「資通安全法律案例宣導彙編」

第八輯

行政院國家資通安全會報技術服務中心編印
中華民國99年12月

序

行政院已將雲端技術作為未來政府與產業發展之「軟實力」政策，將整體社會生活推向新的境界，例如社群網站打破傳統溝通的有形疆界，讓民眾可以透過網路隨時了解政府政策與親朋好友之動態。然而，在新型態與便利的資訊運用活躍之同時，資訊安全議題仍不斷衍生。資訊活動所設計的功能，讓公務機關、非公務機關及民眾日常生活的互動，都可能在資訊交換之同時而產生不斷循環的風險。若使用者未注意資訊流通與串流服務所造成的資訊風險時，其一舉一動將輕易被不特定人讀取或無法保護其隱私權。將資料應用在雲端系統上，如何確保資料完整性與機密性，亦將是政府應用雲端系統必須注意的資訊安全議題。此外，立法院於 *99* 年 *4* 月 *27* 日三讀通過個人資料保護法，未來所有公務機關、非公務機關及個人如何因應個人資料保護法之規定，將是資訊安全不可迴避的重要議題。

「行政院國家資通安全會報技術服務中心」（以下簡稱技服中心）受行政院研究發展考核委員會之委託，自 *91* 年起已發行 *7* 輯「資通安全法律案例彙編」。此彙編透過對相關案例的分析與學習，幫助政府部門與社會大眾建立網路環境應有的法治概念與安全意識，進而達成預防網路犯罪之目標。在「技服中心」舉辦的各類資安宣導與推廣訓練活動中，此彙編之推廣發行普獲好評，政府機關(構)爭相索取運用，使「技服中心」深感持續推動此項工作之重要性。此次 *100* 年編印之第八輯「資通安全法律案例彙編」，持續委由「國巨律師事務所」蒐集近一年來發生之資安時事新聞與法院實際案例。內容除保持深入淺出的說明與專業法律觀點外，亦提供資訊安全管理指標 *CNS27001*(資訊安全管理系統)之具體管理措施建議，提供案例中各角色(如：公務機關、非公務機關及民眾等)法律面與管理面的建議，增加對讀者的參考價值，並期待此彙編能成為學習與管理資訊安全時最佳參考教材之一。

行政院國家資通安全會報技術服務中心

劉培文主任 謹識

編者序

「行政院研究發展考核委員會」(以下簡稱「行政院研考會」)以及「行政院國家資通安全會報技術服務中心」(以下簡稱「技服中心」),為推動政府與民間企業的資安意識,不遺餘力。

同時,感謝行政院研考會以及技服中心的放心,能夠讓本所將選輯個案相關的資訊安全法律與資訊安全管理議題有整合呈現的風貌,希冀此一方式能提供政府單位與企業有一參考作業基準,進而作為檢視單位內外資訊安全管理或教育訓練之參考資料。此外,有關本輯資訊安全管理之「管理 *Tips*」,特別商請資誠企業管理顧問股份有限公司蔡興樺協理協助提供資訊,並為致謝。

第八輯除延續第七輯之作業模式外,在擷取新聞議題時間是以民國(以下同)*99* 年 *1* 月到 *12* 月為主。斯時,資訊安全議題上最關注的議題莫過於是「個人資料保護法」(新版個資法)之立法通過。同時,因為現行有效的法律仍然是「電腦處理個人資料保護法」(以下簡稱「現行法」),以致於在 *99* 年與 *100* 年間,新版個資法尚未正式施行之際,有關本輯個資議題的呈現即有現行法與新版個資法之對應說明。此一差異,為本輯有關「資訊保護」類中「電腦處理個人資料保護法」之特殊性,還請讀者注意。

在「資訊公開」類,主要以「檔案法」為介紹案例。「資訊監察」類還是以「通訊保障及監察法」為對象。有關「資訊應用」類,則以電子化政府應用以及電子發票為主,並輔以手持式行動裝置應用時可以參考的相關法律與管理規範。

整體案例分布,仍以「資訊保護」佔大宗,有 *23* 則案例。「資訊公開」則為 *1* 則。「資訊監察」*2* 則與「資訊應用」*4* 則。以上案例共計 *30* 則。

以「軟實力」厚植國內產業根基以及運用雲端運算強化政府服務為未來幾年政府之施政目標。可以預見的是,資訊串流與雲端運算已然成為顯學。值此,對於資訊安全議題的重視,必然可為堅固「軟實力」之基石,並為資訊安全挹注產業成長動能,而得發揮電子化政府領頭羊之角色。

國巨律師事務所

朱瑞陽律師 謹識

凡　例

壹、本案例彙編分為以下類別：

一、資訊保護 *(Security)*

01 電腦處理個人資料保護法

02 國家機密保護法

03 營業秘密法

04 刑法

05 醫師法

二、資訊公開 *(Disclosure)*

01 政府資訊公開法

02 檔案法

三、資訊監察 *(Monitors)*

01 通訊保障及監察法

四、資訊應用 *(Application)*

01 電子簽章法

貳、本案例編碼共 *7* 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年份及上述各小類之編碼各兩碼，最後兩碼為該小類中之第幾篇案例。例如：*S990101*，即代表資訊保護類 *99* 年度之電腦處理個人資料保護法第一則案例。

目　　次

壹、資訊保護（*Security*）.....1
一、電腦處理個人資料保護法.....2
銀行個資外洩 客戶心慌慌.....2
港史最大個資弊案　八達通承認獲利 *1.8* 億.....6
遊戲誘供門號 手機認證詐騙.....9
OO 銀行洩個資 聯徵中心取消其消金部門查詢權 *42* 天.....12
Google 街景圖侵隱私 消基會要求移除人像.....16
18 萬公務員身分證號外洩.....19
誹謗官司挑戰 *Google* 對用戶隱私權保護.....22
役政洩個資 愛滋男被父趕出門.....25
二、國家機密保護法.....29
前國安局副處長 著作洩密遭判刑.....29
國慶文告洩中國 台商判刑 *2* 個月.....32
NASA 賣電腦 忘刪敏感資料.....35
美國空軍警告 臉書可能洩漏軍機.....38
三、營業秘密法.....41
影印機複印機密資料　自動儲存易被竊取.....41
補習班惡鬥偷個資 判賠 *1500* 萬.....44
惠普與甲骨文 *25* 年情誼恐生變.....47
四、刑法.....50
刪電腦資料報復 離職會計遭判刑.....50
為公司 秘書侵入上司電郵無罪.....53
旅行社員工 盜刷客戶信用卡.....56
調查官想減工作量 駭主管電腦遭起訴.....59

駭客土法煉鋼 *1* 年半破解 *1* 密碼 62
釣魚網站猖獗 較上月增五成 65
男子分享平台下載軍方資料被求刑 68
五、醫師法 71
公布他人病歷 醫師行政訴訟敗訴 71
貳、資訊公開（*Disclosure*） 75
一、檔案法 76
申請閱覽卷宗 需先有行政程序存在 76
參、資訊監察（*Monitors*） 79
一、通訊保障及監察法 80
美國法院判決非法 *GPS* 追蹤違憲 80
竊聽女秘書電話 董座判賠 83
肆、資訊應用（*Application*） 86
一、電子簽章法 87
統一發票無紙化 未來存晶片卡內 87
地政電子謄本系統提供具備法律效力的電子謄本 90
俄國業者宣稱可破解 手機資料保護機制 93
票選人評委員 政院網路投票員工怕 *IP* 暴露 96

壹、 資訊保護（*Security*）

一、電腦處理個人資料保護法

類別：資訊保護

【案號：*S990101*】

銀行個資外洩 客戶心慌慌

【資料來源：經濟日報 *99/03/12*】

焦點話題

滙豐控股公司（*HSBC*）旗下瑞士私人銀行分行的帳戶資料遭離職員工竊取，可能影響多達 *2.4* 萬名客戶。滙豐表示，其瑞士私人銀行的離職員工法契亞尼（*Herve Falciani*），在 *2006* 年底至 *2007* 年初竊取這些客戶資料。這些客戶來自全球各地，包括 *1.5* 萬名 *2006* 年 *10* 月前開設瑞士帳戶的客戶，和已關閉的 *9,000* 個帳戶。這意味部分客戶的資料可能落入母國稅務機關手中，並面對逃漏稅追查，滙豐可能因此流失大量客戶。

滙豐指出，法契亞尼在公司資訊科技部門任職多年，深受信賴，在一次資料遷移的過程中接觸到這些機密資料。滙豐聲稱，法契亞尼把資料轉存到個人裝置上，然後設法對黎巴嫩數家銀行兜售這些資料。先前也有報導指出，他曾企圖把這些資料以 *250* 萬歐元賣給德國；稅務調查界人士估計，德國可能從這些資料追回 *1* 億歐元稅金。

重點摘要

1. 客戶及帳戶資料屬於個人資料，若有洩露，銀行應依電腦處理個人資料保護法及銀行法之相關規定負法律責任。
2. 依 *99* 年 *5* 月 *26* 日公布之個人資料保護法規定，非公務機關於知悉資料外洩時，應查明後以適當方式通知當事人。

法律觀點

本案例屬於銀行內控疏失導致資料外洩之典型案例。銀行為一般民眾提供存款、放款等業務，因此保有大量民眾個人資料及帳務資料等個人隱私資訊，屬於「電腦處理個人資料保護法」之適用對象，若此案例發生在台灣，受害民眾每人依法[1]可向銀行請求新台幣(下同)*2* 萬元以上 *10* 萬元以下之損害賠償，合計最高總額以 *2000* 萬元為限。另總統已於 *99* 年 *5* 月 *26* 日公布「個人資料保護法」(以下簡稱新版個資法)，未來新版個資法施行後，每人每一事件可以請求之賠償金額為 *500* 元以上 *2* 萬元以下，合計總額提高至 *2* 億元[2]，因此損害賠償上限將大幅提高。又新版個資法第 *12* 條[3]賦予非公務機關於知悉資料外洩時，應查明後以適當方式通知當事人之義務，若違反第 *12* 條規定，由中央目的事業主管機關或直轄市、縣(市)政府限期改正，屆期未改正者，按次處新臺幣 *2* 萬元以上 *20* 萬元以下罰鍰，應特別注意。

另外，為促進銀行健全發展，銀行應特別重視資訊安全之維護，銀行法第 *45* 條之 *1*[4]即規定銀行應建立內部控制及稽核制度，若違反內部控制及稽核制度之相關規定，依銀行法第 *129* 條第 *1* 項第 *7* 款規定[5]，可處 *200* 萬元以上 *1000* 萬元以下罰鍰，亦屬於重罰，不可輕忽。

由此可知，個人資料及機密資訊的保護機制上，應建立適切的保護機制並做好內部員工管理及可攜式個人裝置之控管，否則不但會面臨受害民眾求償及主管機關之處罰，商譽更將嚴重受損，損害範圍將難以估算。

管理 *Tips*

以此案例而言，雖然是離職員工的資料外洩行為，但該員工取走資料的時間是在職期間，所以銀行應就其取得資料之管道再行研議，在本案例中應可就以下 *3* 方面討論之：

- 系統變更(資料遷移)之安全控管：公司內部資訊人員常會因業務需求，而有機會直接接觸公司之重要資料，惟在線上運作環境，往往已有較嚴

格的權限控管與相關的防護或存取紀錄機制，但是當進行重大系統變更時往往容易出現系統控管上較脆弱的狀況，組織應就此再加強控管，如在變更期間增加監督人員或將移轉工作中撰寫程序與執行程序之人交由不同人員執行，應較可能避免案例中發生之狀況。

- 個人資訊裝置的控管：隨著科技的進步，儲存媒介有越來越小與越來越多樣化的趨勢，如隨身碟、手機、數位相機及錄音筆等，組織越來越難全面性地防範相關設備的使用，所以應可就重要的防護區域(如機房)或重要的資訊設備(如核心系統伺服器)進行嚴格的使用控管，如嚴禁攜入安全區域、關閉重要資訊設備之 *USB* 埠、錄影監控或人員陪同等，以避免相關裝置使用帶來的風險。

- 保密協議的有效性：針對處理重要資料之人員，應特別注意其保密協議的有效期，應於離職後仍保有效力，組織也應於辦理離職程序時，再次告知員工應保密之責任。

相關標準

A.8.1.3 聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.9.1.2 實體進入控制措施

安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出。

A.9.1.5 在安全區域內工作

應設計在安全區域內工作的實體保護與指導綱要，並施行之。

A.10.1.3 職務的區隔

職務與責任領域應加以區隔，以降低組織資產遭未經授權或非意圖的

修改或誤用之機會。

A.10.7.1 可移除式媒體的管理

應有適當的程序以管理可移除式媒體。

A.12.5.1 變更控制程序

應藉由使用正式的變更控制程序，以控制變更的實作。

A.12.5.4 資料洩漏

應防範資訊洩漏的機會。

---

[1] 電腦處理個人資料保護法第 27 條第 3 項：「前 2 項損害賠償總額，以每人每一事件新臺幣 2 萬元以上 10 萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。」、第 4 項：「基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣 2000 萬元為限。」、第 28 條第 2 項：「依前項規定請求賠償者，適用前條第 2 項至第 5 項之規定。」

[2] 個人資料保護法第 28 條第 3 項；「依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣 500 元以上 2 萬元以下計算。」、第 4 項：「對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣 2 億元為限。但因該原因事實所涉利益超過新臺幣 2 億元者，以該所涉利益為限。」、第 29 條第 2 項：「依前項規定請求賠償者，適用前條第 2 項至第 6 項規定。」

[3] 個人資料保護法第 12 條:「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

[4] 銀行法第 45 條之 1：「銀行應建立內部控制及稽核制度；其目的、原則、政策、作業程序、內部稽核人員應具備之資格條件、委託會計師辦理內部控制查核之範圍及其他應遵行事項之辦法，由主管機關定之。銀行對資產品質之評估、損失準備之提列、逾期放款催收款之清理及呆帳之轉銷，應建立內部處理制度及程序；其辦法，由主管機關定之。銀行作業委託他人處理者，其對委託事項範圍、客戶權益保障、風險管理及內部控制原則，應訂定內部作業制度及程序；其辦法，由主管機關定之。」

[5] 銀行法第 129 條第 1 項第 7 款：「未依第 45 條之 1 或依第 123 條準用第 45 條之 1 規定建立內部控制與稽核制度、內部處理制度與程序、內部作業制度與程序或未確實執行。」

類別：資訊保護

【案號：*S990102*】

港史最大個資弊案　八達通承認獲利 *1.8* 億

【資料來源：年代新聞 *99/07/27*】

焦點話題

香港八達通公司承認，其自 *2006* 年到 *2010* 年這 *4* 年半內，一共販售了 *197* 萬名的客戶資料，獲利金額達 *4400* 萬港幣，約台幣 *1* 億 *8200* 萬元，單就這筆收入就佔了八達通總收益的 *31%*，堪稱香港有史以來最大宗的個資販售事件。八達通係香港發行智能卡的公司，該卡使用方便，用途廣泛，香港人幾乎人手一張，八達通可說是擁有全香港私人資料最多的公司。原本八達通表示絕不會向第三者出售客戶資料，但竟發生出售客戶資料非法牟利的情形。八達通公司的行政總裁表示，「在過去 *4* 年半裡，我們總共提供了 *197* 萬名客人的資料給參與的公司，而每一個公司平均聯絡客戶 *1.7* 次。」

八達通不僅販售個人資料還兼賣保險產品，八達通因領有保險代理牌照，可利用公司收集資料，再聯合保險公司作推廣和銷售的工作，從中賺取保險佣金，引起香港政府格外重視。由於事涉重大，所以香港特區個人資料私隱專員公署已主動介入調查。

重點摘要

1. 在未經當事人之書面同意下，將個人資料提供給其他公司進行行銷，可能會有刑事責任。
2. 在提供個人資料時，應確認個人資料使用的特定目的及範圍，避免資料被使用在其他地方，致權益受損。

法律觀點

隨著科技進步，現今服務均以便利民眾為設計，案例中八達通卡即屬於電子錢包，可以作為乘車及小額付款之支付工具，此種智慧卡片內即有儲存金額，只要感應即可扣款並完成消費行為，功能等同於現金，因此此類卡片通常不會記載持有人詳細個人資料，性質類似台灣的悠遊卡或台灣通。惟為能提供更便利的服務，並降低卡片遺失之風險，因此智慧卡亦有記載持卡人個人資料，此部分將涉及個人隱私資料的問題。

案例中記名的八達通卡內存有持卡人姓名、出生年月日及身分證字號，均屬於個人資料，若此案例發生於台灣時，則會有是否適用電腦處理個人資料保護法(以下簡稱個資法)的疑問。這是因為，目前個資法規範公務機關及指定之非公務機關，電子票證業目前雖非指定適用個資法之行業別，惟案例中八達通公司亦有兼營保險代理業務，如以我國個資法而論，應屬保險業而有適用個資法，且八達通乃是為進行共同行銷而將提供給其他公司，因此該公司若未取得當事人書面同意而將資料販售給其他公司進行行銷時，該公司負責人可能會有處 *2* 年以下有期徒刑、拘役或科或併科新臺幣 *4* 萬元以下罰金[1]，且應對資料遭到外洩之民眾負損害賠償責任。

另依新版的個人資料保護法(以下簡稱新版個資法)，所有非公務機關及非個人或家庭活動之自然人均成為新版個資法適用對象。又直接或間接蒐集個人資料時，除有法律有規定的例外情況，否則均有向當事人告知之義務[2]。若要將個人資料使用在特定目的以外的用途，除有依法免為告知事項外，必須另行告知當事人取得書面同意[3]。因此在蒐集當事人資料時，即必須說明特定目的，且不能夠用概括的方式取得當事人同意。因此在案例中，若八達通將資料出售給其他公司進行行銷時，若未告知當事人且取得當事人書面的情況下，依新版個資法規範將面臨 *5* 年以下有期徒刑，得併科新臺幣 *100* 萬元以下罰金之罰則，同時應對資料遭到外洩之民眾負損害賠償責任。

由於個人資料屬於民眾個人的隱私保護範圍，因此在提供個人資料時，應

要詳加閱讀契約條款，確認個人資料被使用的用途及範圍，避免在沒有注意契約的約定下，資料遭他人利用，而造成個人權益損害。

管理 *Tips*

將案例對比國內現況，原個資法並未指定適用票證業者，而新版個資法則將所有非公務機關均納入，因應這樣的差異，組織應立即因應法令規範調整自身的管理制度，為使其能及時掌握相關法令法規的變動，組織應至少設計定期檢視相關法令法規的機制，以降低違反相關法令法規的風險。

另因應新版個資法組織應重新檢視與盤點組織內所有個人資料的蒐集、處理與利用等活動，並於這些使用行為發生前，取得個人資料所有人之同意方可。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私

[1] 電腦處理個人資料保護法第 33 條：「意圖營利違反第 7 條、第 8 條、第 18 條、第 19 條第 1 項、第 2 項、第 23 條之規定或依第 24 條所發布之限制命令，致生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 4 萬元以下罰金。」

[2] 參照個人資料保護法第 8 條及第 9 條規定。

[3] 個人資料保護法第 7 條第 2 項：「第 16 條第 7 款、第 20 條第 1 項第 6 款所稱書面同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。」

類別：資訊保護

【案號：*S990103*】

遊戲誘供門號 手機認證詐騙

【資料來源：聯合報 *99/07/28*】

焦點話題

近來有不少歹徒在網路線上遊戲誆稱朋友，或以遊戲同好招攬被害民眾方式，以免費提供虛擬貨幣、外掛升級增加點數，不用付月費或較低價格買到遊戲點數等理由，誘騙民眾提供手機門號、身分證字號及小額付費認證密碼，詐騙金額 *1000* 元以下錢財。警方調查表示，進行「手機認證小額付費」操作的被害人，因誤信歹徒為友人，或不知手機電話有小額付費功能，聽信操作，隨後收到付費簡訊或帳單，始發現受騙上當，已來不及阻止。詐騙對象主要以網路遊戲玩家為主。例如有名國中生，在家中上網玩網路遊戲，歹徒假冒被害人的朋友，透過遊戲對話窗謊稱，可幫被害人購買遊戲裝備，被害人誤信提供手機門號及小額付費認證密碼，隨後收到簡訊帳單通知，發現被使用 *3* 筆小額付費各 *1* 千元，才知道受騙。警方呼籲民眾切勿因貪小便宜、輕信網友，而隨意提供手機門號、身分證字號或小額付費認證密碼，以免遭歹徒利用「小額付費」機制詐騙，得不償失。

重點摘要

1. 民眾個人身分資料、手機付費認證密碼均屬重要資訊，應避免在網路上提供相關資料，以降低被歹徒詐騙的風險。
2. 歹徒輸入他人手機號碼加身分證號碼及小額付費認證碼進行小額消費會構成不正利用電腦取財得利罪。

法律觀點

網路遊戲愈漸盛行，不少人都有上網購物或玩遊戲的習慣。虛擬的網路世界都是由使用者註冊帳號密碼登入，因此在以網路進行交流時，無法確認網友的真實身分，是以在進行交談及資訊交換時即應特別小心謹慎。本案例中，歹徒誘騙網友提供的手機門號、身分證字號及小額付費認證密碼都是屬於個人資料，惟由於現行電腦處理個人資料保護法(以下簡稱個資法)適用對象不包括自然人，因此歹徒以此方式取得網友個人資料尚無違反個資法的問題。但預計 *100* 年實施新通過的個人資料保護法(以下簡稱新版個資法)，因所有非公務機關，除個人或家庭活動外，包括自然人均屬適用對象，此行為將會面臨 *5* 年以下有期徒刑之刑責[1]。

一般說來，小額付費是一種新型態的付費模式，提供消費者透過手機、信用卡、網路 *ADSL*、預付卡等帳單作為付費機制，使用者只需輸入相關的認證資料，即可進行小額消費。但進行此種小額消費時，付費的認證方式多是以使用者手機號碼加身分證號碼及小額付費認證密碼等資料，因此歹徒輸入上開資料，取得遊戲點數的不正當利益，將構成刑法第 *339* 條之 *3* 的不正利用電腦取財得利罪[2]。雖然詐騙集團的犯罪行為都有相關刑事責任的規定，但在進行網路行為時，僅憑帳號並無法確認歹徒的實際身分，因此還是應該要避免在網路提供個人資料，以免受到詐騙後求償無門。

管理 *Tips*

在本案例中應可從以下 *2* 個面向思考：*1.*現行網路業者為使網路交易更為順利與容易執行，設計多樣化的付款機制，如：手機小額付款與信用卡等大都是透過資料輸入的機制，即可完成交易，是以提供相關付款機制的廠商應於提供資料時，告知使用者資料使用或外洩時可能帶來的風險，以藉此提高使用者警覺，並降低事件發生時的爭議；*2.*使用者應提高對個人機密性資料保護的警覺，避免將相關資料傳輸或告知他人，以降低資料外洩帶來的風險。

相關標準

A.6.2.2 處理客戶事務的安全說明

在賦予客戶存取組織資訊或資產的權限之前，應闡明所有已識別的安全要求。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

---

[1] 個人資料保護法第 41 條第 2 項：「意圖營利犯前項之罪者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

[2] 刑法第 339 條之 3 第 1 項：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處 7 年以下有期徒刑。」、第 2 項：「以前項方法得財產上不法之利益或使第三人得之者，亦同。」

類別：資訊保護

【案號：*S990104*】

OO 銀行洩個資 聯徵中心取消其消金部門查詢權 *42* 天

【資料來源：工商時報 *99* 年 *8* 月 *11* 日】

焦點話題

日前金管會進行金融檢查時發現，○○銀行將客戶的車貸資料，洩漏給合作車商，且 *3* 年內該行已有類似前例發生，聯徵中心為避免類似的情事再度重演，乃對○○銀行祭出重罰停權 *42* 天。過去聯徵中心對於金融機構有違反規定的情形，大多停止調閱信用資料 *5* 至 *30* 天，這次○○銀行會被停權達 *42* 天，主要是自 *98* 年 *8* 月 *1* 日起，聯徵中心開始採行新版會員規範，新增對於「累犯制」的規定，針對違反規定的金融機構，依情節輕重停止向聯徵中心徵詢會員信用資料的權限，最多可停止 *10* 至 *60* 天，嚴重者甚至可被開除會員資格。為重視民眾權益，聯徵中心近日也已發函給全台 *428* 家金融機構，呼籲金融機構重新審視客戶信用資料處理流程，落實內部教育訓練，以避免類似情形再次發生。

重點摘要

1. 聯徵中心會員在蒐集及處理客戶信用資料時，必須善盡告知義務並取得客戶同意書。
2. 聯徵中心會員查詢信用資料後，僅能依法在特定目的範圍內利用，否則會面臨相關法律責任。

法律觀點

財團法人金融聯合徵信中心(以下簡稱聯徵中心)是為了確保金融交易安全，促進全國信用制度健全發展，維護信用資料當事人及會員機構之利益而設立。聯徵中心會員在客戶提出往來申請、簽署申請書或其他授信契約

書時，應取得客戶、連帶債務人、保證人或關係人等當事人同意書，同意聯徵中心得依法令規定，蒐集與處理其本人信用資料，並應清楚告知會員同意書的內容及依照「電腦處理個人資料保護法」(以下簡稱個資法)、「消費者保護法」及金融管理相關法令規定之應告知事項[1]。聯徵中心會員對於客戶善盡告知義務並取得同意後，即可將客戶的信用相關資料提供給聯徵中心建立檔案。聯徵中心的會員在取得當事人的書面同意或與當事人有契約或類似契約關係下，才能向聯徵中心查詢當事人之信用資訊，且會員必須保存當事人同意書、契約書或其他足以證明與其當事人之間存有類似契約關係之往來資料 *5* 年，並在聯徵中心請求時提供[2]。

由於客戶的信用資料屬於隱密的個人資料，必須特別保護，因此聯徵中心會員規範規定，會員必須確保資訊利用的適法性及合目的性，不得逾越特定目的之必要範圍，並應與授信目的或金融管理法令遵循目的具有正當合理之關聯，且查詢所得的信用資訊，應「嚴限內部參考，不得對外公開或移轉他人」[3]，違反者，聯徵中心可以停止其查詢權限，且依照聯徵中心新版會員規範規定，在 *3* 年內 *2* 度發生停止查詢作業時，停止查詢作業之日數上限得加重至 *60* 日[4]。本案例○○銀行將客戶車貸資料洩露給合作車商，顯然逾越特定目的外的利用，且因為○○銀行在 *3* 年已經有類似前例發生，因此被停止查詢作業 *42* 日。另外由於銀行業屬於現行電腦處理個人資料保護法規範的對象，因此車貸資料被外洩的客戶，可以依照個資法的規定，每人每一事件可以請求新台幣 *2* 萬元以上 *10* 萬元以下的損害賠償金額。

聯徵中心會員在查詢資料時，應該確實遵守相關規定進行查詢相關資料，並建立嚴格的內控機制，避免違反相關規定遭到聯徵中心停止查詢作業，而影響日常業務，並負擔相關法律責任，甚者更因此失去客戶的信賴，所受損失恐無法計算。

管理 Tips

任何持有個資的單位，都應對所持有的個資負起保護的責任；現今由於資

訊科技的發達，致使資料有更多不同方式的利用與交換，在面對這些個資的利用與交換前，組織應先行評估其利用或交換合法性，法令上是否有任何相關限制，並依法令之規定設計必要程序，如：於利用與交換前應通知個資所有人，並取得其同意等。

另外在將資料交付與其它組織利用或交換時，組織除應於交換前確認法令上應遵守的事項均符合外，也應於相關合約或協議中，清楚敘明取用資料方對個資的保護責任，此部分可依個資生命週期(蒐集/取得、使用/利用、保存、交換及銷毀)為主軸，訂定其需遵守之事項，並可不定期依此對取用資料方進行查核，以確保個人資料被妥善的保存。

相關標準

A.6.2.1 與外部團體相關的風險之識別

由涉及外部團體的營運過程產生對組織資訊及資訊處理設施之風險，應在核准外部團體存取之前加以識別，並實作適當的控制措施。

A.6.2.3 第三方協議中之安全說明

涉及存取、處理、通信或管理組織的資訊或資訊處理設施，或在資訊處理設施上附加產品或服務的與第三方之協議，應涵蓋所有相關的安全要求。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

[1] 參照聯徵中心會員規範第 10 條
[2] 參照聯徵中心會員規範第 12 條
[3] 參照聯徵中心會員規範第 15 條
[4] 參照聯徵中心會員規範第 17 條

類別：資訊保護

【案號：*S990105*】

Google 街景圖侵隱私 消基會要求移除人像

【資料來源：自由時報 *99/09/16*】

焦點話題

在 *Google Map* 上輸入地址不只能搜尋「實景街圖」，就連車牌和路人穿著都清楚可見，消基會批評 *Google Map* 這項功能已經侵犯個人隱私，因為「人車上路隨時都可能被拍」。據消費者報導雜誌副社長表示，從街景圖中可看見車號，就能判斷車主是誰；若剛好有認識的車輛出現在旅館或當鋪附近，除被侵犯隱私權外，還可能造成爭端、損害車主個人信用，這些都有侵犯民眾隱私的問題。雖然 *Google* 表示會針對人臉部分為模糊處理，但仍有質疑認為透過穿著、體態依然可辨認出照片主角，建議 *Google* 應將「人」完全從實景圖中移除。消基會指出，*Google* 街景上線以來，遭世界各地民眾、隱私權團體及政府機構質疑侵犯隱私權聲浪不斷，但在台灣，*Google* 街景未受阻力，目前 *Google* 的台灣街景已遍及 *14* 縣市，只差台九線的台東至屏東南迴公路一段，路線幾乎已經環台一周。為免 *Google* 美其名的服務，卻讓民眾付出隱私代價，消基會要求 *Google* 應改善可搜尋車牌號碼的功能，並把「人像」移除，同時也呼籲網路服務主管機關 *NCC* 應介入管理。

重點摘要

1. 如知悉車牌號碼為特定個人所有即屬個資法中足資識別該個人的資料。
2. 「實景街圖」照片雖是取自公開場所或公開活動而不屬個人資料之範疇，但對於過去個人公開活動之紀錄，仍應另為影像處理，以免侵犯民眾隱私。

法律觀點

拜網路發達之賜，現今的地圖多可線上查詢，民眾只要透過手機或上網輸入查詢地址，即可清楚知道所有路線資訊。近來網路服務業者為提供更詳盡的地圖資訊，甚至還發展出有實景街道建築的網路地圖，僅需輸入地標位置，就可跨地區或國界的看到遠處的地形樓房，*Google Map* 的「實景街圖」正是時下最夯的網路地圖查詢服務。

只是「實景街圖」的查詢服務，往往涉及到將周邊街景人車也一併拍攝入鏡的問題，民眾的個人活動或車牌號碼，一不小心都有可能成為「實景街圖」的一部份。雖然我國目前的「電腦處理個人資料保護法」(以下簡稱個資法)並未將車牌號碼、個人照片明文列為個人資料的保護範疇，但這些資料的蒐集，如果公布於網站上供一般人瀏覽，而使一般人對街景圖中的個人產生識別性，還是有個人資料與侵犯隱私權的疑慮，因為一般人在從事社會活動時並不會預想到有人會將自己的行為攝影後放在網路上供人觀賞。

值得注意的是，新通過的個人資料保護法(以下簡稱新版個資法)規定只要基於「公共利益」就可為個人資料的蒐集、處理和利用[1]，並且如果個人資料的蒐集、處理和利用是為新聞報導之公益目的，則可免去事先告知的義務[2]。在公開場合或公開活動的影音資料若未與其他個資結合者，也排除新版個資法保護的適用範圍[3]，使得只要是在公開場所或公開活動中所蒐集的影音資料只要未與個人資料結合者都將不會有違反個資法的問題。

不過，「實景街圖」固然提供了民眾一個便捷的新穎服務，取景過程也都是在公開場所為之，雖然沒有觸犯個資法，但還是有民眾隱私權的議題[4]，這是因為隱私權的概念是會隨這社會觀念的演化而會有不同的標準，不適用個資法並不代表未侵犯民眾隱私權。

管理 Tips

隨著資訊科技的進步，越來越多樣的資訊服務陸陸續續的出現，但是隨著

某些新服務的採用使得隱私權的保護受到質疑，例如線上法拍屋資料、監視系統或是案例中所提及之「實景街圖」，均會發生此類狀況。就組織面應於各項服務導入或建置前，即應考量其相關法律上的議題，確認其符合法令法規的要求。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

---

[1] 個人資料保護法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定資料外，應有特定目的，並符合下列情形之一者：六、與公共利益有關。」

[2] 個人資料保護法第 9 條第 1 項：「公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第 1 項第 1 款至第 5 款所列事項。
有下列情形之一者，得免為前項之告知：
一、有前條第 2 項所列各款情形之一。
二、當事人自行公開或其他已合法公開之個人資料。
三、不能向當事人或其法定代理人為告知。
四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。」

[3] 個人資料保護法第 51 條第 1 項：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」

[4] 民法第 18 條：「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。前項情形，以法律有特別規定者為限，得請求損害賠償或慰撫金。」第 195 條第 1 項：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

類別：資訊保護

【案號：*S990106*】

18 萬公務員身分證號外洩

【資料來源：聯合報 *99/10/03*】

焦點話題

OO 局地方行政研習中心的網站，日前突然出現大量身分證字號。這個網站架設的目的，是給初任公務員註冊累積研習時數用的開放式交流平台，公務員只要申請帳號、密碼，都可以進入論壇、發表意見，身分證字號僅作為帳號使用，且會員得隨時更改帳號。但日前有公務員使用該網站時發現突然有 *18* 萬筆的身分證字號大量出現在公共論壇首頁，因事涉公務體系，不免讓人覺得有個資控管上疏失的問題。*OO* 局地方研習中心的主任表示，這套系統使用一年多年來，已多次向使用者建議更改帳號，不過仍有許多使用者認為不涉個人隱私，未將身分證字號改掉，為避免類似情況再次發生，已請廠商針對仍保留身分證字號的使用者，以「隱藏四碼」的方式加強保密。

重點摘要

1. 資訊平台對使用者帳戶密碼的保管，應有完整的維護系統和安全防護，以避免使用者資訊的外洩。
2. 使用者應盡量避免以身分證字號作為帳號密碼的設定，以防資訊輕易的被識別外漏。

法律觀點

許多資訊網站經常會要求使用者，設定帳號密碼以作為登入網站平台的辨識號碼，而一般人最常用來設定帳號密碼的組合，多以身分證字號、出生

年月日或電話號碼等基本資訊作為設定，但隨著個資外洩的問題愈益嚴重，以身分證字號等資訊作為帳號密碼的做法，容易被他人識破和猜出，因此在帳號密碼的設定上建議應定期更換密碼，以維護自身資訊安全。

本案中行政研習中心的網站，以身分證字號作為使用者帳號登入的機制是一般常見的登入方式，但使用上也就冒著容易被辨別和一旦外洩後的風險，由於現今科技的發達，破解程式的盛行，外部人往往只需要輕鬆的使用一些技術，就能入侵網站獲取資訊內容，所以平台網頁才會有定期要求使用者更換密碼的提示或登入之前需輸入額外的英文數字字串的辨識步驟。依照現行的「電腦處理個人資料保護法」，公務機關對於所蒐集的個人資訊，有依法需為安全維護的義務[1]。並且在即將施行的「個人資料保護法」中[2]，亦有就公務機關違反規定的情形，規範每人每一事件可受賠償的損害額度，最高可賠償至新台幣 2 億元。因此未來網站平台業者不論是公務機關或非公務機關，對於公布他人得獎資訊、中獎名單或補助對象等這類可識別該個人之資料與敏感訊息時，都應更加謹慎小心或另外其他的處理。同時如果行政機關與企業團體，是將資訊的蒐集與處理委託外部資訊業者或廠商辦理，此時受委託的廠商或業者，也將被視為是委託機關之人，因此委託機關對於這類廠商或業者外洩資訊的行為，也將一併負起責任[3]。

管理 *Tips*

在此案例中主要發生原因係在系統開發過程中未完善地考量所應具有的安全控管需求，組織在各個系統開發時，應適當的考量所需的安全需求，包含機敏性資料的保存、傳輸等，乃至於存取權限的設計均需被考量在系統開發的規格之中，方可確保系統上線後不會造成其它的資安議題。

另方面並可透過宣導、教育及訓練，讓使用者可以更清楚使用上的風險，以期可以達到最合適的控管。

相關標準

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.12.1.1 安全要求分析與規格

新資訊系統或現有資訊系統提升的營運要求聲明中，應詳述安全控制措施的要求。

---

1 電腦處理個人資料保護法第 17 條：「公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

2 個人資料保護法第 28 條第 1 項：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」第 3、4 項：「依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣 5 百元以上 2 萬元以下計算。」、「對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣 2 億元為限。但因該原因事實所涉利益超過新臺幣 2 億元者，以該所涉利益為限。」

3 電腦處理個人資料保護法第 5 條：「受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人。」

類別：資訊保護

【案號：*S990107*】

誹謗官司挑戰 *Google* 對用戶隱私權保護

【資料來源：中廣新聞網 *99/10/21*】

焦點話題

紐約一位企業顧問從去年開始便遭匿名人士，在 *YouTube* 網站上，張貼好幾段過去自己在哥倫比亞大學攻讀碩士時留下的影像，影片上還附加了涉及性別歧視等不堪入耳的言語。為查出到底是誰在網路上造謠誹謗他，該名企業顧問因而訴諸司法行動，法院強制 *Google* 須揭露藏鏡人的身分，提供其真實身分與聯絡資料。有認為這起判例對於網路匿名誹謗，應該可以發揮嚇阻效果，但對於網站經營業者來說，這將挑戰他們對用戶隱私權保護的堅持。匿名雖然是網路的一種傳統，甚至被許多人認為是一種價值，但隨著有愈來愈多人嚐到被匿名霸凌的苦果後，如何在網路上打擊語言暴力，將言論自由限制在合法的範圍內，就成了資訊時代下，司法必須面臨的新挑戰。

重點摘要

1. 網際網路雖具有匿名的特性，但在網路上散布不實的言論，仍將受到法律的制裁。
2. 網友在網站上註冊的資料雖然受到個人資料保護法的保護，但司法機關基於審理案件所需，仍得依法向網站業者調取個人資料。

法律觀點

在網路活動未發達以前，一般人的言行多需透過親自交往會面才能互相溝通接觸，但拜科技進步之賜，越來越多的人際溝通及活動是透過網路來進

行。匿名性是網路世界的特性，且因不會直接面對面接觸，因此一般人不易辨識使用者的真實身分。

目前大多數網路平台是採取註冊會員制，使用者必須註冊成為會員後，才能在網站上張貼文章或進行交易。使用者在註冊時不可避免的會提供個人資料。為避免使用者擔心隱私權受到侵害，而不願意使用網站服務或提供個人資料，大多網路服務業者均會在網站揭示隱私權政策，讓使用者可以安心使用。在現行法下，使用者的隱私權受到不法侵害時，除可以透過民法請求損害賠償外，由於主管機關指定無店面零售業者自 *99* 年 *7* 月 *1* 日起適用電腦處理個人資料保護法[1](以下簡稱個資法)，因此使用者在購物網站提供的個人資料，亦會受到個資法的保護。但使用的網站非屬網路拍賣時，必須等到個人資料保護法(以下簡稱新版個資法)施行後，才會受到規範。依個資法及新版個資法的規定[2]，公務機關在執行法定職務的範圍內，可以蒐集、處理及利用個人資料，因此司法機關基於調查犯罪的需求，可以向網路服務業者調取犯罪嫌疑人的個人資料。至於對網路服務業者而言，提供使用者個人資料給司法機關，屬於法律有明文規定而可以為特定目的外利用之情況[3]，因此並未違反個資法之規定。

雖然使用者在註冊時未必會提供正確的個人資料，但使用者的帳號可以連結其登錄位址，再透過登錄位址查詢使用者於上網時實際所在位置，在抽絲剝繭下，仍然可以特定使用者的真實身分，因此使用者在從事網路行為時，還是應該遵守法律規定，以免觸法。

管理 Tips

本案例可就以下兩方面討論之：

1. 對網路服務提供者：應於使用者註冊時，適當地告知其所需遵循的法律責任，並可於使用期間定期或不定期抽查，以確認相關內容均不違反法令法規之規範，確保盡善良管理者之責任。

2. 對網路服務使用者：應需針對其行為，清楚地辨識其所需遵循的法令法規。針對他人的文字應避免誹謗或人身攻擊，不該躲在網路匿名性的保護傘下，而踰越法律的規範。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

---

[1] 經濟部 99 年 2 月 9 日經商字第 09902001510 號函。

[2] 參照電腦處理個人資料保護法第 7 條、個人資料保護法第 15 條規定。

[3] 參照電腦處理個人資料保護法第 23 條、個人資料保護法第 20 條規定。

類別：資訊保護

【案號：*S990108*】

役政洩個資 愛滋男被父趕出門

【資料來源：中國時報 *99/11/09*】

焦點話題

兵役處理疏失，意外讓役男愛滋感染身分曝光，造成家庭關係緊張，險被掃地出門！愛滋感染者權益促進會呼籲，政府已明文規定，處理愛滋相關業務務必保密，但部分業務承辦人員常疏失造成感染者身分曝光，侵害權益。

剛大學畢業準備投入職場的某甲因感染愛滋而辦理免役，但有天竟接到母親電話，泣責他感染愛滋卻不告知。原來是地方里幹事在兵役體位判定書上註明「後天免疫缺乏症候群」，應由本人親自領取，透過大樓管理員轉交母親，讓甲頓時啞口無言，親子關係緊張。

某乙研究所畢業，父親希望他提早入伍，自行打電話詢問市公所為何遲遲沒收到兵單，役政人員逕自告知某乙免役的理由是「愛滋」。父親擔心造成親戚恐慌，要求兒子搬出去住。

權促會社工強調，內政部役政署明文要求，處理愛滋相關業務務必以「密件」處理，文書通知應以電話聯絡或掛號郵件由役男親領，不得代領。依據「人類免疫缺乏病毒傳染防治及感染者權益保障條例」規定，洩漏違者處 *3* 萬元以上 *15* 萬元以下罰鍰。

重點摘要

1. 相關人員因業務知悉後天免疫缺乏症候群感染者之個人資料時，除法律有規定或基於防治所需要外，不得洩漏給其他人。

2. 後天免疫缺乏症候群感染者之個人醫療資料屬於敏感性資料，除法律有特別規定外，不得蒐集、處理或利用。

法律觀點

愛滋病又稱為「後天免疫缺乏症候群」，雖然感染者不會立刻發病，但因為這種病毒目前還無藥物可供治療，所以往往令人聞之色變，敬而遠之。為保障人類免疫缺乏病毒感染者(以下簡稱感染者)之人權，我國於 79 年 12 月 17 日即公布實施「人類免疫缺乏病毒傳染防治及感染者權益保障條例」(以下簡稱本條例)，以保障感染者的安養、居住、就醫及隱私等基本權利。依照本條例第 14 條之規定：「主管機關、醫事機構、醫事人員及其他因業務知悉感染者之姓名及病歷等有關資料者，除依法律規定或基於防治需要者外，對於該項資料，不得洩漏。」因此，相關人員除因法律規定或基於防治需要者外，不得洩漏因業務知悉感染者姓名及病歷等有關資料。案例中感染者資料遭到外洩，乃是因為相關人員未將兵役體位判定書交付給本人親自領取或對本人以外的人洩漏感染乙事，且此等行為並非法律規定或基於防治所需要，已違反上開規定，依本條例第 23 條規定，將面臨 3 萬至 15 萬元之罰鍰[1]。

新版個人資料保護法(以下簡稱新版個資法)對於醫療、基因、性生活、健康檢查及犯罪前科等較敏感之個人資料，特別規定原則不得蒐集、處理或利用[2]，後天免疫缺乏症候群感染者之個人資料，屬於醫療資料部分，將受到新版個資法之保護。如違反新版個資法規定，而致他人受有損害者，將可能會有 2 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金[3]，當事人並可以請求民事損害賠償。以本案例來說，洩露者依本條例規定將被處以屬行政罰性質之罰鍰，固不待言，但若法院依新版個資法規定認為洩漏者應負刑事責任時，基於行政罰法[4]的規定，洩露者將只須負刑事責任，此乃是基於一事不二罰原則，避免行為人被重覆處罰。

管理 *Tips*

本案例主要發生原因係為組織內員工教育訓練之缺乏。依據本條例第 *14* 條:「主管機關、醫事機構、醫事人員及其他因業務知悉感染者之姓名及病歷等有關資料者，除依法律規定或基於防治需要者外，對於該項資料，不得洩漏。」役政人員不應將愛滋感染者資料外洩。新版個資法第 *6* 條提及「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」本案例中之敏感個人資料，係公務機關執行法定職務所必要，因此可加以蒐集、處理或利用，惟組織應更謹慎處理此類敏感個人資料，不應輕易傳遞或洩漏予他人。組織可透過教育訓練及宣導，使業務執行人員更清楚瞭解所應擔負之法律責任。

相關標準

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

---

[1] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 23 條:「違反第 11 條第 3 項、第 12 條、第 13 條、第 14 條、第 15 條第 1 項及第 4 項、第 17 條或拒絕第 16 條規定之檢查或治療者，處新臺幣 3 萬元以上 15 萬元以下罰鍰。」

[2] 個人資料保護法第 6 條:「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。」

[3] 個人資料保護法第 41 條：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。」

[4] 行政罰法第 26 條第 1 項：「一行為同時觸犯刑事法律及違反行政法上義務規定者，依刑事法律處罰之。但其行為應處以其他種類行政罰或得沒入之物而未經法院宣告沒收者，亦得裁處之。」

二、 國家機密保護法

類別：資訊保護

【案號：*S990201*】

前國安局副處長 著作洩密遭判刑

【資料來源：中國時報 *99/06/26*】

焦點話題

前國安局副處長蕭○○退休後撰寫《情報工作卅年》一書，被控洩漏國家機密及相關資訊。蕭○○曾任職國安局長達 *30* 年，退休前擔任該局第一處副處長 *5* 年多，負責國安局的國際情報合作、情報組織佈建、情報蒐集等工作，同時也是國安局安全幹部訓練「佈建總論」課程的教材編寫人及講授教官。蕭○○於 *95* 年 *1* 月初退休後，將他個人過去參與情報工作、人員訓練的各項經驗彙整，加上個人 *30* 年工作的心得，於 *96* 年 *11* 月集結成書，交由出版社印製出版。蕭 *OO* 在撰寫期間，曾於 *96* 年 *3*、*4* 月間，請國安局審查底稿，同年 *4* 月，國安局發函蕭○○，告知該書內容涉及多項國安局已奉核定的機密，請他勿公開發行，若出版將涉危害公務機密。蕭○○認為其未提及任何情報人員的姓名，也沒有附有情報工作文件影本，不涉及洩密，蕭○○並主張國安局是在本案發生後，才補核定為機密。惟台灣高等法院認為蕭○○出書內容涉及國務機密，有違反國家機密保護法判處其有期徒刑 *1* 年 *2* 個月，緩刑 *3* 年。

重點摘要

1. 已核定為國家機密之資料，即必須依保密等級維護，不得任意洩漏。
2. 洩漏內容若屬機密資料，縱未具體指名情報人員姓名，亦無實際明顯之情資描述，依法仍應負洩密責任。

法律觀點

國家機密保護法(以下簡稱本法)之制訂，乃是為了建立國家機密保護制度，以確保國家安全及利益，內容對於機密的認定、保存方式、機密期限及維護均設有相關規定。本法規定的國家機密，是指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依法核定機密等級者[1]。政府機關持有或保管的資料，經核定為國家機密後，相關人員即應負保密義務，不得洩漏。若故意洩漏或交付經核定為機密之事項，依本法第 *32* 條[2]規定，處 *1* 年以上 *7* 年以下有期徒刑，若因過失洩漏或交付，也將面臨 *2* 年以下有期徒刑、拘役或科或併科新臺幣 *20* 萬元以下罰金。所以行為人若知悉資訊已被核定為機密資料，則應遵守國家機密保護法的規定，不得任意洩漏。本案例蕭○○在尚未出版印製該著作之前，即已接獲國安局的通知，表示該著作所揭露之部分內容已被核定為國家機密，請他不可以公開發行。但蕭○○知悉該等事項已經有不得公開的情形後，卻仍然出版印製著作，顯然違反上述本法第 *32* 條的規定。

至於蕭○○抗辯本案發生後，國安局才補核定為機密，若蕭○○的抗辯屬實，因蕭○○洩漏時，該資料並非本法規定的機密資料，恐難依國家機密保護法規定追究責任。但若資料屬於國防機密，仍應依刑法第 *109* 條[3]負刑事責任，應注意之。

管理 *Tips*

在此案例中很明顯地在組織與員工間針對機密資訊的判定有不一樣的認知，所以就管理面而言，組織應在初期便對其人員可能接觸的所有資料進行機密等級之判定，並將判定結果清楚宣達予所有可能接觸資料的人員，使所有人員瞭解其所應該擔負之責任，並避免其中的爭議之處。

相關標準

A.7.2.1 分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

---

[1] 國家機密保護法第 2 條：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[2] 國家機密保護法第 32 條第 1 項：「洩漏或交付經依本法核定之國家機密者，處 1 年以上 7 年以下有期徒刑。」、第 2 項：「因過失犯前項之罪者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。」

[3] 刑法第 109 條第 1 項：「洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處 1 年以上 7 年以下有期徒刑。」

類別：資訊保護

【案號：*S990202*】

國慶文告洩中國 台商判刑 *2* 個月

【資料來源：中央社 *99/07/28*】

焦點話題

甲○○為印刷廠離職員工，赴中國大陸經商，利用老東家承包印製總統國慶文告機會，於民國 *93* 年國慶前夕找前同事取得文告全文並傳真大陸。甲○○向承印總統國慶文告講稿、並為總統府人員聯繫窗口的印刷廠公司組長乙○○探詢口風。乙○○取得總統府國慶文告資料後，私下將原稿影本拿給甲○○，甲○○再將資料傳真給中國大陸某經商友人。台北地檢署認為國慶當天由總統所宣示的國慶文告，在正式公布前，均屬國家機密，不得外洩，是以違反「國家機密保護法」之規定，將兩人提起公訴。全案經台北地院審理後，認定國慶文告非屬國家機密事項，但認為內容涉及政府施政方針，與國家政務仍有利害關係，因此改依刑法「洩漏國防以外之秘密罪」，將兩人判刑 *5* 月，減為 *2* 月又 *15* 日，得易科罰金。

重點摘要

1. 是否屬於國防以外應秘密事項，是採實質認定，客觀上若已採取實質保密措施，即使未經核定為公務機密，仍屬於國防以外應秘密事項。
2. 刑法第 *132* 條乃是保護國家法益，因此所洩漏之國防以外之秘密，應指與國家政務或事務上具有利害關係之文書、圖畫、消息或物品。

法律觀點

在此案例中，檢察官雖然以違反「國家機密保護法」之規定起訴，惟法院認為國慶日按總統講話原稿實質內容所示，其秘密性並不涉及與國防整體

安全或利益，而是屬於與國防人事、情報、作戰、演訓、軍備、編裝及軍事整建、防衛動員、通信資訊及電子、主計等具體事務相關的內容，因此認為國慶日總統講話是一般公務機密。

甲○○及乙○○抗辯國慶總統講話內容不屬於國防以外之機密，但法院認為刑法第 *132* 條第 *1* 項[1]所謂「應秘密」者，是指國家政務或事務上具有利害關係而應保守秘密之文書、圖畫、消息或物品。總統文告的內容，是總統基於憲法及憲法增修條文所賦予的行政權範圍，涉及政策宣示、國家施政方向或國家定位等內容意旨，雖然不涉及具體性、技術性的執行事項，但屬於未公開前一般人非可容易取得的資訊來源，與國家政務或事務上具有利害關係。而且總統文告內容有時會涉及重要政策宣示意旨，人民及國內外政經勢力均會予以關注，而形成相當合理期待，認定總統文告會產生國家政策重大方向之實質宣示意涵，因此可認是國防以外應秘密之事項。本案總統府承辦人員將密封的總統國慶文告擬稿交付給乙 *OO* 時，口頭上均有告知此為機密文件不可洩漏，因此法院認定客觀上總統府已採取相當的保密措施。甲○○及乙○○將總統文告轉交給第三人，依刑法第 *132* 條第 *2* 項[2]規定，非公務人員若利用職務或業務上知悉有關國防以外應秘密之事時，將有刑法洩漏國防以外祕密罪的成立，最重可處 *1* 年以下有期徒刑。因此，一般人即使非公務人員只要因為職務上或業務上的關係而知悉國家機密或應秘密事項時，不論是否經過核定機密的程序，都應遵守保密義務，以免不慎誤觸法網。

管理 Tips

此案例中雙方(印刷廠與總統府)對未公告國慶文告之機密程度認知有不一致的現象，組織在處理機密或敏感資料，除在組織內部應遵循公司內部控管方式外，在委託外部廠商時更應加強注意，應在委外時清楚告知委外廠商其所處理資料的機密性質與其應負的保密責任，以確保在整個資料生命週期中資料都能獲得妥善的保護，且相關人員均瞭解其所應負的責任。

相關標準

A.6.2.3 第三方協議中之安全說明

涉及存取、處理、通信或管理組織的資訊或資訊處理設施，或在資訊處理設施上附加產品或服務的與第三方之協議，應涵蓋所有相關的安全要求。

A.10.2.1 服務交付

應確保包含於第三方服務交付協議內的安全控制措施、服務定義及交付等級已由第三方予以實作、執行及維持。

[1] 刑法第 132 條第 1 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。」

[2] 刑法第 132 條第 2 項：「非公務員因職務或業務知悉或持有第 1 項之文書、圖畫、消息或物品，而洩漏或交付之者，處 1 年以下有期徒刑，拘役或 3 百元以下罰金。」

類別：資訊保護

【案號：*S990203*】

NASA 賣電腦 忘刪敏感資料

【資料來源：中央社 *99/12/08*】

焦點話題

美國國會的稽核報告顯示，美國國家航空暨太空總署（*NASA*）即將在明年結束太空梭計畫，準備要把數以千計的多餘物品處理掉，但卻未先清除電腦和硬碟裡的敏感資料，就把設備賣出去。該報告表示甘迺迪太空中心（*Kennedy Space Center*）有 *14* 台電腦未事先測試是否已清除敏感資料即遭處理，其中 *10* 台已釋出給大眾。同時，甘迺迪太空中心和維州朗里研究中心（*Langley Research Center*）亦有硬碟遺失，稍後雖在甘迺迪太空中心的垃圾場找回部分硬碟，但垃圾場通常存放準備出售的物品，民眾可任意出入。檢查人員也發現多個準備出售的電腦板，都標有 *NASA* 網際網路通訊協定的 *IP* 位址。稽核報告指出，*IP* 位址可以讓駭客取得進出 *NASA* 內部電腦網絡的管道，此些行為已造成佛羅里達州、德州、加州和維吉尼亞州的 *NASA* 中心有嚴重的安全漏洞。

重點摘要

1. 處分存有敏感資料的電腦或儲存裝置，應確認敏感資料已刪除，避免敏感資料不慎外洩。
2. 公務人員因為疏失洩漏機密資料，將會視機密資料性質，依照國家機密保護法或刑法追究刑事責任。

法律觀點

本案例中，美國國家航空暨太空總署(*NASA*)針對報廢和汰舊的電腦與硬碟

設備，未在處分前刪除電腦內的敏感資料，導致敏感性資料有外洩之虞，且將準備出售之物品存放在一般人可以任意進出的垃圾場，可能會遭人取走。*NASA* 執掌的檔案資料，多涉及該機關中重要的研究計畫和訊息資料，甚至有些衛星照片還與國家間太空競爭有關，涉及國防安全，可能屬於國家機密。此案例若發生在台灣，若外洩的資料屬於國家機密保護法核定的國家機密時[1]，雖然案例中人員並非故意外洩敏感資料，但國家機密保護法有處罰過失洩漏國家機密的罰則[2]，因此過失洩漏國家機密亦將有刑事責任。若洩漏的敏感資料非屬於國家機密時，依照刑法的規定，公務員因為過失洩漏國防秘密[3]或國防以外秘密[4]，亦均有刑事責任。因此公務人員在處分儲存敏感資料的電腦或儲存裝置時，應特別注意在處分前確認敏感資料是否已徹底刪除，以免因為疏失而被追究刑事責任。

管理 *Tips*

組織於管理媒體及設備時應有正式之程序，並應需於出售或汰除裝載資料之媒體時，確保敏感資料與業務相關軟體等均已依適當之程序移除或覆寫。本案例中之一般民眾可任意出入存放待出售之設備及媒體的區域，對資訊設備管理安全有一定威脅。組織對於存放設備之區域應加以控管及保護，以降低資訊處理設施遭受未經授權之存取或遺失的可能性。

相關標準

A.9.1.1 實體安全周界

應使用安全周界(諸如牆、卡控入口閘門或人員駐守的接待櫃檯等屏障)，以保護含有資訊及資訊處理設施的區域。

A.9.2.6 設備的安全汰除或再使用

含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫。

A.10.7.1 可移除式媒體的管理

應有適當的程序以管理可移除式媒體。

A.10.7.2 媒體的汰除

媒體不再需要時，應使用正式程序加以安全地和無害地汰除。

---

[1] 國家機密保護法第 2 條：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[2] 參照國家機密保護法第 32 條第 2 項及第 33 條第 2 項規定。

[3] 參照刑法第 110 條規定。

[4] 參照刑法第 132 條第 2 項規定。

類別：資訊保護

【案號：*S990204*】

美國空軍警告 臉書可能洩漏軍機

【資料來源：台灣醒報 *99/11/19*】

焦點話題

美國空軍發布警告表示，使用者使用社群網站時若粗心大意，洩漏方位，可能會破壞作業系統安全和隱私。空軍官員擔憂部隊使用黑莓機等其他具有 *GPS* 定位系統的設備，還擔心像臉書的網站提供的定位功能，會洩漏使用者的方位。

在大多數的社群網站上，使用者可以調整隱私設定，避免洩漏所處方位，讓自己不會無所遁形。但臉書經常引發出隱私權爭議。該網站曾更改設定，除非使用者特別設定，否則使用者的個人檔案將向任何人開放。臉書也曾推出新功能「地標」(*place*)，讓使用者標記自己的所在位置。臉書坦承，部分應用程式開發商私下將用戶 *ID* 賣給資訊掮客。

重點摘要

1. 使用具有 *GPS* 定位系統功能的設備或服務，可能會暴露使用者的位置，而使隱私外洩。
2. 不慎使用具備定位功能的設備或服務，導致具機密性的軍事基地曝光時，將違反國家機密保護法或刑法的規定。

法律觀點

「標記位置」是目前社群網站和行動上網流行的一種新功能，它可以標示使用者目前所在位置，並將位置分享給朋友，此功能讓業者可以提供更多加值服務，例如餐飲娛樂資訊或地圖索引，也增加使用者與親朋好友間的

互動，為生活帶來便利性，但同時也將揭露個人隱私予他人知悉。甚者，軍事人員一旦使用手機或社群網站的標記位置功能，可能會將具機密性的軍事基地位置外洩。基於國家安全的考量，軍事基地對其位置資訊和管制均相當嚴格。軍事人員不慎洩漏軍事基地所在位置時可能會觸犯國家機密保護法[1]或刑法[2]，外洩者將可能面臨 *1* 年以上 *7* 年以下有期徒刑。若軍事基地位置經核定為國家機密，則因國家機密保護法為特別法，應優先作為處罰依據，且若外洩者具備公務員身分，並將按情節輕重，受到懲戒或懲處[3]。若外洩的軍事基地位置非屬國家機密，則將被論以刑法洩漏國防機密罪。

科技新功能固然可以提升人民生活的便利性，並提供更多的娛樂效果，增加生活樂趣，但在使用上必須特別注意，尤其是所在位置必須保密時，更應提高警覺，以免無意間暴露所在位置，不但隱私外洩，更可能影響國防軍事安全。

管理 *Tips*

本案例可就以下 *3* 方面討論之：

- 社群網站：應以適當方式告知或提醒使用者其資料使用情況，以及相關隱私狀態。針對與應用程式開發商間之資料交換，應有相關政策與協議加以規範。
- 社群網站使用者：應定期檢視隱私設定，並且於張貼任何個人相關資訊於社群網站或使用應用程式前，謹慎思考可能對個人隱私造成的威脅。
- 軍事單位：組織可透過教育訓練，讓使用者了解相關地理位置等資訊的暴露將對組織造成的衝擊，並應適當地進行宣導，使其能更正確地辨識需保護的資料。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作

職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.8.1 資訊交換政策與程序

應備妥適當的正式交換政策、程序及控制措施，以保護經由使用所有型式通訊設施的資訊交換。

A.10.8.2 交換協議

組織與外部團體間資訊與軟體的交換應建立協議。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

---

[1] 國家機密保護法第 32 條第 1 項:「洩漏或交付經依本法核定之國家機密者,處 1 年以上 7 年以下有期徒刑。」

[2] 刑法第 109 條第 1 項：「洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處 1 年以上 7 年以下有期徒刑。」

[3] 國家機密保護法第 38 條：「公務員違反本法規定者，應按其情節輕重，依法予以懲戒或懲處。」

三、 營業秘密法

類別：資訊保護

【案號：*S990301*】

影印機複印機密資料　自動儲存易被竊取

【資料來源：年代新聞 *99/08/30*】

焦點話題

目前市售的影印機都具有記憶功能，尤其是中高等級的還配備有大容量硬碟，只要透過很簡單的程式，經過影印掃描的機密資料或者個人證件，就能夠一覽無遺、並且重新複印，使得影印機無形中成為最大的洩密者。根據網路消息所揭露，所有經過影印機掃描的圖像和文字，都會被儲存在影印機裡，只要透過很簡單的程式，就可以調出這些資料。影印機維修員也表示，掃描進去的原稿檔案都在這內部儲存空間裡面，可以隨時調閱，隨時複印，現在的數位影印機一般可存 *50* 頁。只要在複印檔案前，先對檔案進行掃描，然後儲存到硬碟空間裡，就具有一次掃描，多次複印的功能。雖然這項內部記憶功能，可由操作者決定儲存，或者不儲存，但大部分民眾對於這個功能的表示多是，「我對這個不怎麼瞭解」。一般消費者既不懂、也不會注意到影印機的記憶功能，因此，要去店家影印時，如果資料或者證件特別須要保密，最好去信任的店家，以免所有資料都一覽無遺。

重點摘要

1. 對於機密資料應該採取合理的保密措施，始符合營業秘密法的保護要件。

2. 擅自重製影印機內所儲存之機密資料，屬於侵害營業秘密，應負相關法律責任。

法律觀點

影印機是處理事務不可或缺之重要工具，一般被使用來重製資料並進行備份。傳統影印機必須將資料放置在影印機上才能進行重製，並無資料外洩的疑慮。但隨著科技進步，多數的影印機都採數位模式的方式，即先將資料掃描儲存在硬碟裡後再列印，因此資料會儲存在影印機硬碟裡，並按機器的功能及設定，決定資料留存的狀況。

影印機雖然為生活帶來極大的便利，但若使用在影印機密資料，將會有資料外洩的問題。依照營業秘密法第 *2* 條[1]規定，營業秘密必須符合「非一般涉及該類資訊之人所知」、「因其秘密性而具有實際或潛在之經濟價值」及「所有人已採取合理之保密措施」之要件，因此若資料是屬於公司的營業秘密，除其本質須有秘密性及經濟價值外，公司更應該採取合理的保密措施，嚴格控管機密檔案的列印程式，並應於列印後隨即刪除影印機裡儲存的紀錄，避免遭有心人士藉此取得公司營業秘密。

另依照營業秘密法第 *10* 條第 *1* 項第 *1* 款[2]的規定，以不正當方法取得營業秘密者，為侵害營業秘密，而擅自重製即屬於不正當方法[3]，因此若有心人士利用數位影印機會儲存資料之特性而擅自列印資料，將構成侵害營業秘密，若造成營業秘密所有人受到損害，依法需負損害賠償責任。此外，亦可能會構成刑法第 *359* 條[4]無故取得他人電磁紀錄罪，面臨處 *5* 年以下有期徒刑、拘役或科或併科 *20* 萬元以下罰金。

雖然法律對於機密資料均有相關保護的規定，但是企業或民眾若影印機密資料時，均應特別小心謹慎，以避免資料外洩而造成無法預測的損害。

管理 Tips

由於科技的進步，許多設備為了加強其功能與應用，常會增加內部儲存空間，如可批次傳送的傳真機或可 *1* 次列印多份的影印機等，這些改變雖然使得使用的便利性提高，但也帶來新的資安問題，對於這些有內部儲存空間的設備，組織可從以下 *4* 點來加強其控管：*1.* 將設備置於管制區域內，

透過實體的管理，來避免未經授權人員取得資料；*2.* 定期清空內部儲存空間的資料；*3.* 加強外部人員進行維護時的監控；*4.* 在設備進行報廢或移轉時，加強確認其內部儲存空間上資料的清除。

另外如要處理的資料屬於高度敏感資料，則甚至應考慮避免透過該類設備進行處理。

相關標準

A.9.1.2 實體進入控制措施

安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出。

A.9.1.3 保全辦公室、房間及設施

應設計辦公室、房間及設施的實體安全並施行之。

A.9.2.6 設備的安全汰除或再使用

含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫。

---

[1] 營業秘密法第 2 條;「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[2] 營業秘密法第 10 條第 1 項第 1 款:「有左列情形之一者，為侵害營業秘密。一、以不正當方法取得營業秘密者。…」

[3] 營業秘密法第 10 條第 2 項:「前項所稱之不正當方法，係指竊盜、詐欺、脅迫、賄賂、擅自重製、違反保密義務、引誘他人違反其保密義務或其他類似方法。」

[4] 刑法第 359 條:「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

類別：資訊保護

【案號：*S990302*】

補習班惡鬥偷個資 判賠 *1500* 萬

【資料來源：中國時報 *99* 年 *8* 月 *21* 日】

焦點話題

A 美語補習班控告對手 *B* 英語補習班以駭客方式竊取兩萬多筆客戶資料，並提起 *2.4* 億多元的附帶民事賠償。被控的 *B* 補習班負責人甲指示程式設計及網路管理工程師乙、丙利用自己撰寫的程式，駭入 *A* 美語補習班電腦竊取客戶資料、客戶訪談紀錄及相關營業資訊等紀錄。*A* 美語補習班員工亦作證離職員工乙曾知悉其電子郵件信箱帳號及密碼。

雖然被控的 *B* 補習班辯稱其所獲取之資訊僅為 *A* 與客戶間聯繫過程的歷史資料，與一般保險業招攬客戶之推銷、閒聊經過無異，且部分包含「非既有客戶」，應非屬營業秘密的範圍。但法官參考 *A* 提供的廣告費用支出、自行陳報推估的來客成交率等資料後，認為該筆客戶資料利益為 *1200* 萬元。另 *B* 補習班雇用 *A* 補習班離職員工乙，從事互相競爭之美語顧問營業，共同竊取 *A* 補習班營業秘密，屬於典型同業競爭商業間諜模式，惡性重大，判賠懲罰性賠償金 *300* 萬元，合計應賠償 *1500* 萬元。

重點摘要

1. 具有經濟價值的客戶資料屬於營業秘密，受到法律的保護。
2. 故意侵害他人的營業秘密，法院可以在損害額 *3* 倍以內的範圍內酌定損害賠償數額。

法律觀點

近年來補習班競爭激烈，接連發生多起個人資料外洩事件。本案中 *B* 補習班負責人指示先前任職於 *A* 補習班的員工乙，利用乙知悉 *A* 補習班內部資

訊的作業方式，由乙及另一名員工丙共同撰寫程式入侵 *A* 補習班電腦，以取得 *A* 補習班客戶資料及其他營業資料，涉及觸犯刑法妨害電腦使用罪章相關規定，最重可處 *3* 年以下有期徒刑、拘役或科或併科 *10* 萬元以下罰金[1]。

另 *A* 補習班於電腦中建立的客戶資料、客戶訪談紀錄及相關營業等資料，乃是 *A* 補習班花費人力、時間及行銷成本後進行建檔並可用於銷售的資料，且此等資料具有一定經濟價值，且經過 *A* 補習班以密碼保護，已採取合理保護措施，屬於受保護的營業秘密，案例中甲、乙和丙以不正當方法取得 *A* 補習班上開營業秘密，屬於侵害營業秘密的行為[2]，*A* 補習班可以請求損害賠償[3]。本件 *A* 補習班即以廣告費用支出、推估來客成交率等資料，證明該筆客戶資料利益為 *1200* 萬元，且因為 *B* 補習班是故意行為，法院可以判賠損害額以上的賠償，但不可以超過損害額的 *3* 倍，本件法官據此額外判賠 *300* 萬元，*B* 補習班共計應賠償 *1500* 萬元。此案例的行為人不但有刑事責任，且亦須負高額的損害賠償責任，對於以不正當方式竊取商業機密的業者提供相當的借鏡，不可不慎。

管理 Tips

本案例中 *A* 美語補習班應可就以下 *2* 方面再進行探討及加強管理：

1. 加強離職員工管理：在此案例中所提及 *A* 美語補習班之離職員工乙於離職後仍知悉原工作之電子郵件信箱帳號及密碼，致使可利用其權限去取得客戶資料，致使補習班之損失；組織應建立妥善之離調職程序，讓員工與離調職時可立即地移除其實體面權限(如實體門禁進出及識別證等)及邏輯面權限(如系統面及電子郵件等)，以避免員工離調職仍可利用相關權限取得組織重要資訊。
2. 避免不必要之存取管道的開放：在此案例中乙、丙係透過網路駭入 *A* 美語補習班取得客戶資料，組織應可考量重要或敏感之資料，依其使用需求，將存取權限作最小限度之開放，如無需於網路上應用，應避免開放

其網路存取之路徑，如此方可將資料外洩之風險降至最低；另案例中似乎是從電子郵件帳號內取得資料，組織更應仔細衡量資料存放的必要性，如無於網路上使用的必要，應可將資料下載存放於實體隔離的電腦，以降低其外洩的風險與管道。

相關標準

A.8.3.3 存取權限的移除

所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.11.4.5 網路區隔

應將資訊服務、使用者及資訊系統各群組使用的網路加以區隔。

---

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」刑法第 358 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁記錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[2] 營業秘密法第 10 條第 1 款:「有左列情形之一者，為侵害營業秘密。一、以不正當方法取得營業秘密者。…」

[3] 營業秘密法第 13 條：「依前條請求損害賠償時，被害人得依左列各款規定擇一請求：一、依民法第 216 條之規定請求。但被害人不能證明其損害時，得以其使用時依通常情形可得預期之利益，減除被侵害後使用同一營業秘密所得利益之差額，為其所受損害。二、請求侵害人因侵害行為所得之利益。但侵害人不能證明其成本或必要費用時，以其侵害行為所得之全部收入，為其所得利益。依前項規定，侵害行為如屬故意，法院得因被害人之請求，依侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之 3 倍。」

類別：資訊保護

【案號：*S990303*】

惠普與甲骨文 *25* 年情誼恐生變

【資料來源：中時電子報 *99/09/09*】

焦點話題

惠普前執行長在今年 *8* 月，因被控性騷擾連帶扯出帳目不實的醜聞後，遭惠普董事會資遣，並就在前執行長黯然離開惠普 *31* 天之後，即加入甲骨文團隊，不但成為甲骨文管理高層還加入董事會。惠普因不滿甲骨文延攬其前執行長，並恐其執行職務過程時會使用或對外透露惠普的交易機密與其他機密資料，因此對甲骨文提出控告。控告書中指出，由於前執行長加入甲骨文的行為「可能導致惠普客戶、技術、市場優勢及交易機密隨之外流，使公司蒙受莫大損失。」且離職當天亦和惠普簽訂書面約定，表示未來 *2* 年內不得接受與惠普利益衝突的職務安排，並且在其任職至今每年也都均與惠普簽署有保密協定，內容除禁止洩漏惠普機密之外，也禁止搶走公司客戶、員工或供應商。甲骨文執行長艾利森認為，惠普提告一事是踐踏彼此合作關係，也無視自家股東、員工權益，使兩家公司無法繼續合作，完全是出於「報復心態」，揚言公司不惜和惠普斷絕 *25* 年來的合作關係。

重點摘要

1. 基於私法自治和契約自由，以及保護商業機密等競爭優勢需要，原則上雇主均得在與受雇人合意的情況下簽定保密條款，以保護商業機密外洩，受雇人若有違反規定，雇主將可依約求償。
2. 離職員工到競爭對手公司任職的新聞時有所聞，是否有商業機密外洩的問題，仍應以不同個案情形來判斷。

法律觀點

根據憲法第 15 條的規定，人民享有生存、工作及財產的基本權利。但在某些時候為獎勵企業創新和研發商業機密的辛勞，並維護產業倫理和競爭秩序，法律也會明定某些因職務關係而知悉營業秘密的員工，要求遵守在職期間的競業禁止[1]。針對離職員工的競業禁止規範，法律比較少見諸有明文的規範，原因是為保障離職員工的工作權，因此不宜多做規定，只是企業本於維護營業秘密的必要，通常都會和離職員工約定有一定期間內的競業禁止條款，限制離職員工的營業活動或工作範圍。除了一般常見的私人競業禁止約定，公務體系的公務人員也有離職後就業禁止的規範[2]，有稱之為「利益迴避條款」，或稱之為「旋轉門條款」。目的是為避免公務員利用離職前擁有之政府豐富人脈經驗或資源，造成官商勾結等不當利益輸送情事，同時也防止公務員洩漏相關政府業務機密，進而圖謀私人不當利益。

在實務上曾有公務員因離職後立即任職於民營單位擔任顧問，從事與原先職務有直接相關的業務，因此遭法院認定有違反公務員服務法中有關利益迴避條款規定，處以刑責的情形。法院認為該公務員在離職後 3 年即從事與原先職務直接相關的事業，是違反公務員服務法，判處該離職公務員有期徒刑 3 個月[3]。法院指出所謂與原先「職務直接相關」者是：「一、離職前服務機關為各該營利事業之目的事業主管機關，且其職務對各該營利事業具有監督或管理之權責人員，亦即各該營利事業之目的事業主管機關內各級直接承辦相關業務單位之承辦人員、副主管及主管，暨該機關之幕僚長、副首長及首長，各級地方政府亦同；二、離職前服務機關與營利事業有營建或採購業務關係之承辦人員及其各級主管人員。」雖然這樣的規定，在某種程度上限制了公務員離職後的工作權，但如果能證明所從事的業務與原先職務並無直接相關，就不受法律規定的限制。民眾與公務人員都應有離職後競業或轉業禁止規範的認識，以對自身權益有更多一層的了解。

管理 Tips

在本案例中主要係人員管理之議題，組織應適當評估人員面向之風險，如

該員會接觸組織內所定義之機敏性資訊或營業秘密，特別是接觸幅度大或深度高的話，則更應於人員聘僱時即將相關要求明列於聘僱契約中，包含應保密內容或旋轉門條款等，均需於事件發生前即與員工達成協議，一方面要釐清權責，另方面也可讓員工清楚知道其所該擔負之責任。

相關標準

A.8.1.1 角色與責任

員工、承包者及第三方使用者的安全角色與責任，應依照組織的資訊安全政策加以界定與文件化。

A.8.1.3 聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

---

[1] 公司法第 32 條：「經理人不得兼任其他營利事業之經理人，並不得自營或為他人經營同類之業務。但經依第 29 條第 1 項規定之方式同意者，不在此限。」、第 209 條：「董事為自己或他人為屬於公司營業範圍內之行為，應對股東會說明其行為之重要內容並取得其許可。」

[2] 公務員服務法第 14 條之 1：「公務員於其離職後 3 年內，不得擔任與其離職前五年內之職務直接相關之營利事業董事、監察人、經理、執行業務之股東或顧問。」

[3] 公務員服務法第 22 條之 1：「離職公務員違反本法第 14 條之 1 者，處 2 年以下有期徒刑，得併科新台幣 1 百萬元以下罰金。犯前項之罪者，所得之利益沒收之。如全部或一部不能沒收時，追徵其價額。」

四、 刑法

類別：資訊保護

【案號：*S990401*】

刪電腦資料報復 離職會計遭判刑

【資料來源：聯合報 *99/06/29*】

焦點話題

一家生產自行車五金零件公司的離職會計，因不滿離職時公司不給當月薪水，於是偷偷刪除公司電腦內 *180* 多筆營業資料，遭最高法院依「破壞電磁紀錄罪」，判決有罪。

判決書指出，該名會計於任職期間，負責管理公司員工資料、公司帳務、報關資料等電腦資料，離職時，因公司沒付她當月薪水，遂將公司電腦主機內公司的生產資料、產品設計圖片、報關資料、帳目明細及客戶資料等相關電磁紀錄部分或全數刪除，並留下一片「備份資料光碟片」後離職。該名會計則辯稱可能是電腦當機，造成檔案遺失，離職前有將電腦內的資料備份在光碟內，交給老闆娘，不知道為何光碟內沒有她任職期間的電腦檔案。

最高法院依「破壞電磁紀錄罪」，判決該名會計有期徒刑 *4* 個月，減刑為 *2* 個月，得易科罰金，該名會計不想坐牢，就要付出 *6* 萬元代價。

重點摘要

1. 任意刪除他人電腦內的電磁紀錄，導致他人受到損害時，將觸犯刑法妨害電腦使用罪章之破壞電磁紀錄罪。
2. 職務上掌管之文書或電磁紀錄，應於離職時交接清楚並製作交接清單供雙方簽認，以作為舉證證明之用。

法律觀點

所謂電磁紀錄[1]，是指電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄，因此存放在電腦裡的資料，例如文字檔、虛擬寶物等，均屬於刑法規範的電磁紀錄。有鑑於電腦已成為當今日常生活中的重要工具，民眾對電腦之依賴性與日俱增，且電腦常常儲存重要資訊，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人受到重大損害，刑法第 *359* 條[2]即是在防範一般人在沒有正當理由之情況下，取得、變更或刪除他人電腦或其相關設備的電磁紀錄，導致公眾或他人受到損害之情形，一般人若違反前述規定，將面臨 *5* 年以下有期徒刑、拘役或科或併科 *20* 萬元以下罰金。

本案件，公司電腦主機內的生產資料、產品設計圖片、報關資料、帳目明細及客戶資料等相關電磁紀錄，均屬於公司資產且為公司營運的重要資料，被刪除後，將嚴重影響公司營運。該名離職會計不滿公司未給付當月薪水，應透過向當地勞工主管機關申請調解或尋求法律途徑救濟，任意的採取報復手段將公司過去營業、客戶、產品資訊及帳目等資料刪除，顯然是無濟於事的作法，還將觸犯刑法第 *359* 條破壞電磁紀錄罪，以致有牢獄之災上身，且本件雇主針對該名離職會計因刪除資料導致公司營運受到損害的部分，還可以依照民法侵權行為的規定附帶請求損害賠償，不可不慎。

管理 *Tips*

以此案例中應可就以下 *3* 方面討論之：

- 離職程序：在案例中該員工似乎是於離職後確認未收到薪資時，方才進行相關行為，所以組織應可再加強離職員工存取權限的移除，包含實體與系統權限，以避免此類風險的存在。
- 權限的授與：會計應只為應用系統之使用者或管理者，是否應該有刪除如此多資料的權限？組織應遵照最小權限授與原則僅授與員工執行業務所需之權限，以避免此類風險的存在。

- 備份作業：在案例中該員工刪除資料後即無法取回相關資料，顯示了組織對於重要資料並無合宜之備份，一般而言，組織應考量定期將重要資料備份，並保留最近 3 個版本以上，以利發生異常狀況時回復之用。

相關標準

A.8.3.3 存取權限的移除

所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

A.10.5.1 資訊備份

應依據所議定的備份政策，定期進行資訊與軟體的備份與測試。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.11.6.1 資訊存取限制

應根據所界定的存取控制政策，限制使用者與支援人員對資訊與應用系統功能之存取。

---

[1] 刑法第 10 條第 6 項：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄、致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

類別：資訊保護

【案號：*S990402*】

為公司 秘書侵入上司電郵無罪

【資料來源：台灣台北地方法院 *99* 年度易字第 *273* 號判決】

焦點話題

甲○○原擔任 *A* 公司執行副總乙○○的助理，乙○○突然離職並旋即出國，離職前亦未就有關業務移交給相關人員，且公司信箱均已清空，*A* 公司無法與乙○○取得聯繫。甲○○為了解乙○○負責的客戶與 *A* 公司間扣款事宜的進度，想到乙○○平時會使用私人信箱指示業務，並同時會寄送副本到該信箱。甲○○遂以乙先前告知的帳號密碼登入該信箱，尋找關於 *A* 公司客戶扣款之相關郵件往來。法院審理後，認為甲○○是為解決 *A* 公司扣款問題，有正當理由，因此判決甲○○無罪。

重點摘要

1. 若有正當理由而使用他人的帳號密碼進入電子郵件，即非屬無故侵害他人秘密或妨害電腦使用，而不構成刑法上的犯罪。
2. 公司對離職員工應進行完整的交接並備份所有資料，避免重要業務資料遺漏而影響公司業務。

法律觀點

本案例中，甲○○進入乙○○私人信箱，由於私人信箱屬於個人隱私權範圍，將構成窺視他人非公開之言論，且進入信箱須輸入帳號密碼，因此甲○○的行為可能涉嫌刑法第 *315* 條之 *1*[1]妨害秘密罪及第 *358* 條[2]入侵電腦罪，但前開罪名都是以「無故」為要件，亦即若是有正當理由，即不會構成犯罪。

本件案例中乙○○於離職前，因未就先前所處理的事務辦理交接程序，並刪

除公司信箱所有資料，且旋即出國而無法聯繫，致 A 公司無法掌握與客戶間扣款糾紛之處理程序，甲○○乃係在情急之下，始進入乙○○信箱查詢相關資料。法官在審理後，認定甲○○具有正當理由，難認甲○○有侵害乙○○秘密或妨害其電腦使用的犯罪意圖，而判決無罪。惟應注意的是，在此案中 A 公司在與乙○○取得聯繫之前，並無其他方式可以取得乙○○與客戶往來之相關資料，且乙○○在職時確實以該私人信箱指示公司業務並作為備份用途，甲○○亦係以乙○○先前告知之帳號密碼登入，因此要主張具有正當理由，必須盡相當的舉證責任，且應具有急迫及必要性，否則應盡量尋求其他方式處理，以避免有違法疑慮。另外公司對離職員工應進行完整的交接並備份所有資料，避免重要業務資料遺漏而影響公司業務。

管理 *Tips*

在此案例中組織應可考量加強以下 *2* 個面向的管理措施：*1.* 人員任用時，於聘僱契約中清楚說明對於公司所提供資訊資源(如個人電腦、電子郵件或網路磁碟等)的使用權限，可考量清楚規範其使用範圍(公務用途)，以降低日後發生爭議之機會；*2.* 加強人員離調職時的管理，於人員離調職應建立交接清單，並由相關人員(如業務上有互動之人員與主管等)協助檢視其完整性，並依此落實交接，另如有離職契約時更可於其上敘明組織可進行後續處置的權利。

相關標準

A.7.1.3 資產之可被接受的使用

與資訊處理設施相關的資訊與資產，其可被接受的使用之規則應予以識別、文件化及實作。

A.8.1.3 聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.8.3.1 終止責任

執行聘僱終止或變更的責任應明確的界定與指派。

---

[1] 刑法第 315 條之 1：「有下列行為之一者，處 3 年以下有期徒刑、拘役或 3 萬元以下罰金：一 無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二 無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[2] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

類別：資訊保護

【案號：*S990403*】

旅行社員工 盜刷客戶信用卡

【資料來源：自由時報 *99/08/29*】

焦點話題

鐵路警察局高鐵段接獲 *6* 家銀行報案，指稱有多名參加旅行團的持卡人，將信用卡資料傳真予旅行社進行人工刷卡交易後，信用卡隨即遭人盜刷購買高鐵車票，購入的車票全遭歹徒變賣兌現。警方發現，被害人全是參加 *OO* 旅行社的出團遊客，信用卡遭盜刷時間，都發生在回傳旅行社「刷卡確認單」進行人工刷卡交易後，研判應係旅行社內部員工所為，隨即與受害銀行及台灣高鐵公司配合監控。

警方調查後發現，○○旅行社員工甲因負債百餘萬元，於是利用同事對客戶回傳「信用卡交易刷卡確認單」未嚴加控管，輕易拿走相關資料盜刷，並交由乙販售兌現。○○旅行社經警方通知後得知此事，已馬上清查所屬客戶，並解除甲職務；同時全面加強刷卡安全流程，以免再有不肖員工有機可乘的漏洞；也會與銀行協調處理客人盜刷金額，絕對不會讓顧客損失或影響權益。

重點摘要

1. 在未獲得持卡人授權的情況下進行線上刷卡，將構成行使偽造私文書罪及詐欺得利罪。

2. 特約商店若因內部控管程序疏失導致消費者信用卡遭盜刷時，須對消費者負損害賠償責任。

法律觀點

信用卡又稱為塑膠貨幣，乃是現代人用來作為支付工具。由於民眾在進行交易時，未必能夠親自持卡片進行刷卡，因此在民眾填寫刷卡授權書後，特約商店即可憑授權書及上面記載的發卡銀行、卡別、信用卡卡號、有效日期、及卡片背面 *3* 位數授權碼進行刷卡，可以減少民眾須至現場刷卡的麻煩。然而，透過此種方式刷卡，銀行端只驗證輸入卡號及授權碼是否正確，並無法確認每筆消費是否均獲得授權，因此有被盜刷的風險。

本案例中，旅行社因為辦理消費者刷卡繳付團費的事項，所以擁有消費者個人資料及信用卡資訊。但因辦理刷卡的員工未嚴加控管消費者回傳的「信用卡交易刷卡確認單」，導致不法員工甲有機可乘，利用「信用卡交易刷卡確認單」記載的資訊私自上網盜刷購買高鐵車票，致銀行給付刷卡金額予特約商店而受有損害。員工甲明知道其沒有獲得消費者授權，而在網路上進行刷卡，影響發卡銀行對於持卡人刷卡交易管理之正確性、特約商店管理網路線上交易之正確性，將構成行使偽造私文書罪[1]，且因此致銀行陷於錯誤而給付刷卡金額給特約商店，也恐因個案差異而有構成詐欺罪中的詐欺得利罪[2]或不正利用電腦取財罪[3]。至於○○旅行社對於甲的不法行為，應屬未盡到監督管理的義務，導致旅客受有損害，○○旅行社恐須負擔僱用人連帶賠償責任[4]。特約商店對於因為交易關係而取得持卡人的信用卡相關資訊，應該建立嚴格的控管程序，避免因內部員工或不法人士取得後盜刷，影響持卡人權益，除應負損害賠償責任外，更將嚴重影響商譽。

管理 Tips

在本案例中就旅行社的內部控制程序，應可從以下 *2* 個步驟來加強內部控制程序的強度：

1. 辨識組織所持有資料重要性：組織於日常運作常會接觸許多不同重要程度之資料，如：報名時的客戶資料(姓名、電話及地址等)、加保旅保時的客戶資料(姓名、身分證字號及緊急聯絡人等)或付款資料(信用卡交易刷卡確認單上之資料…等)，組織應先瞭解這些資料外洩或控管

不當時可能帶來的風險大小，並依此做為選定控管強度的依據。

2. 依風險大小與類型設計控制措施：組織應於瞭解風險後，依其性質決定控管類型與強度，例如針對信用卡資料，如：外洩或管理不當將導致客戶的金錢損失及客戶對公司的信賴感下降等，即應加強其控管強度，如：重要資料可保存於獨立網路之區段以降低外洩疑慮，而使用上更應該有覆核之機制，以避免資料遭不當的利用。

相關標準

A.7.1.1 資產清冊

應明確識別所有資產，並製作與維持所有重要資產的清冊。

A.7.2.1 分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.11.4.5 網路區隔

應將資訊服務、使用者及資訊系統各群組使用的網路加以區隔。

---

[1] 刑法第 210 條：「偽造、變造私文書，足以生損害於公眾或他人者，處 5 年以下有期徒刑。」、第 216 條：「行使第 210 條至第 215 條之文書者，依偽造、變造文書或登載不實事項或使登載不實事項之規定處斷。」

[2] 刑法第 339 條：「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處 5 年以下有期徒刑、拘役或科或併科 1 千元以下罰金。」

[3] 刑法第 339 條之 3 第 1 項：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處 7 年以下有期徒刑。」

[4] 民法第 188 條：「受僱人因執行職務，不法侵害他人之權利者，由僱用人與行為人連帶負損害賠償責任。但選任受僱人及監督其職務之執行，已盡相當之注意或縱加以相當之注意而仍不免發生損害者，僱用人不負賠償責任。」

類別：資訊保護

【案號：*S990404*】

調查官想減工作量 駭主管電腦遭起訴

【資料來源：聯合晚報 *99/10/04*】

焦點話題

負責監控大陸來台人士在台活動的調查局國家安全維護處第二科調查專員，日前因認為工作沉重心生不滿，所以盜取其上司的密碼，進入主管的電腦，將列管的大陸人士代碼刪除，使失去監控的大陸人士高達 *113* 人。由於兩岸開放直航後，大陸人士來台觀光、探親人數驟增，調查局據點同仁情蒐來台的大陸人士資料變多，依調查局內部偵防流程，據點陳報大陸人士資料後需輸入電腦列管、追蹤，監控一段時日，發現未有異常後，再由據點同仁建議撤銷監控，該專員即為想減輕工作負擔，才出此下策刪除入侵公務電腦，刪除代碼資訊。該行為因為可能已造成國家安全網上的漏洞，所以已遭台北地檢署起訴，並交由法院審理當中，而調查局公共事務室主任說，待全案刑事責任確定後，還會針對其個人行為做出行政懲處。

重點摘要

1. 竊取他人帳號密碼並入侵電腦，進而刪除他人電腦內的紀錄內容，造成損害，須負刑事責任。
2. 公務機關的電腦資料具有公益性質，一旦被入侵或資料被刪除，在量刑上，除造成公務機關損害也損及公益而有加重行為人刑度 *1/2*。

法律觀點

本案中的調查局專員，先是利用竊取上司電腦的帳號與密碼方式，輸入指令進入上司電腦，再依此瀏覽管理系統內的資訊，找尋欲刪除的檔案後點

選註記刪除。因此該專員的行為已屬違法，應無疑問。

首先，無故輸入上司帳號密碼進入電腦管理系統的行為，是刑法妨害電腦使用罪的典型行為，依法可對未經他人同意而侵入他人電腦或其相關設備的犯罪行為人，處 *3* 年以下有期徒刑或併科 *10* 萬元以下罰金[1]。這類行為欲保護是對電腦使用的權限，因為電腦系統一旦遭到他人惡意入侵之後，通常需要再耗費更高的人力與時間去做修復或確保電腦安全系統的安全，所以一旦有人利用不法的方式，輸入他人帳號密碼進入電腦，不需要有任何的資訊被竊取或觀看，也會觸法。

案例中的專員因不滿工作內容需監管眾多大陸人士，為減輕壓力而私自刪除代碼資訊，這樣的行為已構成了無故刪除他人電腦之電磁紀錄罪，最重可處 *5* 年以下的有期徒刑或併科 *20* 萬元的罰金[2]。類似常見的情況還有像離職員工因不滿被公司解雇而入侵公司電腦刪除重要商業資訊或公司檔案，這些都是由於機構內部對自身員工接觸資訊的管理疏漏所造成，因此有關單位對機關職員或雇員的資訊防範都應有更嚴密的控管作業程序，例如建立內部資訊異常刪除紀錄的警示提醒和定期帳密資料的更換，以避免因內部人員的不法行為而造成資安疑慮。同時，如果入侵電腦或刪除的是公務機關所屬的電腦紀錄，則因涉及公務機關的資訊安全，刑法上有特別加重處罰的規定，可加重其刑至二分之一[3]，所以本案中的調查局專員，因一時思慮不周為減輕工作所犯下的罪刑，不僅可能會讓他吃上妨害公務機關之電腦使用罪的官司，還得遭受內部行政懲處的裁罰，甚至影響將來升遷與考績檢核的評分，實在得不償失。

管理 Tips

在本案例中主要發生的問題係因個人帳號/密碼的使用與保存失當：在案例中該員盜取了上司的密碼，導致後續違法事項的發生。因應這樣的事件，組織中應對於成員帳號/密碼(主要為密碼)的設定或保存，應有適當訂定明確的責任定義(如密碼應英數字混合、長度、更改週期及妥善保護)，並將

相關權責適當地透過宣導或教育訓練告知並要求成員遵守。

相關標準

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.11.3.1 通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

---

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[3] 刑法第 361 條：「對於公務機關之電腦或其相關設備犯前 3 條之罪者，加重其刑至二分之一。」

類別：資訊保護

【案號：*S990405*】

駭客土法煉鋼 *1* 年半破解 *1* 密碼

【資料來源：聯合報 *99/10/13*】

焦點話題

桃園縣一名顏姓男子和人合夥經營餐廳，因不滿餐廳經營不到半年即關門倒閉，懷疑合夥人盧姓女子吞了他的錢，憤而告對方侵占；為打贏官司該名男子上網搜尋盧女姓名，查出對方在不同網站所留下的電子信箱與住址，再用生日、身分證字號、電話、門牌、英文名字與縮寫等排列組合近廿萬筆密碼，花了 *1* 年 *6* 個月，終於以盧女的車牌號碼猜對密碼，「駭」進盧女電子信箱尋找證據，出庭時不僅能清楚說出對方每筆資金流向，分毫不差，盧女懷疑顏姓男子找徵信社違法調查她，向警方報案。該名男子坦承因不甘砸下百萬元投資的血汗錢一去無回，所以才會想盡辦法花很多時間「猜」盧女的電子信箱密碼，並竊取對方機密資料。警方表示該名男子其實對電腦並不內行，為打贏官司竟排列組合廿萬筆可能的密碼，可謂是「土法煉鋼的另類駭客」，偵訊之後已依妨害電腦使用罪將他函送。

重點摘要

1. 帳號密碼設定，應盡量避免使用生日、身分證字號、電話、車牌等容易得知之個人資訊，以避免輕易被人猜出。
2. 侵入他人信箱查看他人信箱訊息，不僅會有刑事責任，也會有侵犯個人隱私的問題。

法律觀點

電子郵件信箱已成為現代人日常溝通往來的主要方式之一，電子郵件可以

即時傳遞給對方，並可留存作為往來紀錄的證據，因此電子郵件內容常常會涉及重要業務資料或個人社交活動的隱私資料，一旦發生電子郵件帳號遭人入侵時，帳號內留存之資料就有可能會被外洩或竊取。

一般常見駭客入侵方式，多是利用電腦程式入侵他人電子郵件帳號。但案例中的顏姓男子即透過土法煉鋼的方式，藉由排列受害人生日、身分證字號、電話、門牌、車牌、英文名字與縮寫，最後終於在歷時 *1* 年 *6* 個月的時間，猜出受害人信箱密碼，並登入後取得訴訟所需的資金流向。顏姓男子雖然沒有使用電腦程式，但仍然構成犯罪。顏姓男子輸入受害人電子郵件信箱的帳號密碼，乃觸犯刑法第 *358* 條無故入侵他人電腦罪[1]。進入信箱後取得電子郵件，將構成無故取得電磁紀錄罪[2]。並且除了上述的刑事責任外，被害人還另可依民法的相關規定[3]請求因隱私權被侵害的損害賠償。

由此案例可知，在設定任何帳號密碼時，應該盡量避免使用與個人資料有關之資訊，更應避免有「一碼通用」或「萬年密碼」的情況，以免身邊的人輕易猜測出帳號密碼而竊取相關個人資料。

管理 *Tips*

因密碼複雜度低或為追求方便，而將密碼抄寫在易被看見的地方，導致密碼被破解或機密資料外洩的案例在現今社會層出不窮。組織或個人在設定密碼時，應避免使用容易被猜測出的顯性密碼或多帳號使用同樣一組密碼，並且定期更換密碼，以降低被盜取或破解的風險。電子郵件服務提供者應記錄輸入密碼錯誤次數、時間及網路位址等，並應以適當方式通知或提醒使用者。

相關標準

A.10.10.5 失誤存錄

失誤應予以存錄、分析，並採取適當措施。

A.11.3.1 通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[3] 民法第 18 條：「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。前項情形，以法律有特別規定者為限，得請求損害賠償或慰撫金。」第 195 條第 1 項：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

類別：資訊保護

【案號：*S990406*】

釣魚網站猖獗 較上月增五成

【資料來源：中廣新聞網 *99/10/19*】

焦點話題

越來越多的釣魚網站幾可亂真，就連國外知名社群網站，也難逃為駭客偽裝的目標，目的就是想要竊取使用者的資料。日前有資安業者公布最新一期的垃圾郵件及網路釣魚網站統計報告，報告內表示，釣魚網站依舊猖獗，光是九月分就成長達 *52%*，主要原因與不斷出現一些特殊的釣魚網站，以及自動化製作工具持續增加的原因有關。這些釣魚網站的製作，兼及有很多自動化工具，這些自動化工具跟釣魚網站結合後，便會大量製作出假網站來欺騙使用者，當使用者點選這些網站時，網站可能就會收集使用者的資料，或是把惡意連結藏在部分垃圾郵件裡。雖然報告內亦表示，垃圾郵件的濫發情形已呈現下降趨勢，但其他的網路資訊安全威脅依然存在，網友不要任意開啟來路不明的檔案與連結，定期更新安全軟體病毒定義檔，以防範病毒威脅。

重點摘要

1. 利用釣魚網站進行不法行為，將構成刑事犯罪，並受到相關法律的制裁。

2. 在網路輸入帳號密碼或提供個人資料時，應特別注意其網站或電子郵件來源，以避免資料外洩而造成損害。

法律觀點

所謂釣魚網站是仿冒知名網站，使一般民眾誤信而點選進入網頁頁面。犯罪手法大致可以分成兩類，一種是仿冒知名網站之頁面，利用不知情的使

用者登入輸入帳戶密碼後，記錄使用者輸入之資料，其後利用取得資料進行不法行為。另一種是使用者進入釣魚網站後，即會自動下載木馬程式或啟動遠端遙控程式，且安裝至使用者電腦，此時使用者電腦裡的資料，除將遭到竊取外，更可能成為駭客攻擊他人的跳板，使受害人不計其數。

釣魚網站乃偽裝成知名網站，網頁依照刑法第 *220* 條 *2* 項之規定屬於準文書[1]，因製作人非有權製作之人，按照偽造內容是否屬於公務員職權上製作之文書，將可能構成偽造私文書罪[2]或偽造公文書罪[3]。此種釣魚網站會誘騙使用者輸入帳號密碼，記錄其輸入之資料，再以其帳號密碼登入後修改密碼，讓使用者無法登入，以便之後利用該帳號進行不法行為，例如假拍賣，致使其他網友受騙而受有財產上的損害。另外，釣魚網站可能還會要求使用者提供銀行帳戶或信用卡資料，再利用取得資料進行交易或惡意行為，讓使用者受到損害或誘使銀行誤以為是真實交易而支付金錢。輸入他人帳號密碼的行為，將構成刑法第 *358* 條入侵電腦罪[4]，若進一步竄改密碼，則會構成刑法第 *359* 條無故取得或變更電磁紀錄罪[5]。至於利用使用者帳號進行假拍賣或利用銀行資料進行交易，將分別構成刑法第 *339* 條詐欺罪[6]或第 *339* 條之 *3* 違法製作財產權罪[7]。若植入木馬或惡意程式之釣魚網站，將涉及刑法第 *360* 條干擾電腦罪[8]，利用此等惡意程式取得使用者電腦資料時，亦將構成刑法第 *359* 條。

雖然法律對於釣魚網站涉及的犯罪行為均有相關刑責可以制裁。可是一旦帳號密碼遭到不法人士的利用，則損害即可能會發生。因此，在網路上輸入帳號密碼並提供個人資料時，應特別注意網站來源，並不要任意點選不明來源的連結，以避免成為下一個受害人。

管理 Tips

釣魚網站最常見的手法不外乎是將惡意程式或假冒網頁之連結隱藏於合法網頁中、電子郵件超連結，或利用搜尋引擎讓使用者無意間進入假冒網頁等，一旦使用者點選連結，即可能在不自覺的情況下被植入病毒或個資外

洩。避免網路釣魚的方法有下列幾種，例如不亂點信件或網頁中的連結，若要造訪網站，可於瀏覽器中自行輸入網址；或不點選瀏覽網頁時，彈出廣告中的任何按鈕等。辨識釣魚網站其中一種方法為依靠使用者本身的警覺心，例如檢視超連結的內容，確認連結網址是否導向欲前往之網頁；除依靠使用者警覺心外，目前有些瀏覽器內建有網路釣魚篩選工具，或瀏覽防護功能，在使用者造訪疑似釣魚網站之前，對使用者發出警告訊息。除此之外網路服務提供者應適當地對使用者進行教育及宣導，加強使用者辨識釣魚網站的能力，以降低網路攻擊成功機率。

相關標準

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.4.1 對抗惡意碼的控制措施

應實作防範惡意碼的偵測、預防及復原控制措施以及適切的使用者認知程序。

---

[1] 刑法第 220 條第 2 項：「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」

[2] 刑法第 210 條：「偽造、變造私文書，足以生損害於公眾或他人者，處 5 年以下有期徒刑。」

[3] 刑法第 211 條：「偽造、變造公文書，足以生損害於公眾或他人者，處 1 年以上 7 年以下有期徒刑。」

[4] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[5] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[6] 刑法第 339 條：「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處 5 年以下有期徒刑、拘役或科或併科 1 千元以下罰金。」

[7] 刑法第 339 條之 3 第 1 項：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處 7 年以下有期徒刑。」

[8] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

類別：資訊保護

【案號：*S990407*】

男子分享平台下載軍方資料被求刑

【資料來源：中廣新聞網 *99/11/14*】

焦點話題

一名男子從 *FOXY* 網站分享平台發現陸軍作戰、防禦計畫等檔案，因為剛剛退伍，對軍事消息充滿興趣，所以下載了二十件檔案，包括陸軍砲指部資料、作戰防禦計畫等，而這些檔案當中，有部分資料尚未解密。高雄市調處在網路上意外發現該起事件，報請檢察官偵辦，對於這些資料如何流出，軍方還在瞭解。地檢署偵辦後依「外患罪」起訴該名男子，求處 *8* 個月徒刑，因為沒有造成損害，所以建議法院緩刑。

重點摘要

1. 下載國防應秘密資料，可能會構成蒐集國防秘密罪，將面臨 *5* 年以下有期徒刑的刑事責任。

2. 使用網路分享網站，可能會遭植入木馬程式，而使機密資料外洩或毀損，因此從事網路行為必須小心謹慎。

法律觀點

FOXY 分享網站是利用 *P2P* 方式進行資料分享，使用者在網路上搜尋到想要的檔案時，可直接從他人電腦開放分享的資料夾下載檔案，造福使用者能夠快速且方便的分享檔案。但此技術經常成為侵害著作權的工具，使用者更常因為在下載時遭有心人士植入木馬程式，導致使用者電腦裡的檔案變成公開資料夾，使機密資料一覽無遺，國內有多起機密資料外洩事件，即是肇因於 *P2P* 軟體。

本案例中的男子透過 *FOXY* 下載陸軍砲指部資料、作戰防禦計畫，由於部分資料尚未解密，應屬於刑法第 *109* 條「中華民國國防應秘密之文書、圖畫、消息或物品」，因此該名男子在網路上蒐集及下載檔案資料的行為，屬於蒐集國防秘密，依照刑法第 *111*[1]條的規定，可能會面臨 *5* 年以下有期徒刑的刑事責任。至於本案例機密資料外洩原因雖然不明，但洩漏的來源應為公務員，一旦被查獲，會因為其主觀上是故意或過失，分別構成刑法第 *109* 條第 *1* 項[2]及第 *110* 條[3]的罪責。

網路資料分享固然可以達到資料流通的目的，但是不當下載檔案不但可能構成犯罪，亦可能無意間被植入木馬程式而導致機密資料外洩或被毀損，因此在從事網路行為時，應特別小心謹慎，以免不慎觸法。

管理 *Tips*

本案例可就以下 *2* 方面討論之：

- 對使用者：應需針對其行為，清楚地辨識其所需遵循的法令法規。於分享平台下載資料前，應謹慎思考下載之行為及所下載之資料是否有觸法之疑慮。
- 對軍事單位：此案例主要發生原因係為組織對於資料之管控不確實，致機敏資料被未經授權的揭露。組織應透過教育訓練及宣導，讓組織內人員於處理機敏資料時更加謹慎，並應建立資料保護機制，避免此類資料被未經授權的揭露。組織可透過系統監視及相關存取活動紀錄，以期降低資料外洩之可能性，及釐清相關責任歸屬。另也可於相關文件上適當標示警語，讓不知情之人員拾獲或取得時可立即回報，以將損害降至最低。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作

職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.7.3 資訊處置程序

應建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用。

A.10.10.2 監控系統的使用

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A.10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

---

[1] 刑法第 111 條：「刺探或收集第一百零九條第一項之文書、圖畫、消息或物品者，處 5 年以下有期徒刑。」

[2] 刑法第 109 條第 1 項：「洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處 1 年以上 7 年以下有期徒刑。」

[3] 刑法第 110 條：「公務員對於職務上知悉或持有前條第一項之文書、圖畫、消息或物品，因過失而洩漏或交付者，處 2 年以下有期徒刑、拘役或 1 千元以下罰金。」

五、 醫師法

類別：資訊保護

【案號：*S990501*】

公布他人病歷 醫師行政訴訟敗訴

【資料來源：台北高等行政法院 *98* 年度訴更一字第 *142* 號判決】

焦點話題

原告是執業醫師並擔任台中市診所協會理事長，於 *94* 年 *11* 月 *29* 日在台中市議會，以醫師身分參加由「台中醫界聯盟」就署名胡○○之病歷記者會，與 *11* 名醫師並坐一排，會場桌上並立有原告等各醫師頭銜，同時由陳○○醫師主持會議，介紹原告之身分。記者會現場並張貼有「胡○○健康問題爭議」、「病歷表解析」等海報，署名胡○○之病歷自始均放置在林○○醫師桌面，並由林○○持病歷向媒體解說，與會記者以長鏡頭從遠處拍攝放大該病歷資料，記者會歷時 *21* 分鐘，由立委和其他多名醫師評論分析胡○○之病歷，原告未在記者會陳述意見。事後原告遭醫師懲戒委員會以其違反醫師法規定而懲處警告並命接受 *8* 小時之醫學倫理繼續教育。

原告主張其是以人民團體理事長身分受邀，非以醫師身分出席，事前不知道記者會要公布胡○○病歷，記者會僅在場旁觀，並未持有病歷或公開病歷，且醫師法第 *25* 條第 *4* 款[1]應限於執行醫療業務之行為，因而提起訴訟。

台北高等行政法院認為，原告身為醫師，於記者會時親臨現場，且在林○○及其他醫師評論、分析胡○○病歷、記者拍攝病歷時，均未為任何制止或異議表示，顯然是以 *12* 醫師團體方式進行公開他人病歷資料行為，有執行業務違背醫學倫理之違法，於是駁回原告之訴訟。

重點摘要

1. 病歷資料屬於病人隱私權核心領域，在其他醫師公然揭露病人的病歷資料時在場而當場未制止或異議，即屬於侵害病人隱私權的共同行為人。

2. 醫師對外所顯現與專業印象或專業能力有關的事務，即屬其執行業務的範圍，須遵循醫師倫理規範。

法律觀點

本件判決認為尊重病人隱私權乃所有醫生應有社會責任，也是醫師倫理規範明定規定，身為醫師既然不可以主動洩漏病人之病歷資料，在他人有洩漏病人之病歷資料時，當然也不可以有幫助或在旁助勢之舉，否則即與倫理規範要求的不符。再者，病人就診資料事涉個人私密事項，若任意外洩，對個人之名譽及社會活動皆有重大之影響，因此對個人就診資料之保密，乃病人隱私權核心領域，亦是醫病關係中，病人可以信賴醫師之基礎；若醫病關係不存有醫療資訊隱私或機密性之保護，病人將因為不信任醫師，而拒絕透露完整且必要之個人資訊，或拒絕接受必要之檢驗、治療，其結果除造成醫療資源浪費，並將影響正確診斷與治療之進行，甚至瓦解醫病關係之存續，結果反將有害大眾健康之維護，亦不利於整體社會之福祉。因此，解釋醫師法第 25 條之「執行業務」是否違背醫學倫理時，即應在符合醫師倫理規範制訂之目的範圍內進行解釋。

判決認定原告是經過受邀醫師於電話中說明後，才決定參加記者會，且記者會在客觀上亦讓社會大眾認為是 12 名醫師共同召開記者會，因此是以醫師身分參加記者會。且原告在其他醫師持特定病患病歷，面向媒體解說，記者以長鏡頭從遠處拍攝放大該病歷資料，以及其他醫師當場評論、分析該病歷，原告未為任何制止或異議，原告屬於共同行為人，醫師懲戒委員會之懲處自屬有據，並判決原告敗訴。

醫療屬於敏感性資料，若洩露會對當事人造成不可回復之損害，因此新修正「個人資料保護法」(以下簡稱新版個資法)第 6 條[2]即規定醫療、基因、

性生活、健康檢查及犯罪前科等具敏感性的個人資料，原則上不得蒐集、處理或利用。因此，未來醫療院所及從業人員對於醫療及健康檢查資料之使用及管理，必須特別注意，以避免違反新版個資法之規定而被追究相關法律責任。

管理 *Tips*

在此案例中法令已有明確地規定病歷內容屬於應保密的範圍，所以就管理面而言，組織應在初期便對其人員可能接觸的所有資料進行機密等級之判定，尤其針對受法令規範部分，並將判定結果清楚宣達予所有可能接觸資料的人員，使所有人員瞭解其所應擔負之責任；另在案例中有提及實體病歷出現於記者會中的部分，組織應可就實體文件的保存再行加強。

相關標準

A.4.3.2 文件管制

(h) 確保文件分發受管制

A.7.2.1 分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

[1] 醫師法第 25 條第 4 款：「醫師有下列行為情事之一者，由醫師公會或主管機關移付懲戒：...四、執行業務違背醫學倫理。」

[2] 個人資料保護法第 6 條：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定者。
二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。
前項第四款之個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。」

貳、 資訊公開（*Disclosure*）

一、檔案法

類別：資訊公開

【案號：*D990201*】

申請閱覽卷宗 需先有行政程序存在

【資料來源：最高行政法院 *99* 年度判字第 *476* 號判決】

焦點話題

甲約於 *87* 年 *8* 月因病於 *A* 醫院所屬復健中心住院治療，卻遭同房病患乙攻擊，以致腦部受傷成殘，並經法院裁定宣告為禁治產人。甲之法定代理人丙以 *A* 醫院所屬人員在管理病患上有過失及怠忽職務之情事，因此擬請求國家賠償，經最高法院判決敗訴。嗣後丙主張為訴訟之需要，向 *A* 醫院請求閱覽復健病房之工友值班及開放病床數等資料。*A* 醫院認於法不合，而予以否准。甲不服提起訴願及行政訴訟，最高行政法院審理後，認依行政程序法聲請閱覽卷宗需有先行之行政程序，不得僅以訴訟所需為由申請。事發當時檔案法尚未公布施行，因此 *A* 醫院當時並無歸檔管理之義務。又不論依照檔案法或行政程序法請求閱覽檔案，均須以檔案與卷宗存在為前提，*A* 醫院業已銷毀檔案，亦無法提供，因此駁回丙的上訴。

重點摘要

1. 依行政程序法申請閱覽卷宗必須有先行的行政程序存在，如只是基於訴訟需要，即無法申請。
2. 依行政程序法或檔案法申請閱覽卷宗，均是以檔案存在為前提，若行政機關於法定保存期間過後銷毀檔案，並不違法。

法律觀點

本案例中，丙是以行政程序法第 *46* 條[1]及檔案法第 *17* 條[2]之規定，作為向 *A*

醫院申請閱覽卷宗之基礎。最高行政法院認為行政程序法第 46 條規定之申請閱覽卷宗請求權，係指特定之行政程序中之當事人或利害關係人，為主張或維護其法律上之利益必要，有向行政機關申請閱覽、抄寫、複印或攝影有關資料或卷宗之權利，該種資料提供之對象，並非一般大眾，僅限於行政程序中之當事人或利害關係人[3]。因此，申請閱覽卷宗必須有先行的行政程序存在並具備當事人或利害關係人之資格，若僅係為訴訟需求，即於法不合。再者，事件發生時為 87 年 8 月間，檔案法是在 91 年 1 月 1 日開始施行，因此 A 醫院並無從依檔案法歸檔及管理。又不論是以行政程序法或以檔案法請求，均應以檔案卷宗存在為前提。丙請求之資料，依證人證述均已銷毀，事實上已不能閱覽。93 年 4 月 28 日修正後醫療法第 67 條第 2 項第 3 款，雖規定病歷包括「其他各類醫事人員執行業務所製作之紀錄」，惟同法第 70 條第 1 項病歷保存期限為 7 年[4]，丙申請閱覽資料時，距離案發當時已逾 7 年，因此縱使 A 醫院銷毀資料並不違法。最高行政法院基於上述理由，駁回丙的上訴。

人民依法有知的權利，因此行政程序法及檔案法均賦予人民閱覽卷宗之權利，94 年 12 月 28 日公布的政府資訊公開法更將人民知的權利具體落實至相關規定。但人民在請求閱覽卷宗的同時，除應符合法定程序外，更應注意檔案保存時效，避免因為檔案銷毀而無法閱覽。

管理 *Tips*

在本案例中之申請人應辨識並考量相關法律、法令的規範、申請程序及申請要件等。案例中之申請人對於申請閱覽卷宗規定的對象及申請需求無清楚概念，政府機關對民眾應有適當的宣導及解說，使民眾了解其所依循之法律。

相關標準

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

---

[1] 行政程序法第 46 條：「當事人或利害關係人得向行政機關申請閱覽、抄寫、複印或攝影有關資料或卷宗。但以主張或維護其法律上利益有必要者為限。」

[2] 檔案法第 17 條：「申請閱覽、抄錄或複製檔案，應以書面敘明理由為之，各機關非有法律依據不得拒絕。」

[3] 行政程序法第 20 條：「本法所稱之當事人如下：一、申請人及申請人之相對人。二、行政機關所為行政處分之相對人。三、與行政機關締結行政契約之相對人。 四、行政機關實施行政指導之相對人。五、對行政機關陳情之人。六、其他依本法規定參加行政程序之人。」

[4] 醫療法第 70 條：「醫療機構之病歷，應指定適當場所及人員保管，並至少保存 7 年。但未成年者之病歷，至少應保存至其成年後 7 年；人體試驗之病歷，應永久保存。」

參、 資訊監察（*Monitors*）

一、通訊保障及監察法

類別：資訊監察

【案號：*M990101*】

美國法院判決非法 *GPS* 追蹤違憲

【資料來源：法新社華盛頓 *99/08/07*】

焦點話題

美國聯邦上訴法庭裁定，警方不得在未獲許可情況下，利用全球定位系統（*GPS*）科技追蹤嫌犯。華盛頓聯邦上訴法庭駁回被告瓊斯（*Antoine Jones*）在 *2008* 的有罪判決。法院表示警方在未經許可之情況下，在被告車上安裝衛星導航裝置以追蹤其行蹤的行為，侵害被告在憲法上的權利。判決書中陳述：「路人看見甚至追隨某人上市場或下班返家的單一行程是一回事。但一個陌生人抓到線索，第二天起，第三天，一週又一週的跟蹤獵物，直到掌握獵物所有見過的人、去過的地方、所作娛樂、雜務等一切私人日常生活瑣事，則完全是另一回事。」因此法官們認為利用全 *GPS* 追蹤，違反憲法第四修正案對免受無理搜索、扣押權的保護，屬「侵犯私人領域」的行為。

重點摘要

1. *GPS* 可以追蹤當事人位置，並進而推知其從事的活動，侵害隱私權甚鉅。
2. 立法院研擬將 *GPS* 明文納入「通訊保障及監察法」的適用範圍，以在合法偵查及保障人權間取得平衡。

法律觀點

隨著科技越來越進步，追蹤犯人手法日新月異，有些新型態手機或 *PDA* 應用功能，甚至還提供能讓人利用電話追蹤他人實際所在地點的功能。這類

的全球定位系統(*Global Positioning System*，簡稱 *GPS*)可以追查到個人的行蹤，但同時也會侵害到個人隱私權，因此如何在公眾利益及隱私權保護間取得平衡，將是法院判決過程會遇到的一大課題。

本案例乃是涉及行動偵搜，即透過 *GPS* 追蹤犯罪嫌疑人的位置，若 *GPS* 具有同步收音功能，固屬於「通訊保障及監察法」的通訊監察，但若只是單純的定位功能，是否應受到「通訊保障及監察法」的規範，則有探討空間。依「通訊保障及監察法」第 *3* 條第 *1* 項第 *1* 款的規定，通訊包括「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信」之情況，此定義並未明文排除 *GPS* 的適用，因此檢調單位若擬以 *GPS* 追查犯罪嫌疑人所在位置，是否須依「通訊保障及監察法」相關規定申請通訊監察書，尚有待實際個案認定。但裝設 *GPS* 追蹤犯罪嫌疑人位置，能進而推知犯罪嫌疑人從事的活動，將嚴重侵害個人隱私權，因此立法院研擬朝向明文修法將 *GPS* 納入「通訊保障及監察法」的規範範圍內[1]，以在合法偵查及人權保障之間取得平衡。

管理 *Tips*

在此案例中就組織(警方)應在其採用新科技或執行業務手法前，即針對所可能面臨的法律議題進行探討，確認其採用的合法性，以避免發生違法的情形；另組織也應定期針對適用之法令重新進行檢視，以避免因法令修改而導致的不合時宜。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護

與隱私。

[1] 參考法院第 7 屆第 4 會期司法及法制委員會第 34 次全體委員會議紀錄。

類別：資訊監察

【案號：*M990102*】

竊聽女秘書電話 董座判賠

【資料來源：中國時報 *99/12/03*】

焦點話題

某上市公司董事長甲，懷疑他的女秘書乙，經常在半夜帶人進辦公室、電話費過高等「行徑可疑」，以「安全維護」為由，派人在乙的辦公室電話裝竊聽設備，連續監控乙電話 *3* 個多月。乙發現後，指控甲侵犯隱私權請求賠償。高院審理後認為，員工執勤仍應保有隱私權，判決甲應賠乙 *35* 萬元確定。

重點摘要

1. 員工在職場上的行為，仍應有合理的隱私權期待，除非雇主明確宣示監控，或得到員工同意，否則雇主對員工的通訊進行監控，恐有違法之虞。
2. 雇主監控員工的電話通話內容，除應負民事損害賠償責任外，亦可能會違反通訊保障及監察法。

法律觀點

本案例中，甲涉嫌在乙的辦公室裝設竊聽設備，連續監控乙長達 *3* 個月，乙發現後，以隱私權被侵害為由，向甲請求損害賠償。甲雖然主張其是基於僱傭關係提供並負擔電話之費用，各種聯繫設備所進行之談話溝通內容，均屬履行職務且與公司事務有關，非屬個人隱私而不具秘密性。再者，電話位置屬於公開之辦公區域，並非獨立辦公室，亦未有門窗獨立區隔，任何同事均可輕易聽聞其談話內容，乙的通話內容不具有秘密性。復因為乙女形跡可疑，為維護公司利益而有必要進行調查等理由抗辯。但法院審

理後[1]，認為職場固為公開的場所，業主提供員工使用之通訊設備，員工固應限於履行與職務相關事務，但員工仍享有期待和同事或其他私人談話不會被秘密錄音、錄影及播送之隱私合理期待，保有以私密方式履行其職務之權利，縱使員工撥打電話應該全部使用於公務，亦不得謂員工於職場之行為全無秘密通訊之權利，除非業主事先明確宣示告知員工採取監控，或得到員工明示、默示同意，才可以進行監聽、監視、錄音或錄影，因此認定甲應賠償乙 *35* 萬元。

此案例中，甲除應負損害賠償責任外，因為其涉及長期監聽乙的電話，亦可能會違反通訊保障及監察法第 *24* 條第 *1* 項[2]規定，可能會面臨 *5* 年以下有期徒刑的刑責。因此，雇主基於保護公司利益，雖然必須對員工進行必要的管理，但管理方式必須注意程序是否適法，以免過度侵害員工權利而須承擔法律責任。

管理 *Tips*

組織如有需要對員工進行任何監視，應於員工到職時或年度宣導時即於聘僱契約上或相關文件上告知員工相關情況，如本案例中之組織應在其裝設竊聽設備前，即針對所可能面臨的法律議題進行探討，清楚辨識其所需遵循的法令法規，以及所需擔負之法律責任，進而確認其行為的合法性，並適當知會員工，以避免違反相關法規及侵害他人隱私。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護

與隱私。

[1] 參照台灣高等法院 99 年度上易字第 959 號判決。

[2] 通訊保障及監察法第 24 條第 1 項：「違法監察他人通訊者，處 5 年以下有期徒刑。」

肆、 資訊應用（*Application*）

一、電子簽章法

類別：資訊應用

【案號：*A990101*】

統一發票無紙化 未來存晶片卡內

【資料來源：聯合報 *99/06/01*】

焦點話題

財政部長李述德表示，政府積極推動電子發票，研擬以後民眾消費只要用內含晶片的支付工具刷一下，不需收集紙本發票，政府還會自動幫消費者對獎。財稅官員表示，以電子發票取代紙本發票的構想，目前還在研議階段，正與連鎖超商洽談合作，最快會在 *7*、*8* 月間試辦，看試辦結果再決定未來推動方向。李述德說，每年統一發票印製 *70* 億張，交易金額 *33* 兆元，財政部決定推動發票電子化，以類似雲端運算技術進行，達到便民和節能減碳的目的。初步構想是希望讓民眾以手錶、手機、悠遊卡等內建晶片或無線射頻辨識系統（*RFID*）等工具，購物時只要碰觸一下收銀機，消費明細和發票號碼等資訊即會上傳財政部財稅資料中心的資料庫，民眾不用收集發票，業者也省去印製發票的成本。民眾如果想將發票捐贈公益團體，只要告訴店員，店員就會將發票轉給相關公益團體。不過，目前還有複雜的資訊系統要克服，短期內不可能全面上線，每台收銀機亦必須有上傳資料的功能，業者必須修改系統，一旦全國發票電子化後，每年最高可省下 *1200* 億元。

重點摘要

1. 透過電子簽章，可以確保電子發票的完整性，並符合法律的書面要件。

2. 使用電子發票，應徵得相對人同意使用，始得以避免數位落差。

法律觀點

根據 *NII* 產業發展協會的統計，單就 *2004* 年國內三家知名電子商務業者所開立的發票數量高達 *632* 萬張以上，每年花費在發票的寄送與處理成本可達新台幣 *1* 億 *8* 千 *960* 萬元以上，金額相當可觀。由於有些電子商務產品可以從網路上直接下載或取得，例如線上音樂或遊戲點數，未必會有實際產品的寄送，且常屬小額消費，電子商務業者為處理及寄送電子發票所花費之費用往往高於產品價格，因此電子發票實施作業要點第 *18* 點[1]即規定經申請核准之營業人，在銷售貨物或勞務給一般消費者時得使用電子發票。但消費者還是可以向營業人請求寄送紙本發票，且營業人必須通知中獎發票的消費者，並將紙本發票收執聯以掛號方式寄給中獎人進行領獎，因此現行對一般消費者開立電子發票，尚未達到全面無紙化。

財政部目前規劃對一般消費者開立的電子發票，乃朝向全面無紙化的目標邁進，惟應注意確保電子發票內容不會遭到竄改。依照電子簽章法第 *4* 條規定：「依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。」因此透過例如工商憑證進行電子簽章，可使電子文件內容呈現，並可供日後取出查驗，電子發票符合前述規定，即等同於書面文件，且透過電子簽章，亦可以防止內容遭到竄改。隨著現今載具日益多元化，利用 *RFID* 晶片可以儲存或連結發票號碼或消費資訊，營業人將發票資料上傳至財政部電子發票整合服務平台後，消費者即可隨時查詢電子發票資料，且可透過系統完成對獎，不需要逐一對獎，可以節省紙張及整理的時間成本，對一般消費者和社會整體來說，實為一大福音，應盡量響應。

管理 Tips

電子發票的使用是跨單位的資料交換機制與系統整合方可達成的應用，所以在實作面，除可藉由憑證的使用來確保文件的效力外，組織更應考量在跨單位資料傳輸的保護機制(例如加密或虛擬私人網路等)，以確保傳輸時的安全。另對於雙方共同留存的資料，應清楚定義彼此的保密責任與義務。

相關標準

A.10.8.1 資訊交換政策與程序

應備妥適當的正式交換政策、程序及控制措施，以保護經由使用所有型式通訊設施的資訊交換。

A.10.8.2 交換協議

組織與外部團體間資訊與軟體的交換應建立協議。

A.10.8.4 電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

---

[1] 電子發票實施作業要點第 18 點：「營業人銷售貨物或勞務予非營業人符合下列條件者，得向所在地主管稽徵機關申請使用電子發票：
（一）經核准使用電子計算機統一發票。
（二）提供新臺幣 1 百萬元保證金。
（三）無積欠已確定之營業稅及罰鍰、營利事業所得稅及罰鍰。
（四）同意將電子發票上傳整合服務平台留存。
（五）可正確掌握買受人基本資訊。」

類別：資訊應用

【案號：*A990102*】

地政電子謄本系統提供具備法律效力的電子謄本

【資料來源：今日新聞 *99/09/08*】

焦點話題

高雄市政府為服務民眾，突破地政服務周六打烊限制，自即日起將具數位簽章法定效力的「高雄市地政電子謄本系統」網路申請時間，延長為星期一至星期六上午 *08:00* 至下午 *08:00*，以因應全國網際網路使用者需求，讓地政資訊業務又向前邁進一大步。地政處長表示，「地政電子謄本系統」將所有地籍資料「網路化」，民眾可以不用再跑到地政事務所，只要在家利用電腦或 *PDA* 上網即可申領到土地、建物之登記、地價、測量圖資、異動索引、異動清冊、參考資訊檔等謄本資料、同時還提供建物門牌查詢地建號資料服務。所有申請的謄本資料，均附有經濟部核可的數位簽章以及騎縫章、檢核碼與 *QR-Code* (二維條碼)防範偽造，同時線上申請的謄本資料法律效力等同地政事務所核發之紙本謄本。為防有心人士偽造，建議業者與民眾收到他人提供的電子謄本資料時記得作複驗的動作，只要藉由該謄本所附的檢核碼或 *QR-Code*，即可上網調出該謄本的原始資料核對確認。

重點摘要

1. 依照「電子簽章法」規定[1]，以電子文件形式作成的文書，如內容可以完整呈現，且日後可以取出供查驗者，法律效力等同於紙本文件的原本或正本。
2. 行政機關對權利人以外的第三人提供地政資料時，應注意提供個人資料之必要性，以免違反電腦處理個人資料保護法的規定。

法律觀點

地政謄本的電子化是依循「電子簽章法」，建置安全及可信賴之網路環境，民眾可透過網際網路申領「地籍地政電子謄本」，而不必親自到各地政單位申領資料，提供民眾便利的生活。依照「電子簽章法」第 *4* 條第 *1* 項[2]規定，經過民眾同意後，地政機關即得以電子文件形式提供地政資料。為驗證申請者身分，此服務系統要求申請者或其代理人以自然人憑證或工商憑證登入。地政機關受理後，將以政府管理憑證中心核發之電子憑證進行簽章，依「電子簽章法」第 *9* 條第 *1* 項[3]，可達到機關用印的法律效果，且以電子憑證加簽後，可以確保文件的完整性並防止竄改，並於日後進行查驗，依法可作為文書的原本或正本[4]。民眾可以使用網路攝影機或手機讀取 *QR-Code* (二維條碼)連線至系統進行查驗，不僅省事又便捷，還可達到節能減碳環保的功能。

目前實務上土地登記及地價電子資料謄本可分為二類，第一類土地登記謄本，需由本人或經其同意之代理人提出登記名義人的身分證字號，可申請提供各種類土地登記及地價資料，其個人全部登記及地價資料均會予以顯示。但如果有其他共有人、他項權利人及管理者時，他們的身分證字號及出生日期則不會顯示。第二類土地登記謄本則是任何人都可以申請隱匿登記名義人的身分證字號及出生日期資料的土地登記及地價資料。由於登記名義人姓名、出生年月日、身分證字號、住址及不動產所有權歸屬等資訊都屬個人資料之範疇，因此行政機關在提供資料時，應注意申請人的身分，在提供登記名義人資料時，應在必要範圍內提供給第三人，以免違反「電腦處理個人資料保護法」的相關規定。

管理 Tips

在相關法令漸漸齊備下，國內電子化政府的應用範圍不斷地擴大，為民眾帶來無比的方便性，但另方面也增加了身分遭冒用的風險(傳統仍可透過面對面來進行身分確認)，是以隨著這些應用的擴大與推廣，單位除應依服務的差異，確認所採用的身分驗證機制強度外，民眾也應對自己的身分驗證

時使用的密碼、卡片(如：自然人憑證)、戶號或身分證字號等增加保護的警覺與加強保護，以降低身分遭冒用的風險。

相關標準

A.11.3.1 通行碼的使用

應要求使用者遵照良好的安全實務去選擇與使用通行碼。

A.11.4.2 外部連線的使用者鑑別

應使用適當的鑑別方法，以控制遠端使用者的存取。

---

[1] 電子簽章法第 4 條第 2 項：「依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。」

[2] 電子簽章法第 4 條第 1 項：「經相對人同意者，得以電子文件為表示方法。」

[3] 電子簽章法第 9 條第 1 項：「依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。」

[4] 電子簽章法第 5 條第 1 項：「依法令規定應提出文書原本或正本者，如文書係以電子文件形式作成，其內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。但應核對筆跡、印跡或其他為辨識文書真偽之必要或法令另有規定者，不在此限。」

類別：資訊應用

【案號：*A990103*】

俄國業者宣稱可破解 手機資料保護機制

【資料來源：*ITHOME 99/10/05*】

焦點話題

唯一一支讓美國總統歐巴馬不顧國家安全局反對的商業行動通訊裝置－黑莓機。上周遭一家專門提供檔案及密碼回復服務的俄國業者，宣稱已可破解黑莓機上所儲存的受保護資料，黑莓機之所以這麼受歡迎的原因在於終極的安全能力，所有從黑莓企業伺服器與黑莓手機間的資料傳輸都是透過高度安全的 *AES*[1]或 *Triple DES*[2]運算加密；並輔以其獨特的私有加密金鑰，該金鑰是自安全且經雙方認證的環境中產生，再指派給每個黑莓機用戶，並再進一步的透過黑莓企業伺服器的政策，強制要求對包括訊息、通訊錄、任務或行事曆等資訊為密碼認證，另再利用密碼管理工具、系統管理員等功能，以改變黑莓機裝置的密碼或是鎖住遺失的黑莓機與刪除資料。惟其設計上仍被找出有安全上的漏洞，該業者宣稱可透過密碼回復的方式來攻擊黑莓機上的備份資料，甚至有駭客已發展出可透過傳送簡訊的方式來散布惡意程式，使民眾所收到的簡訊內容轉送給駭客。

重點摘要

1. 智慧型手機已具備像行動辦公室的功能，對於手機內所存放的重要資訊也應有安全防護的裝置。
2. 使用手機上網會有電腦病毒或惡意程式入侵的問題，不要任意下載或接收來路不明的檔案。

法律觀點

隨著科技的發達，民眾經常都會使用筆記型電腦和智慧型手機，這些筆電和手機多已具備可輕鬆上網的功能，甚至被當作是生活或辦公不可或缺的貼身記事本，內建的功能與軟體也越來越多，相對的儲存於其內的重要機密資訊也就需有更安全的防護設計。現今的智慧型手機多具備有電腦的功能，可連線上網和操作許多作業軟體，儼然是一種迷你小型電腦，只是手機一旦可以上網之後，隨著而來的就是手機病毒或惡意程式入侵的問題，個人隱私被侵犯和商業機密的外洩風險也就因此增加。

我國刑法針對妨害電腦使用的規定，除有規範破解使用電腦之保護措施而入侵電腦或相關設備會構成犯罪外[3]，並對設計可用來破解他人手機安全防護的電腦程式行為，也有構成犯罪的規定，尤其是程式的設計是供自己或他人犯罪之用時，除行為人構成前述犯罪外，該程式提供人亦有觸犯「製作電腦犯罪程式罪」，依法最重可處 5 年以下的有期徒刑[4]，因此本案例中的俄國業者如果將破解手機的程式提供他人作為犯罪之用就會有觸法的問題。而隨著行動辦公的趨勢逐漸風行，智慧型手機越來越普遍，民眾用手機來辦公、上網、傳簡訊、傳照片、進行小額交易都是生活常見的事，為避免在使用手機上網或傳輸資料的過程中，不當的受到資訊攔截或惡意入侵，因特別留意透過公共網路、網咖、藍芽等方式傳輸資料的安全問題。同時已有業者針對高度需要手機內資訊安全的消費者，提供有防毒軟體或定期掃毒的裝置，不僅可濾掉垃圾簡訊的騷擾也能保護電子郵件在傳送或存取時，不受干擾，惟在使用手機上網時還是應避免下載來路不明程式或開啟不明檔案，以及平常有對重要資料做好備份的習慣，以免資訊外洩，造成損失。

管理 Tips

近兩年來手持式通訊設備技術越來越成熟，使得在其上的應用越來越多，這些設備的使用均是遠端存取的機制來使用組織內的服務；組織在開放遠端存取時，應有更為嚴謹的控管程序，包含授與使用權限的政策與合理性、

終端設備風險的管理及傳輸的安全性均應有適當的考量。

相關標準

A.10.8.4 電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A.11.4.2 外部連線的使用者鑑別

應使用適當的鑑別方法，以控制遠端使用者的存取。

A.11.7.1 行動計算與通信

應備妥正式政策，並應採取適當的安全措施，以防範使用行動計算與通信設施的風險。

A.11.7.2 遠距工作

應發展與實作遠距工作活動的政策、作業計畫及程序。

---

[1] 【名詞解釋】
所謂 AES(Advanced Encryption Standard)，是一種密碼學中的加密方法，這套加密標準是經過 5 年的篩選測試，由美國國家標準與技術研究院（NIST）於 2001 年 11 月 26 日發佈，為美國聯邦政府所採用的區塊加密標準，並已廣為被世界各國所使用，為對稱密鑰加密中最流行的演算法之一。

[2] 【名詞解釋】
所謂 Triple DES(Triple Data Encryption Algorithm)，是密碼學中三重數據加密算法塊密碼的通稱，相當於是對每個數據塊應用 3 次 DES 加密算法。由於計算機運算能力的增強，原版 DES 密碼的密鑰長度變得容易被破解，3DES 的設計則是用來提供一種相對簡單的方法，增加 DES 的密鑰長度來避免類似的攻擊。

[3] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[4] 刑法第 362 條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

類別：資訊應用

【案號：*A990104*】

票選人評委員 政院網路投票員工怕 *IP* 暴露

【資料來源：自由時報 *99/11/24*】

焦點話題

行政院擬對考績委員的選舉舉辦網路投票，但遭部份公務員投訴指控，有「開民主倒車」的嫌疑。爆料公務員表示選舉本應以秘密、無記名投票的方式為之，線上投票的方式，會暴露投票人的 *IP* 位址，「誰投誰」一清二楚，讓公務員不僅不敢投票，還要揣摩上意投票。報料者並表示行政院推動線上簽核，很多人是用自然人憑證登入，本已有資料外洩的顧慮，公務員最在意考績，攸關升遷，而考績及甄審委員掌控生死大權，選前一直有所謂「長官人馬」的名單消息，採用線上投票，更是直接公開投票內容，等同於「記名投票」。資訊室表示，人評委員票選，線上投票只把「整個投票結果」統計出來，不會顯示「個人投票意向」，且電腦資料庫維護嚴密，既不可能被入侵，也不會有資訊技術人員違法，以繁瑣技術進入電腦資料庫探取個人投票意向，各級長官更不會要求查看個人投票意向，所以有人擔心會被查出投票意向，那是「多慮了」。人事局則指出「人評會」票選委員選舉，是依據「公務人員陞遷法」和「考績委員會組織規程」等法規辦理，目前行政院所屬各機關幾乎都是採取線上(網路)投票方式，很多機關已行之多年，反應良好，從沒發生問題。

重點摘要

1. 線上投票只是投票方式的不同，但仍應依據「考績委員會組織規程」之規定採取普通、平等、直接及無記名投票方式。

2. 線上投票可以自 *IP* 位置推知投票人之身分，有侵害「電腦處理個人資料

保護法」之虞。

法律觀點

為辦理公務人員考績評定，各機關應設置考績委員會[1]，考績委員會應設置 5 至 23 名委員[2]，每滿 4 人應有 2 人由機關受考人票選產生[3]，且應採普通、平等、直接及無記名投票之方式進行[4]，因此案例中人評委員之選舉，雖然可以通訊方式進行，但仍必須遵循無記名投票原則。雖然人評會最終只會顯示投票結果，不會顯示個人投票意向，然而若在進行線上投票時，在確認投票人資格或投票進行投票登入的 *IP* 位址，均可能可以查知投票人意向，如此一來，將違反前揭「考績委員會組織規程」所要求的無記名投票原則，且將使投票人無法依照自由意志進行投票。

另外，個人投票意向屬於個人資料的一種，如果公務機關內部人員透過管道取得投票人的投票意向，將會違反「電腦處理個人資料保護法」的規定，除須負損害賠償責任外[5]，若係意圖營利時，並可能有刑事責任[6]。未來新版個人資料保護法施行後，即使沒有營利的意圖，但違法蒐集亦將面臨刑事責任的追究[7]。

近年來透過網路進行社會活動已漸為風潮，舉凡報稅、掛號、銀行等社會行為，都可以透過網路來達成，但在網路的運作過程中，為保護交易安全或線上傳遞資料之機密性，不可避免須確認使用者的身分及確保資料傳輸的安全性。「自然人憑證」相當於網路身分證，可以達到確認使用者身分之目的，並進行數位簽章以確保資料之完整性及機密性，為確保網路交易安全之利器，且可以對資料進行加密，以確保資料的秘密性。因此，如進行線上投票時，考慮以自然人憑證作為確認是否具有投票權的工具，並利用公用電腦進行投票，以避免使用透過 *IP* 位址可識別個人之電腦，如此一來，即相當於現行多數投票制度以國民身分證確認投票權並於領取選票後在隱密環境下圈選，可避免以自然人憑證投票後之結果有可以勾稽追蹤之可能，以此符合無記名投票原則，供作參考。

管理 *Tips*

隨著資訊化的腳步為生活帶來各式各樣的便利性，在本案例組織應先仔細考量活動之性質，考量適當之處理措施，例如投票的隱密性是否由資料的限制存取或加密來確保其隱私性，再依架構下的安全性來對員工進行教育訓練及宣導，讓員工了解資料保護狀態及範圍，以及何種資料會被蒐集或使用，以期能降低員工對於個人投票意向、*IP* 位址及資料外洩或暴露的疑慮，並減輕員工反彈。其中如有保存較隱私之資料，且因業務需要而須檢視或查閱時，應有適當的核准及授權機制，並留存相關活動或操作紀錄，以避免未有正當理由而侵犯個人隱私。

相關標準

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

---

[1] 公務人員考績法第 15 條：「各機關應設考績委員會，其組織規程，由考試院定之。」

[2] 考績委員會組織規程第 2 條第 1 項：「考績委員會置委員 5 人至 23 人…。」

[3] 考績委員會組織規程第 2 條第 4 項：「第 2 項委員，每滿 4 人應有 2 人由本機關受考人票選產生之。受考人得自行登記或經本職單位推薦為票選委員候選人。」

[4] 考績委員會組織規程第 2 條第 5 項：「前項票選，應採普通、平等、直接及無記名投票法行之。但各機關

情形特殊者，得採分組、間接、通訊等票選方式行之。辦理選務人員應嚴守秘密。」

[5] 參照電腦處理個人資料保護法第 27 條規定。

[6] 參照電腦處理個人資料保護法第 33 條規定。

[7] 參照個人資料保護法第 41 條規定。