公務機關利用去識別化資料之風險評估及法律責任 下

文／林裕嘉

（文接上期）

（三）小結

1. 依歐盟 A29WP 之見解，似認為「不可逆之擬匿名化資料」亦屬於「匿名化資料」[15]，並強調資料是否已確實匿名化，須取決於個別情形而定，判斷運用一切可能合理方法是否得以識別特定個人。

2. 依英國資訊保護官及英國法院之見解，則對於「匿名化資料」之範圍界定相對較為寬鬆，其認為縱使係「可逆之擬匿名化資料」，只要原資料保有者並未將對照表或解密方法等連結工具提供給資料接收者，並且採取適當安全措施，使資料接收者無管道及機會重新識別資料當事人，則該釋出的資料也屬上開「匿名化資料」之一種。

三、法務部103年11月17日函釋同德國、英國見解

（一）行政院於 103 年 10 月 29 日召開「虛擬世界發展法規調適工作專案報告」之會議時，會中有出席代表反應，實務上許多公務機關於判斷政府資料得否開放時，有誤解個資法規定之情形。法務部為釐清公務機關適用個資法可能發生之誤解型態，於 103 年 11 月 17 日作成法律字第 10303513040 號函釋，其中說明三提及：「三、復按個資法第 2 條第 1 款規定，所謂個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、……及其他得以直接或間接方式識別該個人之資料。是以，如將公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍。此後，公務機關主動公開或被動受理人民請求提供是類個人資料去識別化後之政府資訊，除考量有無其他特別法限制外，分別依檔案法第 18 條或政府資訊公開法第 18 條等相關規定決定是否公開或提供即可，無須再擔心是否符合個資法所規範之『特定目的內、外利用』的問題。」

（二）按我國個資法之條文實際上並無出現「去識別化」之用語，則去識別化之意義為何？倘若資料依其呈現方式已無從直接或間接識別該特定個人，是否仍為個人資料？是否仍有個資法之適用？法務部於此函釋中表達了其法律見解，與前述德國、英國資訊保護官及英國法院之見解相同，固然公務機關仍然保有原始資料或對照表等工具得以直接或間接識別相關當事人，故公務機關所保有的整體資料仍然屬於個人資料，但其對外公開或提供已無從直接或間接識別之資料並無違反個資法的問題，因為當該資料對外公布釋出之時，其所呈現之方式已不再是個人資料，自無個資法之適用。

肆 加工匿名後無從識別之判斷標準

一、國外法制實務見解

參考歐盟、英國及日本的文獻，均一再強調去識別化不可能絕對毫無風險，僅能檢視其是否已排除「合理可能」識別特定個人之程度。因此，資料保有者須評估所釋出之去識別化資料有無合理之可能性，使資料接收者得與其他資料結合後而識別出特定個人，倘若釋出之資料本身雖不具有特定個人識別性，但如以此為線索，與其他已公開，或一般人可得獲取之「其他資訊」組合、比對下，亦得識別出特定個人時，則該釋出之資料將仍屬得間接識別之個人資料。從而，所謂「其他資訊」之範圍，自會影響去識別化之判斷準據：

（一）日本：學者主張與實務見解並不一致（判決實務上見解亦未見統一），有採「一般人基準說」，所謂「其他資訊」應限於已公開、被公知資訊，一般人於生活中如報章雜誌等媒體或圖書館等得輕易搜尋、獲得之資訊，此說以一般人作基準，判斷其有無「其他資訊」作組合、比對之可能。另有採「特別基準說」，認為「其他資訊」不應僅限於一般人容易獲得之資料，在具體事件上於判斷組合、比對之可能性時，雖僅為一定範疇之關係人（例如同僚、親友、街坊鄰居等）可能知悉、保有之其他資訊，亦應納入考慮[16]。

（二）英國：英國資訊保護官及英國法院對於去識別化資料之判斷，採取「有心侵入者測試」（the motivated intruder test），也就是一個侵入者如果有動機想嘗試時，是否可能成功地再識別，此測試也被歐盟 A29WP 及澳洲政府所採行[17]。有心侵入者是指一個沒有先前知識（prior knowledge）的人，但是想要從去識別化資料中找出特定個人，其沒有專業的電腦知識或技術（例如駭客破解技術），也沒有採取犯罪的方法獲得保密資料，但其具有合理的能力，能夠使用網際網路、圖書館，以及所有公開的資料進行對照、組合、連結。英國資訊保護官認為得用於對照、組合、連結之資料來源包含圖書館、地方政府機關、教會宗教團體檔案、戶政機關、家譜網站、社群網站、網際網路、地方或國家新聞檔案、其他組織團體或公部門所公開之資料等[18]。從上述「有心侵入者測試」之闡述，其對於所謂「其他資訊」之界定範圍應亦是如同日本「一般人基準說」之見解。

二、本文見解

加工匿名後無從識別之判斷標準宜採「一般人基準說」（同英國見解）：

考量到日本學說及實務見解尚有爭議，而且對於一定範圍之有先前知識之人（例如同僚、親友、街坊鄰居、醫師、教師、律師、社工等）而言，雖然其因具有先前知識而增加得以間接識別之可能性，但對於當事人所增加之隱私風險實際上很低，因其原本就已經保有當事人原始的個人資料才有能力得以重新間接識別，所以重點應不在這群人得否識別當事人，而在於其能否透過釋出之資料而取得當事人的新個資（英國資訊保護官及歐盟 A29WP均採此見解[19]）。再者，多數具有先前知識之醫師、律師等專業人員，雖掌握大量敏感性個人資料（病歷、犯罪前科等），但多已依法令負有保密義務或須遵守職業倫理規範，故其成為「有心侵入者」或對外提供執行職務所得資料之可能性較低[20]，例如：某匿名結構資料揭露 2012 年在 A 鎮有 X 人罹患麻疹，沒有其他更進一步的資料，某醫生提供其診治病人之資料給衛生機關，該醫生的診所中持有更多完整的資料，故很容易能從結構資料中再識別出其病人，但其受到醫生保密義務的約束，且其無法因為該資料集被公開提供，而得知比公開前更多的資訊。綜上，所謂「其他資訊」之範圍原則上應採「一般人基準說」。

伍 公務機關開放去識別化資料應作風險評估

鑑於個人資料去識別化難以有絕對性、一致性之標準，公務機關於利用去識別化資料前，應進行整體風險影響評估，針對不同資料屬性、類型或資料提供方式設定風險檻值，依比例原則分級控管去識別化程度：

一、歐盟 A29WP 認為政府機關開放將個人資料去識別化的政府資訊供公眾使用時，事前須先就該資料被再識別的風險進行評估，而評估時應考量的因素包含：1. 對於民眾或特定私人團體而言，哪些資料是其目前已可取得的；2. 擬開放之資料是否容易引發外界對其進行再識別的動機（例如：可能有很高的商業價值或輿論關注）；3. 資料於技術上被再識別的可能性。並應建立測試機制，實際測試資料被再識別的可能性，藉此監測發現是否存在漏洞，以評估資料開放的風險[21]。另一方面，前述英國資訊保護官辦公室於 2012 年所發布之「匿名化：資料保護風險管理實踐準則」（Anonymisation: Managing Data Protection Risk Code of Practice），提供資料保有者將個人資料去識別化時得以遵循的參考標準，要求資料保有者對去識別化後的資料進行風險評估，以自律方式降低可能的風險，並強調當去識別化不足，而導致資料重新被識別時，資料保有者必須負擔相關賠償責任，如此將資料保有者使用去識別化資料所生的風險控制在合理限度。

（文轉三版）

註釋

15. 參考歐盟A29WP，Wp136，同註12，p.18；Wp216，同註10，p.5。
16. 參考范姜真媺，公務員個人資料之公開與保護－日本之立法與實務帶來之啟示，中原財經法學第 33 期，2014 年 12 月，第 90-93 頁。
17. 國家發展委員會委託研究報告，同註10，第70-73頁。
18. Information Commissioner's Office,同註3，pp.22-25。
19. 國家發展委員會委託研究報告，同註10，p.70。
20. Information Commissioner's Office,同註3，p.25。
21. 歐盟A29WP，Wp207，同註2，p.14。
22. Information Commissioner's Office,同註3，p.37。
23. ISO/IEC 17000 第5.5條參照。
24. 104 年 12 月 15 日修正前之個資法第 41 條規定：「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。（第 1 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。（第 2 項）」。
25. 歐盟A29WP，Wp207，同註2，p.18。
26. Information Commissioner's Office， 同 註3，p.24、27；另參考Pseudonymisation, from German delegation to Working Party on Information Exchange and Data Protection, Interinstitutional File: 2012/0011(COD), Brussels, 24, October 2014, 14705/14, p.10, 連結網址：http://www.statewatch.org/news/2015/jan/eu-council-dp-reg-pseudonymisation-14705-rev1-14.pdf

JUDICIAL 司法 徵稿啓事 三、本刊歡迎來稿，有關法律實務、法學理論、法制評析、時事觀察、人物專訪、書評等文章均可，並請加註詳細聯絡資料（含服務機關、職稱、地址、電話、電子信箱）。 四、文稿一律不退件，請自留底稿。 五、稿件一經刊登，酌送稿酬，並寄贈該期刊物。 院網站。 JUDICIAL 司法 訂閱辦法 本刊每週 全年 費用新臺 如蒙 請郵政 帳 5005 帳 司法院

（文接二版）

二、本文認為，資料保有者在進行整體風險影響評估時，應綜合考量個人資料類型、敏感性程度、對外提供資料之方式、引發他人重新識別之意圖等因素，並根據風險評估之結果計算設定風險檻值，進而判斷去識別化之技術類型或程度，例如：

（一）供不特定人利用之開放資料（open data），因並未限制資料提供之對象、使用目的或方法，而是以公開（publication）之方式提供，因此風險檻值相對較高，宜達「匿名化資料」或「不可逆之擬匿名化資料」之程度較為妥適。

（二）供特定公務機關或學術研究機構個別申請使用之資料，因資料提供對象有所限縮（limited access），除能對於資料接收者之身分、使用目的、其他可能取得資料之管道、安全管理措施等先為必要之審查外，並得與資料使用者約定禁止重新識別資料之義務及其他資料利用之限制等，較有利於風險的控管，因此風險檻值相對較低，去識別化之程度可相對放寬，可提供含有個體性、敏感性、較為詳細之擬匿名化資料[22]。

三、重新識別測試為整體風險評估之一環，乃是為偵測及處理資料被重新識別的可能漏洞，倘若經評估重新識別之風險小於原先經計算設定之合理風險檻植，應可認為此時該資料被重新識別之可能性甚微，風險已於合理可接受之範圍，從而可認為該資料依其呈現方式已達「以一切可能合理之方法」（all the means likely reasonably to be used）無從再識別資料當事人之程度。

陸 個人資料去識別化過程驗證規範簡介

所謂「驗證」（Certification），係指對特定產品、過程或服務能符合一定要求，由中立之第三者出具書面證明之程序[23]。為合理評估及控制個人資料去識別化之風險，提升去識別化品質，增加個人資料當事人之信賴感，目前行政院規劃透過中立的第三方驗證機制，提供專家意見書，以因應我國「政府資料開放」及「大數據」之推動，經濟部標準檢驗局爰依行政院指示，參照國家標準CNS 29100及CNS 29191，訂定「個人資料去識別化過程驗證要求及控制措施」之驗證規範，其中「陸、PII（Personally Identifiable Information，即個人可識別資訊）去識別化過程」要求事項，即要求組織應訂定如下之 PII 去識別化步驟，並依此進行去識別化（以下僅摘錄要點）：

1. 由領域專家判定資料集之中的直接識別符。

2. 將直接識別資料遮罩（或變換）。即移除直接識別資料或將其擬匿名化。

3. 建立威脅模型。

4. 判定最小可接受使用之資料。

5. 使用步驟 3 所建立之模型，確定重新識別攻擊之風險的檻值。

6. 由來源資料庫中取得（樣本）資料。

7. 評估實際之重新識別攻擊風險。

8. 比較實際之被重新識別的風險與檻值。

9. 設定參數並套用至所有需去識別資料。

10. 對解決方案進行診斷。

11. 輸出已去識別資料至外部資料集。

自上開步驟可知，該驗證規範已有納入前述風險評估及重新識別測試之觀念，資料保有者可參照前揭要求及相關控制措施，並考量本身資料之型態，自行建置執行之作業程序，申請驗證機構（目前財團法人臺灣電子檢驗中心已有提供本項驗證服務）確認其作業流程及程序文件符合標準及控制措施要求。另須強調的是，公務機關或非公務機關最終是否要負損害賠償責任，因為是由個案承審法院決定，故不能完全保證通過驗證即必然可免除損害賠償責任，惟驗證機制之功能即在協助機關事前檢視其作業管理措施及流程，將去識別化風險控制在合理範圍，並保留相關紀錄資料，以備個案發生時用以強化其舉證能力，擁有較多的證據站在較有利的地位，降低損害賠償責任之風險。

柒 資料釋出者及接收者之法律責任

一、資料釋出者（以公務機關為例）

（一）（公務員）刑事責任：

1. 倘若資料釋出前業經多方風險評估及測試，且採取適當安全措施，並參酌資訊環境及技術發展等因素持續調整，而依當時科技或專業水準可合理期待重新識別之可能性已微乎其微，應可認為已不具有違法利用個人資料之「故意」，而無個資法第 41 條之刑事責任；又過失行為之處罰，以有特別規定者為限（刑法第 12 條第 2 項），而個資法並無處罰過失行為之刑事責任規定。因此，應不構成刑事責任。

2. 另依 104 年 12 月 30 日總統公布，自 105 年 3 月 15 日施行之個資法修正條文第 41 條規定：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第 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 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」[24]其修正理由乃是考量，倘若非意圖為自己或第三人不法之利益或損害他人之利益，而違反個資法相關規定，因其非難性較低，原則以損害賠償、處以行政罰為已足，爰將此部分之刑事處罰刪除，以維持刑罰之最後手段性。是以，新個資法第 41 條之刑事處罰範圍已有所限縮，須具有「為自己或第三人不法之利益或損害他人之利益」之意圖，始該當該條之犯罪構成要件。

（二）（公務員）行政責任：

個資法無特別規範，故回歸人事相關法令處理，須視具體個案有無人員行政疏失情事，再由該人員任職之機關進行後續懲處或懲戒；倘若機關已訂定標準作業流程，並經第三方驗證通過，而公務員亦確實依循該標準作業流程利用去識別化資料，尚難認為公務員有違法之故意或過失。

（三）國家賠償責任：

1. 依個資法第 28 條第 1 項規定：「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。但損害因天災、事變或其他不可抗力所致者，不在此限。」因此，倘若公務機關未善盡安全維護事項，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，對於當事人須負「無過失之損害賠償責任」，被害人僅須證明「公務機關違反個資法規定」及「損害之發生與公務機關之行為具有相當因果關係」已足，公務機關無法以證明無過失之方式免責。

2. 若公務機關依循標準作業流程對外釋出已去識別化之資料，而該資料被重新識別之可能性已微乎其微，即已非個人資料而無個資法之適用，自無違反個資法規定之問題。倘嗣後卻遭有心人士運用非一般人得使用之特殊技術或知識重新識別而揭露個人資料，進而造成當事人之權利侵害，亦尚難謂其權利侵害與公務機關釋出已去識別化之資料間具有相當因果關係，從而應得免負損害賠償責任。

（四）補救措施：

倘若公開資料依一般人之基準，已被證明易於被重新識別者，公務機關應立即停止提供或自「政府資料開放平臺網站」移除該資料。若是自前開網站移除該資料，公務機關也必須盡一切合理的努力通知資料接收者應刪除、停止處理或利用該資料。考量在開放資料之情形，或許召回資料（recall of compromised datasets）通常已來不及避免損害的發生，但仍是減輕對資料當事人產生之不利負面影響所必要的措施[25]。另此種情形倘符合個資法第 28 條所定國家賠償之要件，公務機關自須對個案權益受損之當事人負損害賠償責任。

二、資料接收者

依個資法第 2 條第 3 款之規定，所謂「蒐集」是指以任何方式取得可直接或間接識別特定自然人之個人資料。若資料保有者所釋出之資料係經加工處理後，資料被重新識別之風險已於合理可接受之範圍，依其呈現方式已無法運用一切合理可能之方法識別特定個人，此時所釋出之資料即非屬個人資料，倘資料接收者嗣後卻運用特殊罕見之技術或方法進行重新識別，進而取得個人資料，應可認為亦屬個人資料之「蒐集」行為，該資料接收者自仍須符合個資法有關蒐集、處理或利用之要件[26]。

以非公務機關為例，其蒐集個人資料須符合個資法第 6 條（特種個資）或第 19 條（一般個資）之規定，而個資法第 6 條第 1 項第 3 款及第 19 條第 1 項第 3 款所定「當事人自行公開或其他已合法公開之個人資料」或第 19 條第 1 項第 7 款所定「個人資料取自於一般可得之來源」，必須以「公開」或「一般可得」者是「個人資料」為前提，無法援用於此種「原接收去識別化資料、嗣後透過各種方法或技術而重新識別」之情形，故須符合個資法第 6 條第 1 項或第 19 條第 1 項其他各款情形之一，方得為之。如有違反者，除行政罰之責任外，若致生損害於他人，則尚可能另構成刑事責任及民事損害賠償責任。

捌 結語

依我國現行個資法之解釋，個人資料去識別化後即已非個人資料，與歐盟、英國、日本、美國等外國立法例均採相同見解。惟隨著資訊科技之進步，網際網路上被公開傳輸或分享之資料日益累積，要完全排除去識別化的資料與其他資料對照、組合、連結而重新識別特定個人之可能性，恐怕日益困難，若不考慮可合理接受之風險或重新識別的技術難易程度，則理論上任何去識別化的資料都可能再被重新識別，而為潛在的個人資料。本文認為，在判斷何種資料有納入個資法規範之必要時，該資料能夠識別特定個人的實際風險應是必須考量的重要因素，當該風險僅是理論上可能、實際上卻是微乎其微，則該資料即不應再被認為是個人資料，從而無個資法適用；否則若將所有資料均納入個資法管制，恐怕已超越立法當時所能預見之管制能量。

鑑於上述考量，本文針對公務機關利用去識別化資料之風險評估及法律責任，提供國外法制實務資料及本文見解供各界參考；並簡介個人資料去識別化過程驗證規範，該驗證機制即是提供相關標準作業流程，協助機關進行個人資料去識別化過程得依循一定要求事項及控制措施，合理控制資料被重新識別之風險，提升去識別化之品質，減少利用去識別化資料之違法性疑慮，使我國為推動「政府資料開放」及「大數據」而合理利用資料的同時，亦能兼顧人格權之保障。

（作者為法務部法律事務司科長）

WEEKLY 周刊 徵稿 各事
一、本刊歡迎兼顧理論與實務、法學新知的作品。文長宜在八千字以內，以利一次刊出。文後請加註本人、本刊並歡迎參考。
二、本刊對來稿有權潤飾，司法院及法官學院的故事，以利出版。
三、文章並無版權，請加註說明；如有違反者，自負法律責任。
WEEKLY 周刊
訂閱
劃撥
號
4377
戶
司法周刊
幣400元
訂閱