門 (國家互聯網信息辦公室) 與國務院相關部門會同訂定之出境管理規定。

4、數據交易中介者，須要求交易數據之雙方提供身分、說明數據來源，並留存相關紀錄。

5、配合提供數據予公安或國安相關機關，以利其進行國安事務或調查犯罪。

6、非經核准，禁止對境外提供存儲於中國大陸境內之數據。

二、關於數據發展與利用之規定

《數據安全法》的重點，除了數據安全的維護外，還包含建立數據的發展與利用，這部分主要以

對國家機關的要求來呈現，除了政務數據開放目錄與安全可控的開放平臺建置 (第 42 條)，以及政務數據原則公開的要求 (第 41 條) 外，亦有關於數據安全的規範 (第 38、39 條)，以及委外建置、維護政務系統或存儲、處理數據時的安全維護要求 (第 40 條)。

此外，在鼓勵數據發展、利用以及技術研發及商業創新 (第 13、14、16 條) 方面，《數據安全法》要求相關機關制定關於數據開發技術、產品與數據安全之標準，並提供檢測、驗證服務 (第 17、18 條)；後續亦規劃建立數據交易管理制度與交易市場，及促進相關人才之培訓 (第 19、20 條) 等。這些規定對臺商來說，也可能產生商機；但關於這些商機的具體細節，亦須注意有無類似前述安全維護部分所提之情形。

臺商應有的認知與對策

一、應注意後續之配套標準與規章

《數據安全法》規範之對象甚廣，臺商幾乎不可能自外於該法之規範範疇。在安全維護面向上，尤其是與網際網路或科技製造相關者，如從事數據技術研發、商業創新之企業，以及數據交易中介服務機構之臺商，因所處理之數據不論在質或量上都屬可觀，較可能受到中國大陸關於重要數據或國家核心數據相關之規範。此類臺商務必注意後續各主管部門，如網信辦、商務部或公安部所發布之行政法規，以免遭高額罰款或停業、吊銷執照等處分。

此外，除掌握《數據安全法》相關規定外，對《網絡安全法》等具有高度相關性之既有規定，亦應一併留意。在數據發展與利用方面，對相關商機有興趣之臺商，須關注中國大陸後續提出之標準、辦法等配套措施或規定。

茲就各項業務相關機關之可能分工臚列如下，以利臺商留意。

1、網路環境或設施監管：網信辦、工業和信息化部。

2、企業數據監管：各目的事業主管機關。

3、犯罪防制事務：公安部、國安機關。

雖《數據安全法》甫於 9 月 1 日施行，在各主管部門所訂定之配套法規出爐前，已有單位釋出相關文件，如工業和信息化部所屬之中國互聯網協會於 7 月 1 日發布《數據安全治理能力評估方法》。該方法雖屬自願性之團體標準 (編號：T/ISC-0011-2021)，但其涵蓋數據安全戰略、數據全生命週期安全、基礎安全等內容；針對，例如，數據分類分級、合規管理、監控審計、鑑別訪問、風險與需求分析、以及安全事件應急等事項均有著墨，臺商或可先以之做為投入相關產業規劃之參考。

二、盡快評估數據風險報告提交、數據出口管制、配合同等措施等要求對經營之影響

依《數據安全法》目前的規定看來，企業之資訊一旦在分類上被認定為「重要數據」以上之分級，就必須向主管機關提出這些數據的評估報告，且也會受到出口管理或遵循中國大陸對他國採取同等措施等要求之規範。這對商務之進行及與客戶的保密約定等，必然有所影響。在《數據安全法》之前，中國大陸也出現過個別領域的數據分級規範，例如，2020 年 2 月工業和信息化部發布之《工業數據分類分級指南 (試行)》等。前述規範之分級標準雖與日後《數據安全法》的分級標準不會完全相同，但在《數據安全法》配套規定明確之前，不失為可能的參考。

《工業數據分類分級指南 (試行)》係將研發設計數據、開發測試數據、物流數據、產品售後服務數據、客戶數據、人事財務數據等，依其潛在影響性或發生問題時所可能造成的經濟損失分成三級；此分級參考，對企業在盤點並試著對所持有之資訊先進行分級，以研判可能會被要求提交的數據關聯資料範圍時，或有一定幫助。

此外，臺商在經營上亦須考量我國或其他重要商務往來國家之法律規定，如果臺商之業務經營、其他法遵義務與《數據安全法》間，經評估有難以相容之部分，則必須盡快規劃採取將業務拆分 (至其他國家)，或其他能與客戶達成共識且亦符合我國及其他業務關聯國家法律之處理方式，以免造成經營時之困難。