工商時報

AI應用百工百業 法律風險不容忽視

2025.01.14 / 03:00 / 工商時報　名家廣場

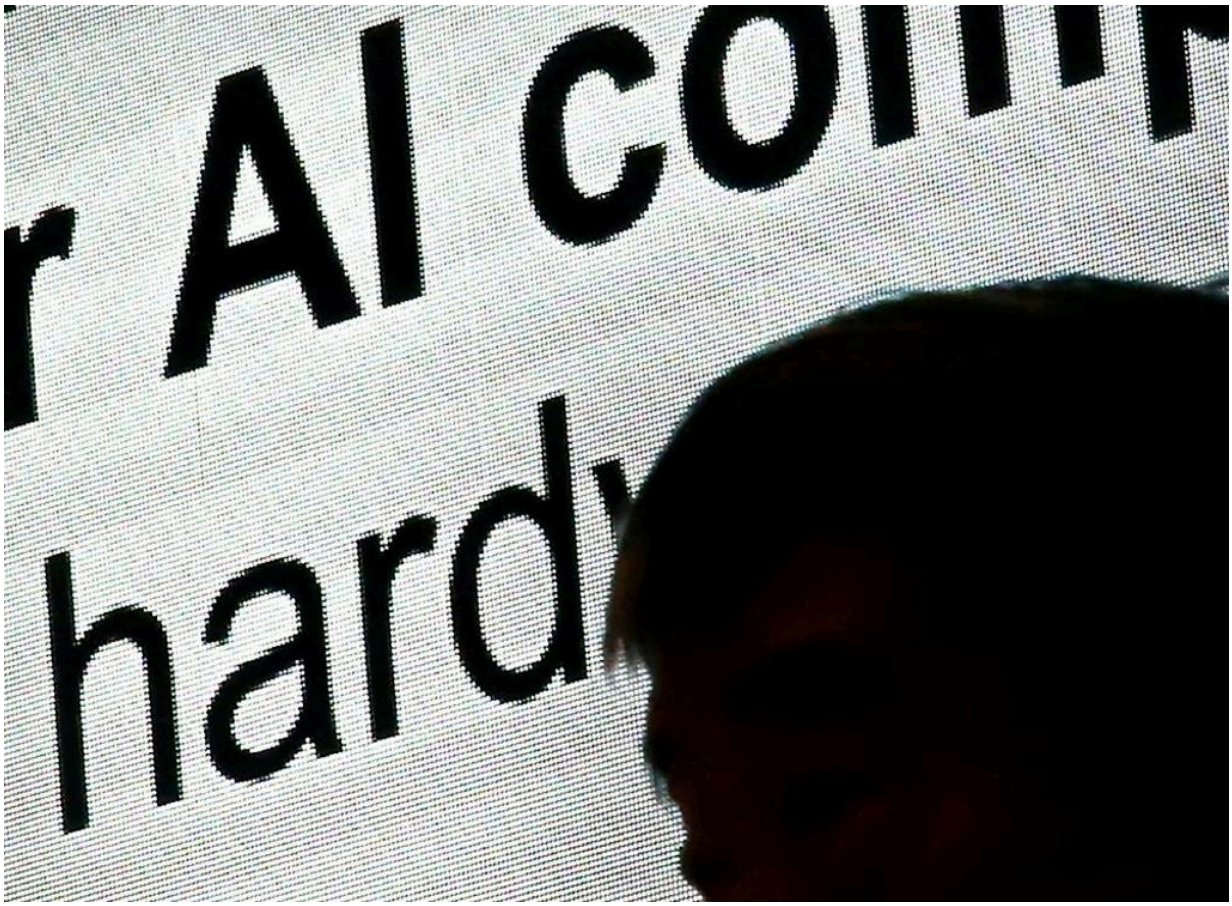

圖 / 本報資料照片

文 / 邵瓊慧、施汝憬■國際通商法律事務所執行合夥律師、合夥律師

自2022年底ChatGPT推出後，全球各種AI的開發及應用如雨後春筍般湧現，各種大語言模型LLM的開發群雄並起、百家爭鳴，這股浪潮迄今方興未艾。而在致力於產業AI化及AI產業化的同時，AI監管、開發及應用所涉及智慧財產權及個資保護議題，也深受各界關注。

歐盟《人工智慧法》已於2024年8月1日生效，其中關於高風險AI相關義務直到2026年8月才生效。儘管其規範效果及對產業的影響仍有待

觀察，其他國家已等不及開始仿效。例如，韓國國會已於2024年12月26日通過《人工智慧基本法》，將從2026年1月開始施行，其規範提供或使用於重要產業之高風險AI系統及生成式AI，違反者最高可處3,000萬韓元（約新台幣70萬元）罰鍰，在特定情形下可能面臨刑責。

在台灣，國科會於2024年7月預告《人工智慧基本法》草案，現已小幅修改後送行政院審查。人工智慧基本法性質上僅為基本法，後續仍待行政院相關部會制定具體規範之作用法。

AI模型的訓練需使用大量資料，可能涉及著作權的重製。國外已有諸多類型的著作權人提起訴訟，主張AI開發商未經同意使用其資料訓練AI模型，構成著作權侵權，AI開發商則主張AI模型訓練屬於合理使用。2025年可望有相關法院就此做成足資參考之判決。

AI模型的訓練資料可能包括大量個人資料，故AI模型的開發及應用亦涉及個資保護議題。2023年3月底義大利個資保護主管機關Garante以ChatGPT違反歐盟GDPR的疑慮，暫時禁止OpenAI處理用戶資料。2024年12月20日Garante正式以違法蒐集用戶個資、未立即通報個資外洩，以及未確實驗證用戶年齡為由，對OpenAI處以1,500萬歐元的罰鍰，並要求OpenAI執行為期六個月的媒體宣導活動，以告知民眾ChatGPT的功能，包括如何蒐集用戶和非使用者資訊來訓練生成式AI，及當事人的權利。

英國資訊委員辦公室（ICO）從2024年1月起，就生成式AI與資料保護之五項議題，提出初步分析並徵詢公眾意見：一、以網路抓取方式訓練生成式AI模型的合法依據；二、生成式AI生命週期中的目的限制；三、訓練資料與模型輸出的正確性；四、對AI模型行使當事人權利；五、在生成式AI供應鏈中分配控管者責任。

ICO於2024年12月13日就徵詢意見結果做出回應，包括四部分：

一、對於以網路抓取方式訓練生成式AI模型，ICO仍認為正當利益為GDPR規定下唯一可能的合法依據。

二、AI開發商未必僅能以網路抓取方式蒐集個資，故AI開發商應說明以網路抓取方式開發AI模型之必要性。

三、網路抓取方式為在當事人不知情下所進行之個資處理行為，對當事人權益有重大影響，當事人在未經告知下難以行使權利，AI開發商可能難以說明其處理行為符合正當利益之利益衡量標準。ICO期望AI開發商大幅改善對當事人之資訊告知。

四、對於訓練資料及訓練好的模型，AI開發商均必須有機制以因應當事人查詢及請求閱覽之權利。採用輸出過濾工具並不足夠，因其並不會移除模型中的個資。

無獨有偶，12月18日歐盟個資保護委員會（EDPB）亦就AI模型之開發及部署階段之四個個資保護問題提出意見：

一、何時及如何可將AI模型視為匿名；二、控管者如何在開發與部署階段證明正當利益為合法依據；三、在AI模型的開發階段違法處理個人資料，會對AI模型之後續處理或運作造成什麼後果？

就問題一，EDPB認為：若AI模型要被視為匿名，直接擷取被用於開發模型的個人資料之可能性，及有意或無意透過詢問取得個人資料的可能性，均應微不足道。

就問題三，EDPB認為：對於在AI模型開發階段違法處理個人資料，各國監管機關可要求之改正措施包括：暫時限制處理、刪除部分或全部資料集、或甚至刪除AI模型。

值得注意的是，EDPB認為：如在AI模型開發階段違法處理個人資料，但確保AI模型匿名後，才將AI模型自行或提供給其他控管者進行後續處理或運作，因GDPR並不適用於匿名後的AI模型，前階段的違法處理並不影響後續AI模型的運作。

AI科技對於百工百業帶來諸多機會，但其所涉及的法律風險，同樣不容忽視。我國個人資料保護委員會籌備處於2024年12月20日預告修正個人資料保護法修正草案，其中增訂主管機關得就個資法之適用及執行訂定相關參考指引。期望個資會就AI開發及應用之個資保護議題提供指引，推動我國數位經濟的發展！