迎接人工智慧時代來臨

淺析使用生成式AI應行注意之法律風險

◎ 李志強／經濟部智慧財產局政風室主任

人工智慧（Artificial Intelligence, AI）泛謂具有人類思考般運作之技術，現處於科技日新月異時代，各領域莫不投入大量資金與人力開發AI系統，各國政府也紛紛鼓勵公部門使用AI來提高處理業務之效率，而生成式AI（Generative AI, GAI）即是其中最常見者，此乃一種電腦程式，旨在創建類似於人類製作（human-made）之新內容，也就是利用機器學習模型來生成原創內容的技術，透過使用者輸入相關提示，自動產生類似人類創作之輸出。

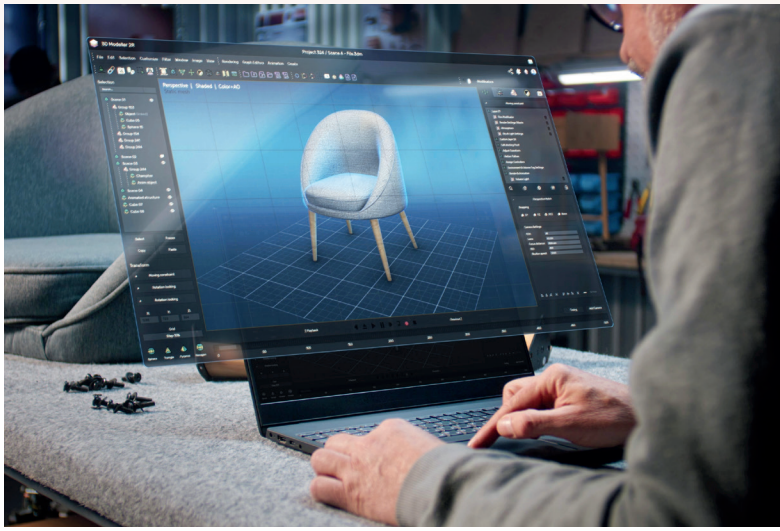
目前坊間生成式AI如雨後春筍般可謂不勝枚舉，其中又以美國OpenAI於2022年11月推出的聊天機器人ChatGPT（Chat Generative Pre-trained Transformer）最為廣泛使用，因容易上手且可因應文書處理、分

析資料、編寫文案及翻譯等需求，大幅減少人力及時間成本，已是個人、企業甚至是政府機關所運用之工具。

可能衍生之風險

使用生成式AI背後可能潛藏哪些風險及法律問題？筆者曾向ChatGPT詢問，據回復資料顯示：使用生成式AI（如ChatGPT、生成圖片工具等）雖然能帶來效率提升與創意靈感，但也存在一些潛在風險，包含內容不準確或誤導、侵犯著作權與智慧財產權、資料隱私與洩露風險、偏見與歧視、淪為惡意用途等。

另向ChatGPT詢問使用生成式AI有何法律風險？本文綜整其回復內容涉及我國法律部分：智慧財產權相關法律（如AI生成的文字、圖片涉及著作權）、《個人資料保護法》（如使用者輸入姓名、電話、地址等個資）、《社會秩序維護法》、《刑法》（如利用生成式AI散布假新聞、假訊息或深偽影片）、《資通安全管理法》（如政府機關使用生成式AI洩漏保密資料）、《消費者保護法》（如利用AI生成內容製作不實廣告或推薦不良商品誤導消費者）、《公平交易法》（如AI平台限制他人資料使用或藉由壟斷訓練資源造成不公平競爭）。



疑義解析及預防之道

以下將就政府部門與社會大眾使用生成式AI常見之疑義提出淺見，並就法律風險提出建言，而有關智慧財產權部分將引用法令主管機關經濟部智慧財產局之見解：

一、民眾使用生成式AI創作是否享有著作權？

首先說明，著作係屬文學、科學、藝術或其他學術範圍之創作，著作必須符合「原創性（非抄襲他人之獨立創作）」及「創作性（具有基本的創意程度）」，始受《著作權法》保護，且著作人於著作完成時享有著作權。

民眾使用生成式AI創作有兩種方式，第一種是「以人工智慧為工具的創作」，也就是人類有實際的創意投入，只是把人工智慧（如繪圖軟體）當作輔助工具來使用，此種透過輔助工具投入創作者的創意而完成之創作成果仍可以受著作權保護，著作權則由該投入創意的自然人享有，除非有《著作權法》第11條（受雇人於職務上完成之著作）及第12條（出資聘請他人完成之著作）之情形。

另一種是「人工智慧獨立創作」，也就是人類並無實際的創意投入，完全是由AI的演算功能獨立進行完成創作，此時由於AI並非自然人，沒有人類精神文明的投入，其創作完成之成果自不屬於《著作權法》保護之著作，原則上無法享有著作權。

二、上傳他人著作至生成式AI是否構成侵權？

使用者上傳他人著作至生成式AI以產出新內容，此種行為因涉及《著作權法》所稱「重製」及「公開傳輸」，亦即若未取得著作財產權人授權，除符合《著作權

法》第44條至第65條所定合理使用外，該利用行為恐將侵害著作權。

因生成式AI並不會針對輸入資料進行來源審查，也不會要求使用者檢附授權證明文件，使用者就其上傳資料之行為應自負法律責任，故使用者上傳資料前應先確認著作權狀態（如取得同意、授權或依法屬於合理使用）。

三、使用者透過生成式AI在網路蒐集資料是否構成侵權？

民眾以人工智慧串接網路資源，以演算法利用網路上之該等著作進行學習，可能會涉及「重製」他人著作之行為，除有符合《著作權法》合理使用規定之情形外，應取得著作財產權人之同意或授權，始得為之。

前述所謂合理使用，經參酌《著作權法》第65條第2項所定利用之目的及性質、所利用著作之性質、質量及其在整個著作所占比例、利用結果對著作潛在市場與現在價值之影響等要件，是否得依此規定主張「合理使用」，仍須個案綜合判斷，尚無一定之標準。

此外，透過生成式AI蒐集網路之資料可能涉及個人資料，從《個人資料保護法》條文可知其範圍非常廣泛，除一般個人資料外（如自然人之姓名、出生年月日、國民身分證統一編號、特徵、指紋、聯絡方式……及其他得以直接或間接方式識別該個人之資料），還包括特種（或稱敏感）個人資料（指病歷、醫療、基因、性生活、健康檢查、犯罪前科），故使用生成式AI若涉及個人資料之蒐集、處理及利用，自當遵循《個人資料保護法》之規範，另若侵犯他人隱私，則又涉及民刑事責任，同理，使用者亦應避免上傳自己或他人之個人資料。

四、使用生成式AI是否可能洩密？

首先說明所謂文書，依《文書處理手冊》所示，指處理公務或與公務有關，不論其形式或性質如何之一切資料。簡言

之，文書並非侷限於公文，也包含與公務有關之任何資訊。

再者，何謂密件？從《文書處理手冊》可知，機密文書區分為國家機密文書（等級區分為絕對機密、極機密、機密）及一般公務機密文書（等級僅有密）。在法源依據部分，國家機密主要是《國家機密保護法》，而一般公務機密則無專法，如《文書處理手冊》揭示，一般公務機密，指本機關持有或保管之資訊，除國家機密外，依法律或法律具體明確授權之法規命令有保密義務者，可見保密條款係散見在不同法令中，我國現行中央及地方（含國營事業）涉及一般公務機密之法令（包含法律、法規命令、行政規則、自治法規、自治條例、自治規則及國營事業之內部規章等）即高達2,300餘種，由此可見其複雜性。

在保密範圍部分，依據《國家機密保護法施行細則》，國家機密包括：一、軍事計畫、武器系統或軍事行動。二、外國政府之國防、政治或經濟資訊。三、情報組織及其活動。四、政府通信、資訊之保密技術、設備或設施。五、外交或大陸事務。六、科技或經濟事務。七、其他為確保國家安全或利益而有保密之必要者，而一般公務機密係在不同法令中有所規定，致使保密範圍不一。

另依實務見解，《刑法》第132條第1項所謂「應秘密」者，係指文書、圖畫、消息或物品等與國家政務或事務上具有利害關係而應保守之秘密者而言，非以有明文規定為唯一標準，個人之車籍、戶籍、前科、通緝、勞保等資料及入出境紀錄，或涉個人隱私，或攸關國家之政務或事務，均屬應秘密之資料，公務員自有保守秘密之義務。綜上，公務員保密範圍並非以明文規定為標準。

最後提醒，保密並非專屬公務員之

義務，凡知悉者均應善盡保密之義務。如《國家機密保護法》即分就洩漏、交付、刺探、收集、毀棄、損壞或隱匿國家機密等不同犯罪行為定其罰則，而《刑法》則定有洩漏或交付國防以外秘密罪之刑責規定，差別在於對違法之公務員加重其刑。

此外，就一般民眾而言，如《營業秘密法》定有妨害營業秘密罪、違反偵查保密令罪，《刑法》定有洩漏業務上知悉他人秘密罪、洩漏工商秘密罪，《個人資料保護法》則定有非公務機關非法蒐集個人資料罪、不法妨害個人資料之正確罪等，可見保密範圍非常廣泛，不可不慎。

五、使用生成式AI有哪些應行注意事項？

利用生成式AI協助執行業務或提供服務，確有助於提升行政效率，然為保持執行公務之機密性及專業性等考量，並促使各機關（構）使用生成式AI有一致之認知及基本原則，行政院經參考各國政府之審慎因應作法，函頒《行政院及所屬機關（構）使用生成式AI參考指引》（以下簡稱本參考指引），此可供政府機關（構）及社會各界參考，重要內容如下：

一、基本原則：使用生成式AI時，應秉持負責任及可信賴之態度，掌握自主權與控制權，並秉持安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱私資訊及不可完全信任生成資訊。

二、參考準則：公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式AI，得準用本參考指引；行政院及所屬機關（構）以外之機關得參照本參考指引，訂定使用生成式AI之規範。

三、判斷義務：生成式AI產出之資訊，須由業務承辦人就其風險進行客觀

且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動。

四、保密義務：製作機密文書應由業務承辦人親自撰寫，禁止使用生成式AI。另不得向生成式AI提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式AI詢問可能涉及機密業務或個人資料之問題。但封閉式地端（註：指機關內不與外部網路連線或資料交換之地端環境）部署之生成式AI模型，於確認系統環境安全性後，得依文書或資訊機密等級分級使用。

五、確認義務：各機關（構）不可完全信任生成式AI產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據。

六、揭露義務：各機關（構）使用生成式AI作為執行業務或提供服務輔助工具時，應適當揭露。

七、法遵義務：使用生成式AI應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。此外，各機關（構）得依使用生成式AI之設備及業務性質，訂定使用生成式AI之規範或內控管理措施。

八、遵守義務：各機關（構）應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守各機關（構）所訂定之規範或內控管理措施。

結語

自人工智慧問世以來，除了影響各個產業結構外，也逐漸改變人類生活。正所謂水能載舟，亦能覆舟，從本文可知，人工智慧確實可能侵害個人隱私、商業利益甚至危及國家安全。因此，我國未來在制定專法促進相關產業發展的同時，亦應確保國家安全及人民基本權利，以免顧此失彼。然正本之道，即是國人應該建立正確資安觀念，例如使用者在輸入或上傳相關資料前，需事先審慎評估風險，因稍一不慎就可能造成難以預料或修復之慘痛結果。