生成式AI的隱私保護風險

名家廣場 2023.04.20

／美聯社

文／施汝憬　國際通商法律事務所合夥律師

今年春假筆者飛往美國華盛頓DC，除了欣賞Tidal Basin池畔盛開的吉野櫻外，更重要的任務是參加國際隱私專家協會（IAPP）2023年全球隱私高峰會。本次是2020年Covid-19疫情爆發以來第一次盛大舉辦的實體會議，吸引全球超過5000名關注個茲與隱私保護最新發展的參加者，包括各國政府官員、企業代表、技術人員及法務人員，開場的keynote speaker為Trevor Noah（前美國The Daily Show節目的主持人及知名喜劇演員），閉幕的 keynote panel包括Andrea Jelinek（歐盟個資保護委員會EDPB的主席）、 Elizabeth Denham（前英國資訊委員辦公室ICO首長，現擔任Baker McKenzie的國際顧問）、Max Schrems（奧地利隱私保護行動者，其對Facebook提起的二次個資侵權訴訟導致歐洲法院二度宣告美國與歐盟間的跨太平洋個資傳輸協議無效，對個資跨國傳輸實務產生重大影響，至今仍餘波盪漾），現場目睹幾位重量級人物暢談全球隱私保護的現在與未來，精采程度不輸一場大型演唱會。

不難想像，今年最熱門的議題環繞著近期爆紅的生成式AI（例如美國新創公司OpenAI於2022年11月推出的聊天機器人ChatGPT）的管制與隱私保護議題。

ChatGPT使用大型語言模型 ，以所有網路上公開資料作為數據集（dataset）進行語言模型訓練，目前最新版GPT-4模型的聰明程度已可用於生成、編輯創意或技術內容（文章或程式碼），其商業API並可應用於例如微軟的Bing搜尋引擎、Office軟體，NVIDIA的執行長黃仁勳更稱ChatGPT為「AI的iPhone時刻」。各行各業都在談論如何運用AI改變現有工作方式創造更多價值，或者思考哪些工作內容即將被AI取代，特別是部分白領工作。

然而，機會時常伴隨著風險，我們期望AI改善我們的生活，卻也擔心AI具有不透明、不實資訊、偏見、歧視等風險，尤其是大家對AI仍有魔鬼終結者的想像。歐盟執委會於2021年4月發布以風險為基礎進行管制的人工智慧法草案（AI Act），對於屬於高度風險的AI類型（例如將AI用於員工聘任或解雇之決定）要求必須事前取得合規評估，該法案目前仍在歐洲議會審議中。2023年3月22日包括Elon Musk在內之科技界重要人士以聯名信表達對於AI開發競賽過於迅速的憂慮，呼籲所有AI實驗室立即暫停開發比GPT-4更強大的AI系統至少六個月，並利用這段時間共同製定和實施一套共享的先進 AI 設計和開發安全協議。

在隱私保護方面，2023年3月底義大利個資保護主管機關Garante開了西方國家的第一槍，基於ChatGPT違反歐盟GDPR的疑慮，暫時禁止OpenAI處理義大利用戶資料，並給OpenAI 20日的改善期間，否則將科處2000萬歐元罰鍰，理由包括ChatGPT大規模地蒐集及儲存個人資料以訓練平台之演算法欠缺法定事由（例如經當事人同意），未執行用戶年齡審查（確認是否非屬兒童），及資料外洩、提供不正確資訊等疑慮。歐盟其他國家主管機關也在研擬是否採取措施，或加入義大利主管機關禁用ChatGPT的行列。

OpenAI隨後發布一篇文章表示部分訓練資料中可能包含網路上公開的個人資料，但模型訓練係針對人們使用之語言，而非針對個人資料，且其已在可能的情況下刪除dataset中的個人資料，並調整模型以拒絕用戶有關個人資料之提問。據瞭解，OpenAI已向義大利主管機關提出相關改善措施提案，以期儘快重新向義大利用戶提供服務。

訓練AI的dataset中如包含受著作權保護之內容，蒐集及訓練該等內容可能涉及重製而構成著作權侵害，但訓練出來的模型中倘不包含受著作權保護之內容，則一般認為使用模型本身應無著作權侵權問題。但如訓練AI的dataset中包含個人資料，情況可能不同。2022年美國聯邦貿易委員會（FTC）在一件涉嫌違反兒童網路隱私保護法（COPPA）的和解案中，認定一間行銷供兒童使用的減肥APP及網站的公司，因在未通知父母或取得父母同意之情況下蒐集兒童個人資料而違反COPPA規定，FTC

除了要求該公司刪除其違法蒐集之兒童個資外，更要求刪除由該等違法蒐集之個資所開發之模型或演算法，亦即，將模型或演算法視為「毒樹上的果實」，即便模型或演算法之使用本身並不違法。

> 因應生成式AI的熱潮，許多企業正在探索運用AI的可能性，也有許多企業仍在審慎評估運用AI伴隨的風險。由於用戶在公眾版CHATGPT中輸入的資訊有可能被OPENAI用於語言模型訓練，一旦將工作上取得之機密資訊輸入CHATGPT，可能導致機密資訊外洩之風險，因此，許多企業已發布政策禁止員工在工作上使用CHATGPT，甚至直接封鎖CHATGPT網站連結。

生成式AI的橫空出現，確實創造了徹底改變我們現有生活及工作方式的機會，但其所涉及的隱私保護及其他風險，同樣不容忽視。目前行政院正在規劃各界盼望已久的我國獨立個資保護主管機關，期望未來主管機關參考國外案例經驗及考量我國國情，就AI隱私保護議題提供清楚的指引，讓開發及使用AI的企業得據以遵循，共同推動我國資料經濟的發展。