社論

提升對政府統計機敏資料的保護意識與作爲

豐沛的數據，加上突飛猛進的科技，提供了對資料進行更多創新運用的機會與期待，不過，更多的訊息與更好的技術也隱藏了許多的危機與傷害。就政府統計而言，這些危機或傷害可能來自兩方面，首先是資訊網絡若受到破壞，政府統計的運作或服務提供可能停擺或產生錯誤資訊；其次是在統計資料之蒐集、保管、處理、利用及發布的各階段中，造成機敏資料的外漏，二者都會造成政府統計公信力的流失，須愼防這些狀況發生。

在整體網路或資訊安全防護方面，行政院國家資通安全會報於 2001 年起即陸續推動 6 個階段，各階段分別進行爲期 4 年之重大資通安全計畫或方案，俾不斷提升資安防護能量與優勢。目前進行的第六期（2021 年至 2024 年）發展方案以「打造堅韌安全之智慧國家」爲願景，從「吸納全球高階人才、培植自主創研能量」、「推動公私協同治理、提升關鍵設施韌性」、「善用智慧前瞻科技、主動抵禦潛在威脅」及「建構安全智慧聯網、提升民間防護能量」等 4 個面向強化國內資安。

根據數位發展部國家資通安全情勢報告，政府機關通報的資安事件由 2020 年的 505 件增至 2022 年之 765 件，其中以「非法入侵」爲大宗，設備異常或毀損、弱密碼或密碼遭暴力破解及網站設計不當等問題爲資安通報主要原因。通報件數增加可能表示各機關通報意識提高，但也顯示在軟、硬體及人員資安素養雖已努力提升，資安威脅仍防不勝防，防護意識與作爲不可稍有鬆懈。

在政府統計辦理過程中機敏資料運用及保護方面，爲充分利用公務資料及減輕受查者負擔，我國統計法已有將業務單位行政資料處理系統納入統計需求，以及跨機關索取資料機制之規範，俾利增進機關間資料串連應用，發揮政府統計最大效用，惟資安威脅日益嚴峻，隱私防護不斷升級，政府機關間資料交流困難度也隨之提高。

聯合國爲兼顧安全處理及共享政府統計機敏資料，於 2023 年提出《強化隱私保護技術指南》（Privacy-Enhancing Technologies Guide），將政府統計作業中涉及的機敏資料保護概分爲兩部分，其一是在處理、分析或跨機關運用時避免個資的揭露；其二爲發布的統計結果避免被識別出機敏資料，並爲強化保護隱私資料，提供多項具體做法。許多國家統計局（National Statistics Office, NSO）與政府機構正嘗試利用這些資料處理技術，在隱私獲得保護的前提下，擴大及深化其統計資料應用範圍。

以美國爲例，普查局每 10 年調查一次每個州的總人口數，調查結果會用來決定各州的國會席次、選區邊界以及數十億美元的聯邦資金分配，而該調查統計數據之發布必須遵守 1974 年公布的《隱私權法》對公民資訊與身分的保護規定。隨大數據重新識別技術的發展，美國人口普查發布的統計數據因隱含機敏訊息而備受挑戰，2020 年美國人口普查採用差分隱私（Differential Privacy）技術，即在資料中注入適當的雜訊（noise），使外界無法從統計特徵反推個資，以兼顧隱私權保護與資料的可用性。

加拿大統計局則是運用合成資料（Synthetic Data）技術，將人口普查、死亡登記、癌症登記等資料集模擬產生人工合成數據取代原始資料，經過兩次黑客松活動的測試，充分驗證合成資料技術不但可保留原始數據的分析效用，同時有效降低披露個資風險。

歐盟統計局爲了對 NSO 的資安與共享資料問題提供解方，與技術商合作開發可信執行環境（Trusted Execution Environments）做爲示範案例，將硬體隔離並結合隱私增強的軟體，在模擬多達 1 億多筆的行動網路業者用戶合成資料上進行測試，成功驗證可信執行環境可讓 NSO 更安全、自信地分析數據。

南韓統計局亦積極推動建立公共大數據系統，嘗試介接各政府機構間的人口、家庭及機關團體等公務登記資料，從而將數據的潛在價值發揮至極大化。爲了達到上述目標，南韓統計局與科學技術資訊通信部於 2021 年至 2024 年間合作建置統計數據中心平臺，利用同態加密（Homomorphic Encryption）、差分隱私及合成資料等先進的加密技術，讓政府資料安全介接與使用。

聯合國指南中建議的方法還有安全多方計算（Secure Multi-Party Computation）、分散式學習（Distributed Learning）、零知識證明（Zero Knowledge Proofs）等，可就不同的資料及運用狀況選擇適當方法。

除了整體資訊網絡與政府統計作業各階段之安全防護外，跨機關或領域資料傳輸的安全性也是隱私保護重要的一環。數位發展部預計於 2024 年底將掌有全國人民個資的 47 個資安 A 級機關全數導入政府資料傳輸平臺（T-Road）與零信任架構（Zero Trust Architecture），其中 T-Road 是在原有的政府網際服務網（Government Service Network, GSN）中，規劃設立跨機關資料傳輸專屬通道，像是一條加密專線，傳輸過程以電子憑證全程加密；在零信任架構部分，概念上爲「永不信任，持續驗證」，即系統對個人指紋、設備、連線行爲是否異常等 3 方面進行確認。T-Road 提供了滴水不漏的安全通道，「零信任」則補足了嚴密的守門機制，有助降低資料洩漏風險。

隨數位化轉型腳步加速，資安威脅的攻擊性、複雜度與破壞力也持續進化，對於以蒐集、整理、分析資料的政府統計工作者來說，既要提升政府統計效用，又要滿足個資防護要求，除可借鏡國際使用保護隱私技術的經驗外，亦須落實各項資安防護措施，時時保持警覺，讓政府統計在機敏資料安全無虞下，得到最好的應用。❖