構建兼具國際視野和本土特色治理體系 助業界數據淘金

數據淘金 系列五（完）

在「數據即黃金」的時代，企業正以前所未有的速度挖掘數據價值，從精準行銷到風險模型，應用場景遍地開花。然而，這場數據淘金熱的狂歡背後，卻潛藏着嚴峻的隱患：個人隱私資料、商業機密、金融交易數據等，正面臨被盜取與濫用的風險，相關法律正是守護數據安全的最後一道防線，構建起保障數據秩序的天羅地網。然而，現實中仍存在諸多法律困局：法規追不上技術迭代、企業合規意識不足、跨境數據流動的管轄爭議，以及執法與監管的落差。當創新的腳步不斷衝撞法律紅線，企業如何在不越界的前提下全速前進，將是決勝未來數據戰場的關鍵。

●香港文匯報記者 蔡競文

●孖士打律師行合夥人梁樂鋒

資料保安措施需涵蓋7大範疇

1. 資料管治及機構性措施；
2. 風險評估；
3. 技術上及操作上的保安措施；
4. 資料處理者的管理；
5. 資料保安事故發生時的補救措施；
6. 監察、評估及改善；
7. 其他考慮，如雲端服務、自攜裝置（BYOD）及便攜式儲存裝置。

資料來源：《資訊及通訊科技的資料保安措施指引》

在數據驅動經濟的時代，企業手握海量數據，猶如擁有一座待開發的金礦。然而，如何合法、合規且安全地「淘金」，成為業界成敗的關鍵。香港的《個人資料（私隱）條例》（PDPO）及其相關指引，不僅是監管框架，為數據行業提供了清晰的「遊戲規則」，引領業界在合法合規的基礎上挖掘數據價值，構建兼具國際視野與本土特色的數據治理體系，為跨境資本與數字產業提供可預期的制度保障。

香港個人資料私隱專員公署(PCPD)近期持續完善監管指引，推動數據治理從被動合規向主動價值創造轉型。孖士打律師行合夥人梁樂鋒在接受香港文匯報訪問時表示，PDPO附表裏的「保障資料原則」不僅劃定數據處理的監管邊界，更通過明確的技術標準為數據資產化鋪平道路。根據PDPO附表裏的「保障資料原則」中的第4原則，資料使用者須採取所有切實可行的步驟，確保其持有的個人資料受到保障，以免資料在未獲准許或意外的情況下被查閱、處理、刪除、喪失或使用。資料使用者須考慮：資料的種類及上述情況可造成的損害；儲存資料的地點；儲存設備的保安措施；確保資料查閱人具有良好操守、審慎態度及辦事能力而採取的措施；及確保資料在保安良好的情況下傳送而採取的措施。

資料保安指引涵蓋七個範疇

在數據安全領域，PCPD頒布的《資訊及通訊科技的資料保安措施指引》確立七個範疇：1.資料管治及機構性措施；2.風險評估；3.技術上及操作上的保安措施；4.資料處理者的管理；5.資料保安事故發生時的補救措施；6.監察、評估及改善；7.其他考慮，如雲端服務、自攜裝置（BYOD）及便攜式儲存裝置。「資料管治及機構性措施」被提升至戰略高度。如上所述，「切實可行」的保安措施會因應不同機構而有所不同。

倡雙重加密技術混合使用

在技術實施層面，加密技術與「雜湊」(hashing)算法的應用已成為基礎配置。梁樂鋒提出，值得注意的是真正的合規突破體現在匿名化技術的進階應用。根據PCPD最新釋義，企業宜將傳輸中和存儲中的個人資料進行加密，並妥善保管加密密鑰。企業亦可為員工安排培訓，確保他們熟習加密軟件的用法。如企業日後無需將資料的原始值或實際值還原，可考慮採用「雜湊」技術 ，以不可逆轉的數值來取代相關資料。

至於匿名化措施是否有效，在於能否令資料無法合理地與某位已識別或可識別的自然人聯繫起來。同時PCPD提出了三項準則，以評估匿名化措施是否穩健，包括：資料是否能令某人從群體中被挑出；與同一人有關的兩項資料能否聯繫在一起；以及可否從資料很大確定性地推斷出某人的未知資訊。

梁樂鋒進一步指出，儘管PDPO第33條跨境傳輸限制尚未生效，但隨着大灣區內的經濟活動漸趨頻繁，監管實踐已顯現靈活姿態。備受市場關注的《粵港澳大灣區個人資訊跨境流動標準合同》實現重要制度突破，為大灣區內地9市與香港的數據流通建立高效通道。PDPO第33條更列明，除非屬於指定的例外情況，否則資料使用者不得將個人資料轉移至香港以外的地方。然而，第33條實施，企業如要將個人資料轉移至香港境外，可先「採取所有合理的預防措施」及「作出所有應作出的努力」，以確保資料不會在接收地，以違反PDPO的方式被收集、持有、處理或使用。方法之一，是利用PCPD所擬備的「建議合約條文範本」，與資料接收者簽訂協議。

與此同時，網絡安全保險市場迎來爆發式增長。梁樂鋒認為，近年不少保險公司均推出了各種針對網絡安全威脅的保險產品，保障範圍亦漸漸擴大，包括駭客或病毒入侵、資訊保安系統故障、資料外洩或被盜、員工故意誤用資料等。企業宜根據業務需要和性質、自身資源、現行政策及措施、所使用的個人資料的種類和數量，以至安全事故可導致的損害和風險，選擇合適的保險計劃。

新條例下 資料外洩須限時通報

目前，PDPO並無強制性規定要求企業就資料外洩作出通報。梁樂鋒稱，需注意的是，《保護關鍵基礎設施（電腦系統）條例》將於2026年1月1日生效，如企業屬於條例下的「關鍵基礎設施營運者」，則須在得悉嚴重電腦系統安全事故後的12小時內，向關鍵基礎設施（電腦系統安全）專員作出通報，而其他事故的通報時限則為48小時。

在數字經濟新階段，香港正通過動態調整的監管框架，平衡數據流動與個人權益保護。香港大學法律學院數字經濟研究中心預測，隨着人工智能法案等新規醞釀，數據合規將演化為包含算法審計、倫理評估在內的全鏈條治理體系。業內共識正在形成：在完善的制度保障下，合規數據流將成為驅動創新的核心要素，香港有望藉此鞏固其作為亞太區數字經濟樞紐的戰略地位。這片法律框架規範下的數據藍海，正待有準備的航者揚帆啟程。

築起保障法網 開路數字產業爭霸

AI技術應用有法可依

香港文匯報訊（記者 蔡競文）香港PDPO並無明文規管應用於網絡安全的AI技術，但PCPD在2024年發出《人工智能(AI)：個人資料保障模範框架》，當中建議機構應建立機制，確保AI系統的運作具足夠透明度，讓終端使用者能夠解釋系統輸出的結果。框架提到，為提高透明度與公開性，機構在與員工、消費者及監管機構等持份者溝通時，應考慮採取三個步驟： (i) 除非AI系統的使用顯而易見，否則應清楚和顯著地作出披露； (ii) 提供足夠資訊，說明在相關產品或服務中使用AI系統的目的、益處、限制和效果；以及 (iii) 披露AI 系統的風險評估結果。

目前，香港透過現行的不同法規對AI進行規管。各個決策和監管機構，例如數字政策辦公室、PCPD、證監會和金管局，亦先後發出了與AI有關的指引、通函或文件。這種務實和循序漸進的方式，有助回應不同界別的需要，平衡創新與風險，確保香港保持競爭力。

梁樂鋒表示，孖士打也有為不同界別的客戶，在個人資料和網絡安全合規方面提供全方位的法律服務，包括制定和審視內部政策和應變機制、舉行模擬演習和法例講座。相關培訓可按受眾的具體需要度身訂造，涵蓋前線員工至董事會成員，確保他們在面對網絡安全事故時，能清楚了解自身的角色與責任。

保護條例明年生效 營運者需提交應急計劃

香港文匯報訊（記者 蔡競文）《保護關鍵基礎設施（電腦系統）條例》(PCI)將於2026年1月1日正式生效，指定的「關鍵基礎設施營運者」有多項責任，包括設立電腦系統安全管理單位、就電腦系統安全提交和實施管理計劃、進行風險評估及安排審核、參與演習、提交和實行應急計劃，以及就事故作出通知等。

雖然條例沒有明文提及NIST等國際標準，但規管當局可發出實務守則，就關鍵基礎設施營運者如何履行其責任提供實務指示，當中可包括標準和規格。保安局於2024年的諮詢報告中亦提到，將會參照最新科技及國際標準制定《實務守則》。

勒索軟件攻擊成最大威脅

有關供應鏈的風險管理，條例亦有所着墨。例如關鍵基礎設施營運者雖然可聘用服務提供者來設立電腦系統安全管理單位，但仍須委任一名擁有足夠專業知識的僱員監管單位。此外，營運者所提交的電腦系統安全管理計劃，亦須涵蓋有關管理供應商合約和通訊的政策及指引。

梁樂鋒指出，根據過往經驗來看，香港當前的網絡安全環境面臨的主要威脅是勒索軟件攻擊。駭客組織現一般都會使用「雙重勒索」的手法進行勒索：一方面駭客組織會使用勒索軟件對受害機構的系統進行加密，使其不能正常營運；另一方面，駭客亦會嘗試盜取機構的資料，並威脅公開敏感或機密資料以迫使受害者支付贖金。

特稿

以法律加技術構建國際數據樞紐

香港文匯報特約評論員 樺民、香港文匯報記者 悅文

在大數據的黃金時代，企業正以前所未有的速度提煉數據價值，從精準行銷、智慧金融，到供應鏈管理與風控模型，數據已成為推動經濟運作的核心元素。然而，數據應用的急速發展，也將私隱及商業機密外洩、跨境傳輸風險與網絡攻擊等問題推至前所未有的新高。若香港要成為國際數據樞紐，必須在創新與安全之間找到平衡，以法律、技術和監管共同協調，構建利於發展的大環境。

香港可擔當「合規轉運站」角色

目前，香港的監管框架主要建立在《個人資料（私隱）條例》（PDPO）之上，而將於2026年生效的《保護關鍵基礎設施（電腦系統）條例》（PCI）則補上之前尚未完善的網絡安全法則。前者規範個人資料的收集和使用，但面對AI模型、大數據演算及自動化決策的發展，原有法例難免出現滯後，特別是對自動化決策透明度、資料可攜性等數據權限尚未具體界定。後者則象徵香港正式把網絡安全提升至關鍵基建層面，透過規範化風險管理要求，加強金融、能源、交通、醫療等領域的資訊系統防護。

跨境數據流動是香港成為國際數據樞紐的核心命題。內地《數據安全法》與《個人信息保護法》（PIPL）對重要數據和個人信息出境的要求嚴格，歐盟GDPR、新加坡PDPA等制度亦日益嚴謹，使跨境傳輸涉及多重司法管轄與責任。香港的優勢在於擁有國際信任的普通法制度、透明監管及成熟的金融法治環境，能在內地與海外制度間扮演「合規轉運站」角色。但若要進一步發揮樞紐功能，香港仍需建立完善的跨境數據分類、風險評估與合規審查機制，特別是在粵港澳大灣區內建立統一的數據流通標準，形成人才、技術與制度並行的「跨境數據走廊」。

人工智能的迅速滲透亦令監管迎來新課題。無論是在金融信貸、市場監控還是公共服務分配，AI決策的透明度、公平性及可解釋性正在被各國視為核心治理項目。香港可參考歐盟《AI Act》及新加坡的AI治理框架，把目前以指引為主的做法提升至制度化層次，具體做法可包括要求企業揭示是否採用自動化決策、在高風險領域實施公平性測試、強制披露測試數據來源，以及對AI模型事故設立通報機制。如此既能保護消費者與投資者權益，也能強化香港在區內的AI合規標準制定權。

須推動加密和網絡安全技術升級

在法律之外，技術亦是數據安全的關鍵防線。若要打造世界級的數據樞紐，必須推動加密和網絡安全技術的全面升級，包括全流程數據加密、加強身份與權限管理等。金融機構和大型企業亦可利用多重加密安全計算技術，實現數據不出門的協作方式，在保持隱私與合規前提下共享模型與分析結果，這將是跨境金融數據合作的關鍵突破口。

要發展成為國際流動數據中心，香港仍需構建更完整的硬件配套，包括提升跨境光纖、海底電纜與數據中心等基建，推動綠色能源和高效冷卻技術以支撐運算需求；同時培育網絡安全工程、AI 監管、法律科技及加密專才，強化本地審查能力；並與大灣區深化制度協作，建立數據流通專區，提升跨境業務便利。