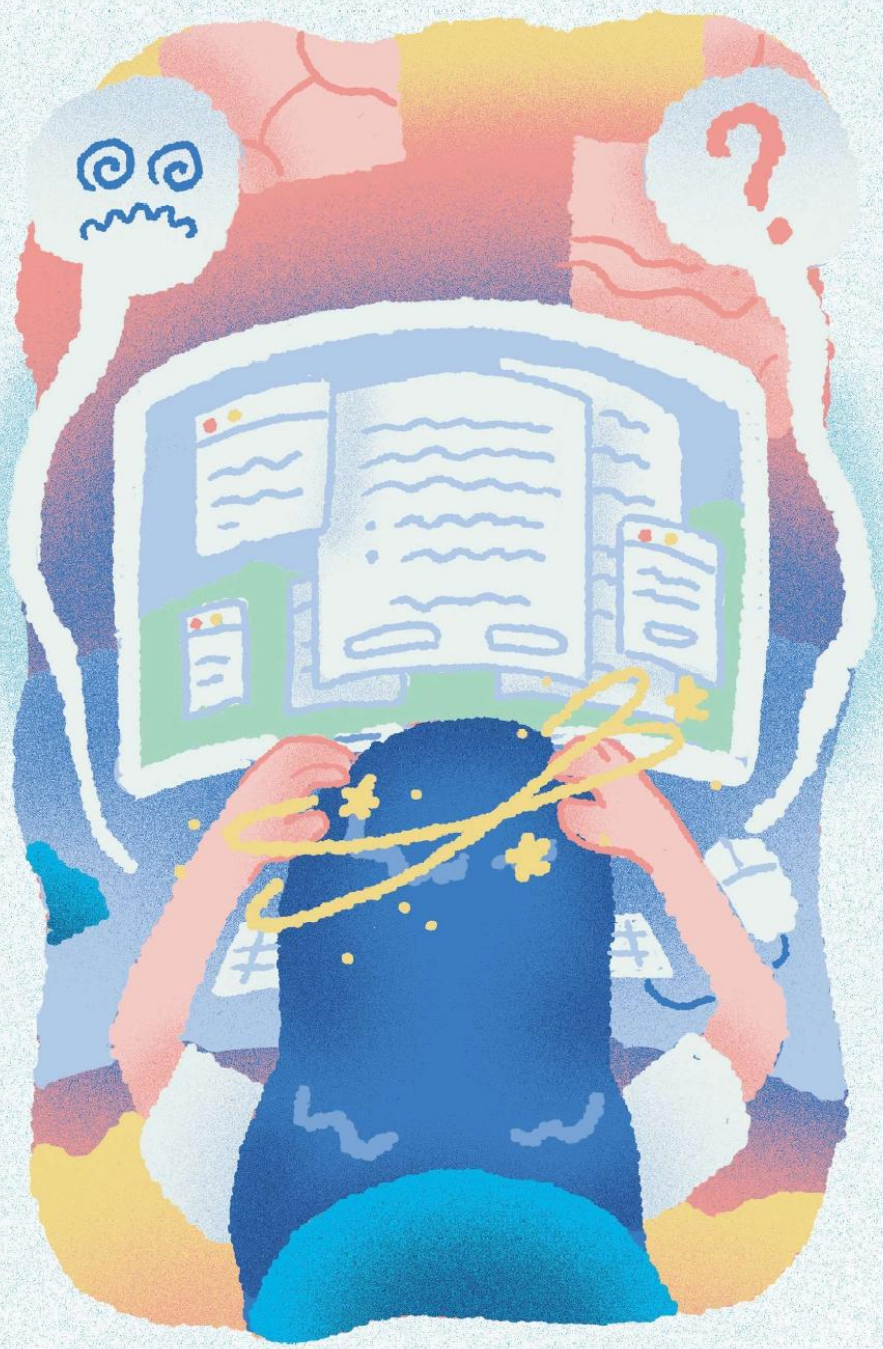
法令天地

哇！AI你怎麼什麼都知道？

第四章



案例問題意識：

Lisa 最近準備寫一篇小論文，她決定試試一款新的 AI 應用系統，來協助她整理資料和潤飾論文的語句。正當她要註冊帳號時，卻發現需要提供眞實姓名、身分證字號等資料，一大串的使用者服務條款讓她眼花撩亂。

「哇，這個也太多資料要寫了吧……」Lisa 點開使用者服務條款，其中一條寫著資料可能會被用於系統訓練，也可能會分享給合作夥伴。

Lisa 有點困惑，不確定自己的資料會被拿來用在哪？

爭點解析：

個人資料保護法的「個人資料」定義：

1. 姓名
2. 出生年月日
3. 國民身分證統一編號
4. 護照號碼
5. 特徵
6. 指紋
7. 婚姻
8. 家庭
9. 教育
10. 職業
11. 病歷
12. 醫療
13. 基因
14. 性生活
15. 健康檢查
16. 犯罪前科
17. 聯絡方式
18. 財務情況
19. 社會活動
20. 其他得以直接或間接方式識別該個人之資料

法律知識介紹：

每個人多少都有些秘密，這些秘密不一定是什麼虧心事，可能只是你的身高體重、出生年月日、過去的學經歷，或是什麼時候看了醫生的病歷資訊。因為這些資料可以辨識出你個人的身分，在注重隱私的現代社會中，需要特別保護。

我們可以決定這些資料要不要讓人知道，還有要在什麼時候、透過什麼方式、讓誰知道，這是我們的「個人資訊自主權」。如果侵害他人的個人資訊

自主權，除了會負擔民事上的損害賠償責任外，也可能違反《個人資料保護法》而受到刑罰制裁。

AI 技術的發展也是目前個人資料使用上的挑戰，因為多數 AI 是使用「大型語言模型」的技術，透過大量資訊讓機器學習，電腦會透過大量資料來進行分析，找出其中的規律性，再用這個規律性來回答使用者提出的問題。

雖然在註冊這些 AI 帳號時，都有使用者服務條款，但這些條款有幾個問題：首先，沒有太多人會仔細閱讀這些密密麻麻的文字，讓使用者的同意經常流於形式；其次是過去某些網頁曾經在沒有知會使用者的情況下，單方面修改服務條款，將使用者的資料交給第三方網頁；最後，如果不同意這些條款，或只同意部分，使用者將無法使用相關服務，即使有些疑慮，多數人仍會選擇妥協。

目前在使用 AI 服務時，我們能做的是許多網站可以設定個人交談的資料是不是要作為語言模型的大資料庫，如果拒絕，我們和 AI 的交談紀錄就不會被拿來使用，或是在對話結束後清除 AI 的記憶。歐盟、美國、日韓等國都已經提出 AI 趨勢下個人資料使用的規範，近期立法院也有人工智慧法案的討論，除了國家立法管制外，大家在使用 AI 時有保護個人資料的基本意識也是相當重要的，建議避免在與 AI 對話的過程中提及個資，防止被 AI 以「說溜嘴」等方式洩漏給第三方。

------轉載自：新北市政府網站

機關安全維護

機關安全維護　錦囊 第 3 號
~「駐外人員自我防護之道」

前言

甲君平時在工作上完全投入，對上級交辦專案任務或份內工作皆能如期如質完成，且精通英文、西班牙文等語言，因此深受長官賞識，於 105 年 12 月再度奉派中南美洲大使館，原本高齡近 80 歲的母親反對再次外派，甲君因此允諾返臺後將辦理退休，陪母親度過晚年，惟隔年 4 月在中南美洲住處被發現遭人刺殺身亡。

案情因果

- 甲君在駐外期間仍秉持勤奮的工作精神，經常加班至深夜，務將當日工作辦完，才返回獨居之租屋處所。105 年○月○日甲君並未準時到辦公室，同事以為可能前晚加班到將近 10 點而睡過頭，但以手機聯絡卻沒有回覆，報警後才發現甲君於獨居處所不幸遇害身亡。
- 甲君派駐中南美洲因政局動盪，加上毒品、治安等問題，曾發生我國大使遭恐嚇，還商請當地軍方派武裝人員擔任護衛，甚至有駐館以駐地治安惡化，而要求外交部同意替駐館人員配槍等情形；且因甲君單身租屋在外，加以經常夜晚加班工作，人身安全風險相對較高。

問題分析

- 我駐外人員遭遇人身和財產危害事件，以遭歹徒行竊、

行搶居多，而行政院所屬部會如外交部、國防部、經濟部、教育部、僑委會等部會，因業務上皆有派駐工作人員赴國外服務之需要，惟因各駐地國之民情及政經狀況不同，駐外人員必須面對各種不同類型的治安風險問題如下：

一、社會治安欠佳地區，毒品猖獗、槍枝氾濫。

二、武裝衝突地區，恐怖活動及反叛軍隊無預期之武力攻擊。

三、社會貧富差距大之地區，被搶劫及綁架之機率高。

四、民族意識高漲，經常發生排華風潮事件。

策進作為

- 對於駐外治安風險較高的地區如中南美洲、東南亞及南非地區之人員，尤其針對初次駐外人員講習，應加強其瞭解當地之民情及治安狀況，提升其風險意識，並由曾長期派駐當地之資深人員傳授經驗，降低因應不良治安之適應期。
- 各駐外館處對居住於無警衛、保全設施之人員，應建立緊急通報及橫向聯繫網路、保護並減少獨居同仁危險之狀況，加強犯罪預防之知識及技能訓練，以增進人身安全保障。
- 針對治安風險高低不同之駐外地區加以評估，就安全性考量，適度提高風險較高層級之安全津貼補助，以維護駐外人員生命財產安全。
- 在住處安裝保全系統、加高刺網圍牆、飼養「狼犬」等嚇阻措施，或選擇有 24 小時警衛的社區住宅。

- 研議專案購建（租賃）駐外人員宿舍之可行性，以適度保障駐外人員之人身基本安全。
- 外交部政風處編印「駐外人員安全維護與自衛要點手冊」提供駐外人員安全防護參考，在預防措施部分，針對個人、家人、小孩、旅行、汽車、住家、辦公室、郵包炸彈等詳列相關應注意事項，強調駐外人員應提高警覺，留意周遭人事物等周邊環境，並針對遭歹徒恐嚇、攻擊之求生及應變訂有處置措施，提醒與歹徒周旋應對之技巧與注意事項，另要求應建立緊急通報及橫向聯繫網路，將警方、館舍及同仁聯繫電話編列成冊，供緊急聯繫之用。

結語

外交工作是相當繁重的，尤其是駐外人員除了要面對工作的壓力外，還要注意人身安全，因為身處異國，膚色、人種與當地不同，容易成為歹徒覬覦的目標，且因工作定期或不定期輪調不同國家，因此針對治安高風險外派地區，訂定相關危安預防及管控措施，同時加強自衛防護教育宣導，以有效降低駐外人員不可預測之危安風險。

------轉載自：廉政署網站

公務機密維護

公務機密維護　錦囊 第 3 號
~「駐外機構資訊保密之道」

前言

駐外機構為我國外交打拼的最前線，其工作環節容易受到敵對勢力的刺探、蒐集，且隨著資訊科技日新月異，網路上的駭客攻擊手法也不斷翻新，部分駐外機構屢遭網路駭客惡意攻擊，蒐集公務機密資料或侵擾其行政運作，網路安全與資安管理面臨嚴峻的挑戰。若相關人員未能提高警覺，極易因疏忽而洩漏相關資訊，加上事後追查不易，致使機敏資料外洩時有所聞。

任何一個能夠上網的裝置或電腦，都很容易被網路上的惡意活動影響，因此，駐外機構人員應嚴格遵守相關資訊安全規定，以降低資通安全威脅，提高電腦資訊使用風險承受能力，並妥善使用公務電腦，避免機敏資料外洩，以確保國家安全及利益，實為駐外機構資訊機密維護的重要課題。

案例摘要

- 駐○○代表處○○組所屬電腦於非上班時間，發生大量資訊封包傳送至外部特定電腦情事，經查係該組乙類雇員林○○使用之外網電腦及實體隔離電腦。據瞭解林員以更新電腦病毒碼為由，私自將內網連接外網電腦，傳送大量資訊封包至外部特定電腦，有洩密之虞。林員所使用之 2 臺電腦硬碟，經查共計 26 件機敏資料外洩，違反資訊安全規

定情節嚴重。案經○○委員會召開專案小組會議，決議將林員解聘。

問題分析

- 系統遭入侵：未經授權之使用人（駭客）入侵資訊系統進行攻擊、竊取或竄改資料等非法破壞情事。例如，「社交工程」(Social engineering) 郵件設計愈來愈精巧可信，不知情的收儲，一旦開啟郵件附件，或點擊郵件內的惡意網站連結，任何一個動作都會讓電腦感染病毒。
- 未落實資訊安全規定：
  一、隔離電腦未落實隔絕於網際網路之外，專用於公務　作業。
  二、個人電腦之使用者識別碼及密碼，未妥善保存或交付他人使用，及未定期更換。
  三、機敏資料存放在對外開放的資訊系統中。
  四、隔離電腦未以人工更新防毒程式病毒碼。
  五、非經權責主管核准，個人電腦擅自下載軟體或變更硬體規格。
  六、遇有資安異常事件發生，未即時向資訊單位反映處理。
- 維護措施不足：
  一、可攜式設備或媒體（如筆記型電腦、行動硬碟、隨身碟等）應妥為保管，非因公務需要並經主管核准，不得攜出辦公處所，攜回時應進行掃毒或系統還原。
  二、對於電腦發生異常情事，未有警示系統，俾及時採取有效的防範措施。
  三、重要機敏檔案之備份媒體，未嚴密管制或由專人管制。

- 稽核功能不彰：未依機關資訊安全環境，實施資訊稽核，致未能即時發現缺失。
- 使用人違規使用：經授權之使用人明知違規而使用，致系統資料外洩等情事。

策進作為

- 網路流量監控、分析及管制：

  為防範系統遭駭客入侵，防火牆建置後，網管人員應隨時對資訊網路進行流量監控、分析及管制，俾利及時因應處理。

- 加強教育宣導：

  辦理駐外人員資訊安全教育訓練，建立正確的資安共識，以避免發生違規使用電腦及公務資訊之情事，其宣導重點如下：

  一、隔離電腦應隔絕網際網路並專用於公務作業，禁止私接；上網電腦連接網際網路並專用於上網瀏覽資訊或收發一般電子郵件。兩者不得混用，並於電腦設備明顯處張貼區別用途之識別標籤。

  二、隔離電腦變更用途為上網電腦或上網電腦變更用途為隔離電腦時，須先將電腦硬碟格式化、重新安裝作業系統。

  三、資料之加解密須在隔離電腦進行。

  四、嚴禁安裝使用 P2P 點對點分享軟體。

  五、禁止下載安裝或使用未經授權來路不明之軟體。

  六、避免開啟來路不明的電子郵件及檔案，以避免駭客病毒入侵。

  七、上網電腦禁止瀏覽非法或機關所限制之網站。

八、電腦應避免 24 小時開機，不使用時即關機或離線。

九、機密性或敏感性資料須以主管機關認可之加密機制加密後儲存於光碟、磁片、外接式硬碟等可攜性媒體或隔離電腦硬碟中，並予以妥善保存。

十、禁止使用上網電腦處理機密性或敏感性公務。

落實機關資訊安全稽核：

為機先發掘資安漏洞，同時檢視駐外機構人員實際執行保密情形，各駐外館處應定期、不定期或遇有重大洩密案件之虞時，執行資安稽核或保密檢查，除改善缺失漏洞並提高防火牆功能以防駭客入侵外，同時據以檢討策進，以建立同仁機密資訊維護的正確認知。

結語

駐外機構資訊機密維護工作，是否落實，攸關國家安全及利益，為確保資訊機密的安全，除了必要的資訊安全機制外，最重要的還是需要使用者的保密素養，因為資訊的掌握者、運用者都是「人」，唯有「人」對於資訊安全與保密工作能夠做好，才是維護資訊機密的根本之道；再者，唯有使用者都具備健全的觀念與知識，體認資訊機密安全的重要性，資訊安全政策才能落實。

------轉載自：廉政署網站

政策宣導-反詐騙宣導

------取材自：line”防詐動態警報”官方帳號