大公報社評

推廣調解文化 構建和諧社會

在中央大力支持下，香港成功爭取國際調解院總部落戶香港，成為首個總部設址於香港的政府間國際組織。特區政府積極作為，希望建成後可提升香港作為全球「調解之都」的國際形象。以此為契機，律政司將於下月6日至10日舉辦調解周及調解會議，期望進一步提高公眾在日常爭議中利用調解技巧息爭止紛的意識，推廣社會的調解文化，共建和諧社會。

小到個人，大至國家，各種矛盾、糾紛層出不窮，這也是人類社會的常態，但「法庭見」並非唯一的選擇，也未必是最好的選擇。一方面，不少糾紛發生於家人、朋友之間，一旦對簿公堂，難免「撕破臉」。就算是打贏官司的一方，往往也是得不償失。**另一方面，雖說法律面前人人平等，指的是每一個人的公民權利平等，但具體到打官司，費用高昂且曠日廢時，並非人人都「打得起」或者「耗得起」，一旦進入司法程序，對訴訟雙方都是沉重的經濟負擔和漫長的精神煎熬。**

調解，可以為爭議雙方提供雙贏的解決方案，更具經濟效益，亦能維持彼此友好關係。中國傳統文化提倡「和為貴」，打官司是最後一步，不少地方在此之前，會有調解環節，努力化干戈為玉帛，讓雙方握手言和。內地各階層近年大力推動和解，節省了大量的社會資源。在現代國際關係中，中國主張「人類命運共同體」理念，國無分大小，共建、共商、共享，用談判解決爭議。沙特和伊朗這對世仇握手言和，是中國發揮調解軟實力的最佳證明。

香港是法治社會，擁有大量法律人才以及具公信力的調解機構，與國際法律組織有着廣泛而深入的交流和合作，成為全球最受歡迎的三大仲裁地之一。**中央力挺香港發展亞太區國際法律及爭議解決服務中心，並支持國際調解院將總部設在香港，體現了中央對香港的高度信賴，也是香港發揮自己之所長、貢獻國家之所需的應有之義。**

特區政府高度重視推廣調解文化。在去年發表的施政報告中，行政長官李家超就致力「深化調解文化」提出一系列措施，包括完善香港調解專業的認證和紀律事宜的制度，在政府合約中加入通用的調解條款，並鼓勵私人機構採用相同的做法。律政司每年舉辦一系列相關活動，不少活動是面向青少年，鼓勵他們建立正面及具建設性的排解爭議價值觀。這些活動包括舉辦校園調解研討會及相關比賽。在日前舉行的第七屆香港中學朋輩調解比賽中，爭議雙方有公平的機會表達自己的意見，由中立的朋輩扮演調解員角色，了解彼此訴求，排除雙方情緒，促成雙方找到共通點，進而尋求解決方法。

青年是香港的未來，要讓調解文化深入社會，最好由青年做起。通過特區政府舉辦的這些調解活動，年輕人可以深入了解調解作為日常生活技巧，學會易地而處，換位思維。**當面對與自己不同的見解時，多一份尊重和理解，多一份換位思考，就有機會化解爭議，促進學校、家庭和社會之間的互信和合作關係，也有助於年輕人走出校門後，可以更好地維繫人際關係，發展個人事業。**

在剛過去的復活節期間，大批港人北上消費，引起社會熱議。其實，隨着大灣區建設日新月異，兩地人員往來、商貿合作愈加密切，同時意味着爭議糾紛的增加，對法律調解的需求上升。有見及此，粵港澳三地法律部門組成粵港澳大灣區調解工作委員會。日前，特區政府公布大灣區調解員資歷評審細則，這標誌着共建大灣區又向前邁出一大步，也有助於進一步鞏固香港國際「調解之都」的地位。

井水集

裝好網絡安全鎖

去年8月，數碼港遭黑客組織入侵、勒索並「撕票」，受害者達13000人。7個月後，私隱專員公署發表調查報告，裁定數碼港違反《私隱條例》有關個人資料保安和保留的規定，向數碼港發出執行通知，要求2個月內提交文件證明已完成工作。這一裁決，也為全港敲響警鐘。

私隱專員公署力數數碼港犯下的5個過錯，包括資訊系統欠缺有效偵測措施、未有為遠端存取資料啟用多重認證功能、對資訊系統進行的保安審計不足、資訊保安政策有欠具體，以及個人資料被不必要的保留等。

數碼港是一家具規模的企業，但令人咋舌的是，黑客長驅直入，數碼港多日後才驚覺，足證其網絡保安系統存嚴重漏洞；又如，按照有關規定，求職者的個人資料保留時間最長為一年，僱員離職後就要立即刪除其個人資料，但數碼港違規保留逾5000名前僱員及求職者的資料，最長的為7年，結果私隱全曝光。

蒼蠅不叮無縫的蛋！數碼港輕易遭到黑客入侵，癥結在於嚴重的人為疏忽。事實上，數碼港事件並非孤案，這些年來，類似事件不時發生，顯示香港在網絡保安方面仍有很大的提升空間。

進一步追問，黑客組織為何盯上了數碼港，難道僅僅是為了勒索贖金嗎？事件未必這麼簡單。眾所周知，黑客組織往往不是一般的犯罪團夥，幕後有更龐大的勢力支持。中國國家安全部、國家電腦病毒應急中心都曾發表報告，揭露美國利用其技術優勢，肆無忌憚地對其他國家進行秘密監控，並把網絡攻擊武器化，頻頻發動網絡戰爭，成為危害網絡安全的最大黑手，是名副其實的「黑客帝國」。

中國是美國網絡攻擊的主要目標，香港首當其衝。所以說，網絡安全是國家安全的重要一環。行政長官李家超早前以建立有效門鎖防止「爆竊」來解釋基本法第23條立法。同理，在網絡安全方面，香港上下也要盡快安裝有效門鎖，令竊賊無機可乘。

數碼港五大缺失 洩1.3萬人資料

缺有效措施防黑客 私隱署限兩月內糾正

數碼港去年八月遭黑客組織Trigona入侵，逾1.3萬人、共超過400GB個人資料外洩，當中約四成爲求職者及已離職僱員。私隱專員公署昨日公布數碼港資料外洩事故的調查報告，裁定事件違反《私隱條例》，指示數碼港兩個月內糾正。

私隱專員鍾麗玲指出，事故由五項缺失導致，包括資訊系統欠缺有效偵測措施，只依賴一款反惡意軟件令黑客成功獲取具管理員權限賬戶憑證，並進行勒索軟件攻擊及竊取儲存個人資料；對資訊系統進行的保安審計不足，每兩年才做一次；個人資料被不必要地逾期保留等。

大公報記者　古倬勳、葉浩源

▲私隱專員公署公布數碼港去年8月資料外洩事故的調查報告，指事件涉及資訊系統的五大缺失。

►數碼港1.3萬名職員及求職者的個人資料於去年外洩。

近年黑客攻擊事件

2024年3月17日	南華體育會電腦伺服器遭未經授權的第三方入侵，會方已報警並立即採取應對措施，關閉受影響的電腦設備，以保護會員的個人資料安全。受影響人士可能涉及約7萬人。
2024年1月30日	港大教育學院電腦伺服器遭受網絡攻擊，校方發現後即時確保伺服器連結中斷，課室預約紀錄、內部指引、系統管理文件等學院內部文件或已外洩，涉及約400名訪問學者、3000名學生的學習進度及4000名研究生申請人摘要。
2023年9月26日	香港桂冠論壇電腦系統遭黑客以勒索軟件惡意入侵，導致大規模系統受到破壞，令日常工作受到影響，黑客在勒索訊息中並無提出贖金，只要求論壇委員會24小時內與他們聯絡，並按指示購買比特幣，受事件影響的資料包括日常工作文件及個人資料，約550人姓名及電郵地址外洩。
2023年9月20日	消委會電腦系統遭黑客勒索軟件入侵，涉及投訴人、員工、前員工及求職者等個人資料，黑客要求消委會23日晚上11時20分前繳交50萬美元贖金，若遲於該時間則要交70萬美元，消委會稱絕對不會繳交贖金，並會全力配合警方的調查工作。
2023年8月中	數碼港發現部分電腦檔案被鎖上，遭未經授權的第三方入侵數碼港的電腦系統，黑客持有超過400GB數碼港的資料，包括初創公司職員的身份證明文件、公司文件、照片等，並要求數碼港就資料繳付30萬美元。

大公報記者整理

八年前資料至今未銷毀

私隱專員公署公布數碼港去年8月資料外洩事故的調查報告，發現逾1.3萬名員工和求職者的個人資料洩漏，包括逾5000名求職者的個人資料，部分超過法例容許的保留期限，有最早2016年保存至今的應銷毀但未銷毀資料，涉及的個人資料包括姓名、身份證號碼及副本、護照號碼，亦有部分人士的財務資料，例如銀行戶口號碼、醫療報告、照片、僱傭資料等。據了解，在「暗網」遭黑客外洩的資料包括數碼港行政總裁任景信、首席營運官鄭希穎、首席公眾使命官陳思源、首席投資官陳覺忠、項目總監余達彰，共五名高層的身份證號碼、薪金、銀行賬戶號碼、住址及電話號碼等個人資料。

私隱專員鍾麗玲指出，事故由五項缺失導致，包括資訊系統欠缺有效偵測措施，只依賴一款反惡意軟件令黑客成功獲取具管理員權限賬戶憑證，並進行勒索軟件攻擊及竊取儲存個人資料；亦無為遠端存取資料啟用多重認證功能，核實獲授權可遠端登入數碼港網絡的用戶身份；亦對資訊系統進行的保安審計不足，每兩年才做一次，事發前審計已於2021年底進行，相隔逾19個月，未能適時應對資訊科技變化和網絡安全風險。除此之外，數碼港資訊保安政策有欠具體，未能讓員工有具體網絡保安框架可依循；個人資料亦被不必要地保留，公署曾就逾期保留資料向數碼港查問原因，但數碼港未能解釋。

數碼港：定期檢視保安措施

鍾麗玲認為，數碼港是一間具規模的機構，恆常持有並處理大量不同人士的個人資料，持份者和公眾會合理期望數碼港投入足夠資源確保系統和數據安全，因此應採取足夠保安措施。私隱專員已在上月26日向數碼港送達執行通知，指示兩個月內，即5月26日前糾正違反事項，之後向公署提交證據，又指如果再次違規將是刑事罪行。她又建議公司設立個人資料私隱管理系統，並委任保障資料主任，適時對系統進行風險評估，及適時刪除個人資料，防止類似違規再次發生。

數碼港回應私隱專員公署調查報告表示，董事局早前已就事件成立專責小組完成督導調查及跟進，包括鞏固網絡防護屏障，強化偵測網絡攻擊及入侵的能力，並成功堵截後續網絡攻擊，亦委託第三方定期監測網絡安全及道德黑客入侵測試，以及增加監察網絡安全的工具等。專責小組的調查發現，數碼港在內部資訊保安及數據管理方面存在改善空間，數碼港已加強多項措施，持續提升各個營運層面的資訊系統保安及數據安全水平和意識；同時已審視並加強有關個人資料管理的措施，以確保完全符合《個人資料（私隱）條例》訂明的個人資料保障原則。

數碼港董事、網絡安全事件專責小組主席伍志強表示，自事件發生以來，專責小組與管理層積極審視及即時跟進，快速增強網絡及數據防護屏障，有效防範後續的網絡入侵攻擊，並致力支援受影響人士，盡力減低潛在影響，以及全面配合有關部門與私隱專員公署的調查。數碼港亦會加強內部審查，定期檢視執行資訊保安措施的情況，並向董事局轄下的審計委員會匯報，提升相關管治水平。

分類儲存數據 減少洩密規模

專家之言

香港智慧城市聯盟資訊科技管治委員會主席龐博文表示，十分認同私隱專員公署對數碼港資料外洩事故的調查報告。他說，數碼港涉及外洩很久以前的資料，如果未必有保存的需要，而沒有把數據適時刪除，這種漏洞也是過往國際上出現重大資料外洩事故的共通點。

加密數據增盜用難度

就數碼港的事件，外洩的資料新與舊的都有，而且是跨部門，可見沒有做好數據分類，龐博文指出正確的做法應是將新與舊的資料分開儲存，加上有些部門毋須用上舊資料，所以亦應分部門儲存，而非「大雜燴」，即使被入侵，外洩的資料範圍也能受限。

龐博文說，數碼港的事故最嚴重的問題是，沒有發現何時、為何及是誰攻擊，即沒有做好安全監控，是很明顯的漏洞。他續指，事實上很多企業都未有做好安全監控方面，基於貪圖使用數據時的方便，或加重成本負擔等原因。

他建議企業要做好安全監控，最簡單直接亦最應該做的是將數據加密，不要「等別人要取數據時才由他來加密，而應該是在別人取出之前自己已先加密」。他解釋，一旦黑客入侵見到的是一堆已加密的數據，得物無所用或需耗費人力物力解密，自然減低盜用意圖。

大公報記者葉浩源

數碼港形象受損

透視鏡

蔡樹文

個人資料私隱專員公署（私隱專員公署）完成對香港數碼港管理有限公司（數碼港）資料外洩事故的調查，個人資料私隱專員鍾麗玲指出，資料外洩事故存在五項漏洞。數碼港在資料外洩事故發生前，未有採取足夠及有效的措施以保障其資訊系統的安全，亦未有及時根據其資料保留政策刪除已屆保存期限的資料。

數碼港是香港數碼科技的推動者之一，理論上，數碼港的系統設計和管理應該是最先進、最嚴謹。然而，資料外洩事故暴露出數碼港在防範黑客入侵方面嚴重缺憾，讓數碼港的形象受到傷害。

互聯網科技日新月異，「道高一尺，魔高一丈」，黑客的技術手段同樣與時俱進。我們要對數碼港資料外洩事故舉一反三，特別是政府、半官方機構、公共事業機構、金融系統等，在防範黑客入侵的系統設計和管理上，必須保持最高戒備狀態。

今天，網絡世界與現實世界同樣不太平，維護網絡安全，防範黑客入侵，是維護國家安全重要組成部分，絕不能掉以輕心。