

公務機密維護宣導

合法使用及妥善管理遠端監控設備 防範網路洩密情事

一、案例緣起：

96年12月間某機關政風室接獲民眾檢舉，指稱該機關資訊單位擅自賦予委外派遣人員使用網路監看軟體之管理權限，該監看軟體可監看機關同仁之電腦畫面、監管進出網站情形、讀取正式人員規劃之採購案需求說明書等機敏資料，如無適當管制，恐有侵犯隱私權及影響公務機密安全之虞。案經查察瞭解，該機關資訊單位所掌管之監看系統稱為「神網系統」，具遙控傳檔、畫面擷取等遠端監控功能，其管理權限設定給委外派遣人員，並由該資訊單位承辦人員來監督，該承辦人員則聲稱93年奉主管指派接辦該項工作至今，從未曾啟用過監看功能，亦不瞭解監看系統管理權限是否有依規定簽陳核准。本案姑不論該承辦人所言是否可信，僅就該監看系統如遭不當使用有危及機關資訊安全環境及觸法之虞，卻未有隻字片語規範其使用與管理一節，已足令人憂心與疑慮。

二、案例研析：

(一) 該機關政風室將全案查察結果及建議意見簽陳機關首長核可後，迅速將案情向上級主管政風機構反映，經過研析：

- 1、該機關資訊人員管理是項監看系統及設備並未訂有使用及作業規範，而檢舉所述情節不論從法律層面，或道德層面來看，均有正視並予以釐清必要。
- 2、該機關網管人員可能未經授權即侵入同仁電腦，監看同仁電腦畫面，以及監管進出網站情形，甚至任意讀取承辦採購案件人員規劃中之採購案需求說明書等機敏資料，顯見機關資訊安全環境存有灰色死角，行為者亦涉有違法之虞。
- 3、另委由派遣人員監管重要資訊系統，得以隨時接觸同仁電腦內儲存之資料，甚至公務上之機(保)密資料，是否妥適？亦有藉訂定使用及作業規範時機再加細酌必要。

(二) 目前政府機關均已電子化，資訊系統採遠端管理及維護亦甚普遍，研判所屬其他機關亦可能擁有類似之遠端監控設備，而類似檢舉情節是否亦存在這些機關？實有藉全面清查瞭解各所屬機關管理及使用現況，進而促使資訊單位正視問題，訂定合理使用及管理規範之必要。

三、處理經過：

- (一) 主管政風機構於接獲所屬報告後，先行對本機關遠端監控設備使用情形進行瞭解，嗣即將前揭所屬機關案例簽報首長作詳細分析說明。
- (二) 函請各所屬機關審慎考量執行監看政策之必要性，若有必要，應請資訊單位訂定具體作業規範或納入資訊安全規定及簽陳機關首長核准，

並於執行前與機關同仁充分溝通或明確宣示，以避免引發違法爭議。同時，為檢視各機關之遠端監控設備使用現況，立即進行全面清查，茲說明如下：

- 1、請各機關合法使用具遠端監控功能之軟、硬體相關設備及善盡管理責任。
 - 2、請各機關依清查項目自行檢視機關內現有遠端監控設備之種類、功能、使用單位及現行管理方式等，以利清查現有遠端監控設備之使用及管理情形。
 - 3、將清查結果彙整簽陳首長，本案共清查 33 個機關，計有 28 個機關掌有遠端監控相關設備，約佔清查總數之 84.8%，監看軟體計有神網系統、pcAnywhere、VNC、Smart IT 等 4 種，除擁有神網系統之機關已陸續停用或關閉遠端遙控之相關功能外，其他軟體主要係用於資訊系統之遠端維護、資訊資產管理及資安管理等，並設有若干管理規範，目前尚無涉監看機關同仁電腦行為等侵犯隱私之爭議。
- (三) 為強化對現有遠端監控設備之合法使用及督導管理，於全面清查後，另函請各機關透過定期資安內稽加強查核，以避免機關同仁、資訊系統委外維護廠商因不當使用遠端監控設備而引發違法爭議及防範網路洩密情事，建議檢查重點如下：
- 1、遠端監控設備之使用及管理應訂定具體作業規範或納入資訊安全規定，並經機關首長或其授權人員核定。
 - 2、應嚴格管控遠端監控系統登入者之使用權限，若有提供委外維護廠商執行遠端維護時，尤應特別注意其登入權限、使用情形及維護範圍等，避免因權限管制疏漏，造成資安防護漏洞。
 - 3、遠端監控系統之使用情形，應建置資訊系統使用者紀錄檔 (Log File) 及系統異常管理機制，並定期稽核管考。

資料來源：臺灣臺北地方法院政風專區