僅供委員問政所需參考
不代表本院意見或立場

編號：2453

議題研析

一、 題目：詐欺犯罪防制議題—業者個資安全維護義務之法制研析

二、 議題所涉法規

詐欺犯罪防制條例草案[1]（行政院研擬中）

三、 背景說明

依內政部 113[2]年 3 月 14 日於本院第 11 屆第 1 會期司法及法制委員會「詐欺犯罪防制立法及各部會打詐機制盤點」公聽會報告，該部刻正研擬打詐專法，規劃電信面、網路面、金融面及懲詐面等 4 大面向，內容包括賦予電信業者就疑似詐欺犯罪號碼停止服務之法源、律定業者防詐責任、強化金融機構防詐及納管個人幣商與提高詐騙刑責等[3]。據民間團體與內政部警政署刑事警察局共同調查顯示，臺灣、泰國、馬來西亞個資外洩類型前三大為登入密碼、電話號碼、姓名，臺灣電話號碼外洩率達 65%，掌握個人資料為詐騙手法之第一步[4]，因此，打擊詐欺亦應由強化業者之個資安全維護責任以防止個資外洩著手，惟依上開公聽會報告，打詐專法似僅規劃納

[1] 立法院議事暨公報資訊網站，行政院打擊詐欺辦公室「詐欺犯罪防制立法及各部會打詐機制盤點」公聽會書面資料，113 年 3 月 14 日，網址：https://ppg.ly.gov.tw/ppg/SittingAttachment/download/2024030618/PPGB60500_4300_20769_1130313_0003.pdf，最後瀏覽日期：113 年 4 月 25 日。

[2] 本報告有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[3] 立法院議事暨公報資訊網站，內政部「詐欺犯罪防制立法及各部會打詐機制盤點」公聽會報告，https://ppg.ly.gov.tw/ppg/SittingAttachment/download/2024030618/09105103231451200002.pdf，頁 1-3，最後瀏覽日期：113 年 4 月 25 日。

[4] Gogolook 2022 年度詐騙報告：個資外洩篇，網址：https://gogolook.com/zh-hant/news/gogolook-fraud-report-2022-info-leak，最後瀏覽日期：113 年 4 月 23 日。

入個資保存期限相關規範，業者防詐責任是否包括針對特定業別或一定規模以上業者，就個資安全維護措施為一定程度之要求等未臻明確，爰擬就業者個資安全維護義務與詐欺犯罪防制相關議題進行研析。

四、 探討研析

（一）個人資料保護法就業者應採取之個資安全維護措施並無強行規定

依個人資料保護法（下稱個資法）第 27 條[5]及同法施行細則第 12 條[6]規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，而該「適當之安全措施」係指防止發生上述個資侵害事故之技術上及組織上措施，上開施行細則第 12 條所例示之 11 款得採取之措施，係由該機關以與所欲達成之個人資料保護目的間，具有適當比例為原則衡量，該條立法說明並指出可考量組織規模與保有個人資料之數量或內容[7]。惟論者認，我國個資法之資安法制仍停留在早期電腦作業系統操作思維，施行細則雖例示得包含之安全維護措施，但欠缺具體規範，難以實際操作[8]。此外，保有個人資料之業者雖須採取適當安全維護措施，以防止發生個資事故，惟該安全維護措施應具備之事項，依個資法第 27

[5] 個資法第 27 條規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第 1 項) 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。(第 2 項)前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。(第 3 項)」

[6] 個資法施行細則第 12 條規定：「本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。（第 1 項）前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。（第 2 項）」

[7] 參見個資法施行細則第 12 條之立法說明。

[8] 張志偉，個資保護與資料安全，當代法律，第 22 期，112 年 10 月，頁 16-17。

條第 2 項規定指定，中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法（下稱安維辦法），惟未經指定或未適用安維辦法之業者應採行哪些安全維護措施並無強行規定。

（二）個資法適用對象多元，倘全面提升安全維護義務，須評估對個人及微中小型企業造成嚴重衝擊影響

我國個資法係為公務及非公務機關建構有關個資保護之基本規範，就個資之合法蒐集、處理、利用為一般性框架，其性質為普通法[9]，且適用該法之公務機關包括依法行使公權力之中央、地方機關或行政法人，而除前開所稱公務機關以外之自然人、法人或其他團體，皆屬個資法所稱之非公務機關[10]，因該法規範對象類型廣且多元，倘為一致性之強化監管，將大幅提高法遵成本，並加重個人及微中小型企業之負擔；又倘以所蒐集、處理、利用個資之目的、數量、企業規模等為差異化規範，亦將使作為普通法位階之個資法過於龐雜，進而產生適用疑義。有必要就提升安全維護義務之對象與類型，進行可能衝擊影響評估，以確認強化監管的對象類型。

（三）歐盟透過網路安全法規要求業者提升資安，以防止網路攻擊

歐盟一般資料保護規則（General Data Protection Regulation, GDPR）針對個資安全維護措施似採取與我國個資法類似規範模式[11]；惟查歐盟於 2016 年公布之網路與資訊系統安全指令（Directive on Security of Network and Information Systems, 第 1 版 NIS 指令），業

[9] 國家發展委員會 110 年 1 月 8 日發法字第 1102000017 號函回復司法院秘書長有關大法官審理會台字第 13769 號蔡季勳等人聲請解釋案，參自憲法法庭 111 年憲判字第 13 號【健保資料庫案】其他相關資料，網址：https://cons.judicial.gov.tw/docdata.aspx?fid=38&id=309956，最後瀏覽日期：113 年 4 月 26 日。

[10] 參個資法第 2 條第 7 款及第 8 款規定。

[11] 歐盟一般資料保護規則（General Data Protection Regulation, GDPR）於第 32 條規定控管者與處理者應採取與風險相當之技術上及組織上之適當安全措施，該措施包括但不限於假名化與加密、確保系統及服務持續、及時回復資料可用性及定期評估相關措施之有效性等。

將歐盟關鍵基礎服務運營商與數位服務提供者納入規範[12]，前者係指提供能源、交通、銀行和衛生等特定基礎服務之公私部門，後者主要指提供網路市集、搜尋引擎和雲端服務之企業[13]；為因應網路科技與數位經濟快速發展所產生之大量網路攻擊及網路安全威脅，歐盟以第1版NIS指令為基礎再於2023年公布「歐盟高通用程度資安措施指令」（Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union,第2版NIS指令），除強化提供社交網路平台與資料中心等相關數位服務中大型企業之監管外，並提出更完整之資安風險管理措施，包括資安事件通報與危機管理、密碼之有效使用與解決供應鏈資安風險等。2022 年提出之資安韌性法草案（Cybersecurity Resilience Act）規範對象更包括所有進入歐盟市場之智慧聯網（IoT）設備，除以風險等級訂定不同資安要求外，關鍵產品更應取得相對應之安全檢測與驗證標章[14]。

（四）我國資通安全管理法規僅適用公務機關及特定非公務機關

歐盟針對數位服務業者之資安已透過相關 NIS 指令為一定要求，而我國資通安全管理法僅適用於公務機關及特定非公務機關[15]，一般提供數位服務之企業多不屬此範圍，因此，除個資法及安維辦法外，針對數位服務業者似已別無其他資安、個資安全維護法遵規範。查106年行政院提出之資通安全管理法（下稱資安法）草案，原於第16條規定關鍵基礎設施提供者以外之非公務機關應作為事項[16]，引發是

[12] 施弘文，歐盟通過網路與資訊系統安全指令，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=7531，最後瀏覽日期：113年5月1日。

[13] 余啟民，從歐美資安法制發展淺析我國資通安全管理法修法草案，電腦稽核期刊，第29期，113年2月，頁44-45。

[14] 余啟民，同前註，頁45-46。

[15] 資通安全管理法第3條第6款規定：「本法用詞，定義如下：…六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」，同法第16條第1項規定：「中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。」。

[16] 行政院106年4月28日院臺護字第1060172497號函本院審議之資通安全管理法草案第16條第1項規定略以：「關鍵基礎設施提供者以外之非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」，網址：https://lis.ly.gov.tw/lygazettec/mtcdoc?PD090313:

否應納管非公務機關之爭議[17]，嗣後於本院審議時，將該條規定適用範圍限縮至「關鍵基礎設施提供者以外之『特定』非公務機關」[18]，倘透過資安法之修正再度擴大納管非公務機關，前述曾引發之相關爭議亦有待納入修法之評估。

（五）研析與建議

完善之企業資安防護與個資保護措施，與防止詐欺間具有密不可分之關係，倘考量透過個資法與資安法全面強化業者安全維護義務或提升資安要求，將對微中小型業者造成某種程度衝擊，可能影響其營運成本或加重資源配置負擔，惟可評估將相關強化企業資安與個資保護之措施納入打詐專法規範中，例如針對保有或處理大量個資之數位服務提供者等對象強化監管措施、提升資安要求與個資安全維護義務等，以減少詐騙集團利用業者保有之個資進行詐騙之可能性。

撰稿人：陳育靖

LCEWA01_090313_00155，最後瀏覽日期：113 年 5 月 1 日。

[17] 劉靜怡、徐彪豪，行政院版資通安全管理法草案評析，月旦法學雜誌，第 272 期，107 年 1 月，頁 123。

[18] 資通安全管理法第 17 條。