

個人隱私資料保護機制為各國積極推動之首要工作，我國「個資法」修正完成立法後，必能發揮立竿見影之效果

探究個人隱私資料保護之道

◎ 盧玲朱

壹、前言

有鑒於我國政府機關及民間企業近年來不斷傳出個人隱私資料外洩情事，讓民眾甚為困擾，為保障民眾個人隱私資料，立法院於去(97)年7月7日由15位立法委員聯名建請政府參考日本的現行作法，推動我國公、民營機構「隱私權管理保護」認證制度，法務部也立即邀請政府及民間企業共同討論此一議題，並研究如何推動我國公、民營機構「隱私權管理保護」的認證制度。

英國「隱私國際」與美國「電子隱私資訊中心」於2007年公布國際隱私權評比，第一次被評比的臺灣在隱私保護推動、身分辨識機制及通訊遭竊部分成績均列最後，值得重視。顯見我國在推動個人資料保護方面，仍有許多努力的空間。

貳、國際發展趨勢

個人隱私資料保護之國際趨勢及現況，在亞太經濟組織已針對個人隱私成立「隱私權開路者計畫」，日本則積極推動「隱私權標章制度」，中國大陸大連市大連軟體行業協會亦發行「個人資訊保護評價(Personal Information Protection Assessment, 簡稱PIPA)認證，並與日本「隱私權標章(Privacy Mark, 簡稱P-Mark)」及美國「線上隱私權標章認證(BBBonline)」交互認證，顯見個人隱私資料保護之機制已成為各國積極推動之首要工作。

國際組織間如經濟合作暨發展組織(OECD)、歐盟(EU)及亞太經濟合作組織(APEC)等，均通過相關法令等措施，來處理國際間電子商務行為涉及個人隱私資料保護及網路傳輸等問題。以下針對3個主要的國際組織，說明個人隱私資料保護的相關作法。

一、經濟合作暨發展組織

經濟合作暨發展組織(OECD)於1980年針對個人資料保護制訂8大原則，包含限制蒐集原則、品質確保原則、目的明確原則、限制目的外使用原則、安全確保原則、公開原則、個人參與的原則、責任明確原則，以作為會員國推動個人隱私資料保護之參考原則。

二、歐盟

歐盟(EU)對網際網路應用及電子商務環境所引發之個人隱私權利保護有相關立法及推動機制。1980年歐洲議會訂定「保護自動化處理個人資料公約」，並於次年要求所有會員國共同簽署。該公約已於1985年10月1日正式生效，為世界第一個關於隱私權保護並具拘束力之國際公約。並於1995年10月24日通過個人資料保護指令，要求會員國於同年月24日前依據該指令，立法管理個人資料。

三、亞太經濟合作組織

亞太經濟合作組織(APEC)參考經濟合作暨發展組織(OECD)的隱私保護及個人資料國際傳輸指導方針，於 2004 年制訂亞太經濟合作組織隱私保護綱領(APEC Privacy Framework)，做為提升各國隱私保護之重要推動方針，並確保亞太地區各會員國間資訊自由流動，俾符合隱私保護綱領之規範原則。

參、我國發展趨勢

我國「電腦處理個人資料保護法」（簡稱「個資法」）因時代變遷，已經諸多不宜，也逐漸產生許多問題，在管理層面及稽核層面也都缺乏足夠的配套措施。有鑒於此，我國目前正進行修法中，未來在法律層面完整性的問題將與各先進國家相差不多，惟關於「專責之推動機構」及「隱私權管理保護稽核制度」兩個部分尚未著墨。以下針對我國於個人資料保護之法律面、管理面及稽核面作相關說明：

一、法律面：

法務部早於民國 90 年即開始擬定「電腦處理個人資料保護法」的修法計畫，積極推動研修個資法工作。修法內容重點包括擴大保護客體、普遍適用主體、增修行為規範、強化行政監督、促進民眾參與、妥適調整罰責及配合增修條文，現行法之諸多缺失與漏洞均已作適度之改進。「電腦處理個人資料保護法」修正內容已於 97 年 02 月 15 日函送立法院，但尚待完成立法。本次修法如能順利完成立法程序並公布施行，相信對國內個人資料隱私權益之保護，必能發揮立竿見影之效果。

二、管理面：

國內電腦處理個人資料保護法第 25 條規範「目的事業主管機關，認有必要時，得派員攜帶證明文件，對於應受其許可或登記之非公務機關，就本法規定之相關事項命其提供有關資料或為其他必要之配合措施，並得進入檢查。經發現有違反本法規定之資料，得扣押之。對於前項之命令、檢查或扣押，非公務機關不得規避、妨礙或拒絕。」因此各目的事業主管機關對其下轄非公務機關具有檢查稽核之責任，但因無相關標準、規範、指引或行政指導配套措施，致使無法落實。又公務機關為蒐集、處理與利用個人資料的主要單位，但目前國內並無個人資料保護的專責推動機構，因此無法具有顯著之推動成效。

三、稽核面：

目前個人資料保護法修正條文中並未針對公務機關說明稽核之規範及機制，然行政院主計處於年度機關(構)資安外部稽核服務，已將個人資料管理納入稽核重點項目，並請各機關(構)辦理資安內稽時亦將個人資料管理納入內稽重點，適時宣導所屬有關上揭個資法公務機關應負管理之規定。期能確保個人資料保護之管理作為，落實於各政府機關(構)中。

肆、結語

我國雖於民國 84 年即訂定「電腦處理個人資料保護法」，但由於未指定主管機關，相關之配套措施也尚未推動，所以如臺中市胡志強市長之健康情形遭不當揭露及飛官上網機密報告全被駭之情形仍屢見不鮮。

為有效落實個人資料的保護作業，我國可參照日本訂定階梯式的法制體系，除制定個人隱私保護法律外再配合頒布政令，即行政命令、基本方針及參考指南，其中參考指南部分還針對產業別之不同，訂定 37 套各產業適用之參考指南，以利各個產業於推動個人資料保護時，能依照不同之產業作業特性，執行最大之防護效能。

此外，我國目前公務機關皆已經設立資訊安全長(Chief of Security Officer，簡稱 CISO)職位，負責及執行單位內資訊安全管理之業務，為各政府機關(構)資訊安全的最高主管。個人隱私資料保護應屬資訊安全的一部分，公務機關可將資訊安

全長及隱私長合而為一，單位內之資訊安全長除了資訊安全業務執掌外，亦可兼負個人隱私資料保護之業務，並請參研本單元續篇「個人隱私資料實務建議」所提之作法，以控制領域、管控目標及控制要項之執行架構，落實個人資料保護管理程序基本要素之實務作法，同時效法日本推動隱私權標章制度，必能收到事半功倍之成效。

（作者任職國家資通安全會報技術服務中心）