聖島 智慧財產權實務報導
INTELLECTUAL PROPERTY REPORTS

www.saint-island.com.tw siiplo@mail.saint-island.com.tw 28卷11期2026年11月

本期簡介

從使用情境到可追溯責任：企業對生成式AI之智財治理

余惠如 律師

以往企業對智慧財產之管理，較偏向以既有成果之取得與保護為中心，著重於可辨識智慧財產成果之取得、維護及爭議處理，例如專利申請、商標維護、著作權之利用、授權及侵權與訴訟防禦。然而，在生成式 AI 時代，企業所面臨的價值與風險，往往並非於成果形成之後才發生，而是在資訊取得與處理、工作流程運用及使用與回饋中持續累積的動態過程。……詳全文

以Amarin Pharma, Inc. v. Hikma Pharmaceuticals USA Inc.案探討美國最高法院對於學名藥仿單瘦身(skinny labeling)是否涉及誘導侵權之認定標準

劉家宏 專利師

美國於1984年制定了「藥價競爭及專利期間回復法(Drug Price Competition and Patent Term Restoration Act)」(即Hatch-Waxman Act)，允許學名藥廠在原廠新藥的專利權期滿前，提交簡易新藥上市申請(Abbreviated New Drug Application, ANDA)，但為事先釐清學名藥可能的專利侵權爭議，學名藥廠需提出四類聲明中之一者，或是選擇提出「section viii聲明」，將原廠藥仿單中仍受專利保護之適應症或使用方法剔除(即仿單瘦身(skinny labeling))，以避免落入專利侵權之風險。惟，學名藥廠採用仿單瘦身策略，是否即當然足以排除專利侵權的疑慮，仍有待商榷。特別是，實務上不乏出現「跨仿單(仿單外)使用(Off-label Use)」之狀況，根據美國專利法35 U.S.C. § 271(b)，倘若學名藥廠有積極鼓勵、指導或促使他人將該學名藥物用於受專利保護之適應症或用途，便有可能被認定為「誘導侵權」。……詳全文

© 2026 Saint-Island International Patent & Law Offices

本期內文

從使用情境到可追溯責任：企業對生成式AI之智財治理

❖余惠如 律師❖

一、前言：AI不只是工具，AI之治理是對資訊供應鏈的動態治理

以往企業對智慧財產之管理，較偏向以既有成果之取得與保護為中心，著重於可辨識智慧財產成果之取得、維護及爭議處理，例如專利申請、商標維護、著作權之利用、授權及侵權與訴訟防禦。然而，在生成式 AI 時代，企業所面臨的價值與風險，往往並非於成果形成之後才發生，而是在資訊取得與處理、工作流程運用及使用與回饋中持續累積的動態過程。

在此過程中，生成式AI不僅是提升生產效率的單一IT工具，更可能成為企業建構無形資產的驅動引擎。企業原本以「個別權利或靜態成果」為單位之智財管理，也因此面臨新的治理對象：從資訊取得、文本前處理、知識庫建置、模型及相關元件的選擇與調校、到系統測試、部署、監控與更新，均牽涉一整套技術流程與權利關係。企業內部GPT、RAG系統或專用模型，都是由資料、模型、流程與使用回饋共同構成的複合式資產(註1)。

各國、各產業利用AI之情境、技術成熟度暨法令均有所別，本即無統一的治理模式。就臺灣企業而言，本文認為數發部所倡議的先「盤點AI應用情境」，再據以進行後續風險評估與處理的操作邏輯，提供了一個值得採納的AI治理起點(註2)。以下擬藉由一模擬A 公司導入 AI 系統案例，試提出一涵蓋資訊導入、前處理、知識檢索、模型與元件選擇、系統測試、部署、監控的 AI 資訊供應鏈治理藍圖，討論企業如何將一套AI系統從單純的生產力工具，轉化成可盤點、授權、控管、溯源，也能形成競爭優勢的無形資產。

二、AI系統涉及的資產與風險導覽 - 以製造業導入生成式AI為例

(一) 根據使用情境導入AI並規劃風險治理

企業導入生成式AI時，首先需釐清的是AI擬被應用於何種工作、接觸何種資料，以及其輸出將被如何使用。相同的AI技術，若使用於一般文件格式轉換與使用於產品設計或客戶服務，其所涉及的智財、契約、營業秘密及專業責任風險可能截然不同。因此，AI治理宜從「使用情境」出發，再進一步盤點其背後所涉及的資料、技術元件及權利關係進而治理相關風險。

(二) AI系統在智慧製造設備公司的模擬使用情境

假設一中型智慧製造設備A公司，為提升研發、工程、採購及售後服務效率，導入生成式AI作為企業內部知識助理。該系統可整合產品規格書、設備操作與維修手冊、標準作業程序(SOP)、設計變更紀錄、供應商技術資料及常見問題處理紀錄，再結合檢索增強生成(Retrieval-Augmented Generation，簡稱RAG)技術，協助員工能以自然語言快速結合內部知識庫及外部訊息快速查詢應用相關資訊。從智財治理角度觀察，可能涉及以下使用情境與對應風險：

應用情境	AI應用項目	主要資料	主要智財風險	基本治理措施
內部輔助作業	文件摘要、比對、格式轉換	維修手冊等一般內部文件、公開資料	OCR錯誤、版本錯置、錯誤引用	核准工具、文件版本標示、抽樣覆核
研發與工程支援	故障排除建議、設計變更查詢、零件規格比較	技術文件、SOP、設計資料	過時資訊、跨專案資訊洩漏、引用不完整	權限分級、引用來源、版本與有效日期管理
採購與供應鏈	供應商規格比較、替代料建議、技術問答、文件摘要、交期或品質預警	規格書、圖面、材料報告、報價、契約資料	第三方授權限制、營業秘密洩漏、保密義務、競爭法、出口管制、錯誤替代料或品質判斷、供應商資料跨案混用	資料來源與權限清冊、供應商/專案資料隔離、契約審查；人工工程與採購覆核、跨境處理審查、輸出依據與核准紀錄
對外專業工作	客戶企劃書、故障分析報告、設計變更說明	客戶指示、內部分析資料、經核准之技術/材料資料	錯誤內容、機密洩漏、專業責任	人工最終確認、來源留存、工作紀錄

(三) AI系統處理資訊流程

釐清使用情境後，企業可據以決定哪個環節需要導入AI、該環節適用哪些模型，之後再進一步確認AI系統各環節實際運作所涉及的技術與資訊鏈。以A公司為例，一套企業內部AI知識助理可能依序涉及原始文件資訊集、OCR及文字擷取、文件切分與版本管理、知識庫與RAG檢索、基礎模型或任務型模型、Prompt及工作流程，以及最終輸出與操作紀錄等六個環節。各技術環節所涉資料及管理方式亦有差別，例如：採取RAG架構時，

資料未必進入模型訓練，而僅在RAG架構下作為檢索與生成時的參考依據。將A公司的AI系統拆分為下列「**資料來源層→資料處理層→知識檢索層→模型元件層→應用流程層→輸出監控層**」六個層次：

AI系統	示範案例 智慧製造設備公司應用情境	涉及的資產*	主要智財/法律風險	建議保留的治理證據
1.資料與來源層(原始文件)	產品規格書、維修手冊、SOP、設計變更紀錄、技術問答、供應商文件	企業技術資料、Know-how、營業秘密、受授權資料	著作權、營業秘密、契約限制、個資、第三方授權範圍	資料來源、權利人、取得方式、授權依據、保密等級、使用期限
2.資料處理層(前處理程序)	OCR、文字擷取、格式轉換、文件切分、版本比對、結構化整理	結構化資料、文件索引、版本資訊、衍生資料	原始內容之完整性與正確性、轉換成果是否具有可受保護性、原始資料使用限制是否延伸至結構化或向量化成果，及該等成果的存取與管理	原始文件、處理工具與版本、轉換日期、處理結果、版本/校驗紀錄
3.知識檢索層(知識庫)	可能採用的技術：文件切分、文件索引、向量資料庫、RAG(選擇採用)	知識庫專屬索引、檢索規則，與組織方式	越權檢索、跨部門或跨專案資料洩漏、過時文件引用、知識庫資料污染	文件清冊、來源連結、存取權限、更新日期、版本、刪除紀錄、檢索紀錄
4.模型與技術元件層	開源模型、商用模型、微調模型、第三方軟體元件、Adapter	模型配置、模型選型決策、特定任務設定、可能的微調成果	模型授權、開源條款、第三方供應鏈、版本變更、衍生模型或微調成果的權利義務歸屬	模型名稱與版本、授權條款、核准用途、第三方元件清單、變更紀錄
5.應用與工作流程層	系統提示詞(Prompt)、權限配置、工作流程、任務模板、人工覆核機制	企業自有Prompt、工作流程、評測集、專業規則與Know-how	營業秘密、著作權、錯誤自動化處理、權限設計不當、責任歸屬不明	Prompt與流程版本、核准人員、測試紀錄、評測結果、權限設定、變更紀錄
6.輸出與監控層	生成摘要、翻譯、技術分析、故障排除建議、引用來源、操作日誌	人工覆核後的專業成果、回饋資料、錯誤案例、持續改善資料	AI幻覺、過度依賴AI輸出、錯誤引用、機密資訊洩漏、侵權、責任追究困難	輸入與輸出紀錄、引用來源、模型版本、人工覆核紀錄、錯誤事件、改善紀錄

* 附註：以上AI系統涉及的「資產」與「智慧財產權」並非同一概念，後者之取得須符合相關法定要件。企業應先確認其對資料、模型、程式、知識庫及工作流程所擁有的權利及控制程度，再進一步判斷應以著作權、營業秘密、契約或者其他法律工具加以保護。

以下依資訊進入A公司生成式AI系統的路徑依序探討在各層次的AI治理議題。

三、資料與知識庫治理 - 可取得不等於可供AI利用

近三年來，在全球發生的生成式AI相關訴訟多以「著作權」為核心爭點，訟爭集中於受著作權保護內容被用於模型訓練、資料集建構或RAG系統時，是否構成重製、是否落入「合理使用」之審查、以及在後者之情形是否對既有或潛在授權市場造成替代效果。此類問題須由法院根據資料來源、使用目的、技術處理方式及輸出效果個案判斷是否構成侵權，尚無一體適用之結論(註3)。對於製造業而言，這代表即使可合法取得供應商規格書、圖面、製程條件、材料測試報告、報價、品質紀錄及共同開發文件，也不當然代表具有充分的合法權限可以擷取、轉換、切分、向量化此些原始資料、甚至進一步提供生成之資料予其他供應商、其他專案或關係企業檢索利用。因此「處理資料」是進入系統的第一道風險，可考慮以下處理方式：

(一) 將資料來源進行分類

資料根據進入系統的路徑至少可區分為：

- 企業自有資料
- 員工的工作成果
- 客戶或合作方提供的資料
- 公開網站與政府資料
- 付費資料庫及授權內容
- 使用者在系統中臨時輸入的內容

(二) 評估相關風險

由於合理使用的判斷高度依賴具體事實與用途，無法一概推論所有資料用於生成式AI都合法。且下載、轉換、複製、訓練及輸出，在著作權法下涉及不同的行為，是否具備合理使用之各項要件也都需要個案判斷。此外，即便是付費的商業用資料庫，付費授權利用的範圍經常僅限於「可閱覽」或者「限制數量的重製」，付費資料庫不代表可自行向量化、大批量取得轉換為企業知識庫甚至作為商業性輸出(註4)。因此，資料可供利用之程度可能有別，對於每一類資料宜分別評估：

- 企業取得、閱覽或授權使用的範圍為何？
- 是否有權將資料複製、大量擷取、轉換、切分、建立索引或向量化？
- 是否可供RAG檢索、是否可供微調或評測？
- 是否可以將生成的結果提供予內部其他部門或外部客戶？

(三) **RAG的「權利來源」風險**

1. RAG是目前生成式AI發展中一重要架構，RAG結合了「檢索系統」與「生成式AI模型」。在生成資訊時，模型會先從外部資料庫(如外部網站、新聞或付費資料庫)檢索最新相關內容，再根據這些檢索到的資料與模型生成的輸出結合、生成資訊，以提升答案的準確性與時效性。但RAG也可能產生著作權爭議(註5)：RAG所涉著作權風險，通常首先發生於資料匯入、複製、轉換、儲存與檢索等環節；若系統對外輸出大量近似或替代原作內容，亦可能進一步涉及「重製」、「公開傳輸」、「改作」等利用爭議。是否構成侵害，仍須依資料來源、授權內容、技術處理方式、輸出內容與市場影響個案判斷。
2. 因此， RAG並非使資料利用自動合法化的技術；其雖未必改變基礎模型權重，仍可能在資料匯入、轉換、儲存、檢索及輸出等階段涉及受保護內容之重製或利用。企業在利用RAG連結外部資料庫時，應分別確認以下事項：
   - 分別確認外部資料庫之API、robots.txt、網站使用條款、資料庫授權政策、快取與保存政策，以及外部內容是否會被寫回內部知識庫，在後者之情形則需再考量以下事項。
   - 外部資料庫是否只允許閱覽?文件能否被複製、OCR、切分、向量化與索引?
   - 輸出是否替代原作品或原資料庫服務?
   - 向量化之後會否造成資料污染或跨案件之機密洩漏? 亦即，文件能否跨部門、跨客戶或跨供應商檢索?
   - 舊版本的訊息是否仍可能被系統誤予檢索?
3. **製造業特別需要處理的風險-供應商技術資料不當進入共用知識庫**

   供應商的圖面、材料配方、報價、製程條件、測試報告與設計變更資料，常同時受到契約保密條款、營業秘密法、著作權法之保護及限制。因此即使A公司從供應商合法取得文件，也不當然表示可切分、向量化、讓公司所有部門檢索或與其他供應商資料交叉比對。因此，在製造業供應鏈中，企業部署生成式AI也應同時留意採取「資料隔離」措施，避免將不同供應商或不同共同開發專案之資料，未經權限控管即納入企業內部共用之AI知識庫。

(四) 小結：從以上初步分析可見，資料治理已不只是模型訓練或AI系統建置的問題，在此階段重要的是企業如何篩選資料之「可用範圍」與制度上如何建立其「可追溯性」。

四、模型、元件與AI資產之配置與保護

(一) 開放權重模型、商用模型或依授權條款提供之模型並不代表「可無限制利用」

開源模型不等同於「無條件、無風險」之利用，仍受相關授權條件之約束，模型權重、程式碼、套件、相依元件可能適用不同的授權規則(註6)。以Gemma 4 31B開放權重模型(註7)為例，企業仍應依其適用授權條款，確認使用、修改、部署或向第三人提供服務時的條件(註8)。因此在利用開源模型建置企業內部的模型時應先確認其上附加的使用政策、散布條件與揭示義務。以下例示應檢索確認項目：

- 模型權重採取何種授權模式?
- 模型經修改、量化或微調後，是否有標示或散布義務?
- 商業部署是否受到特定條件限制?
- vLLM、OCR工具、嵌入模型及其他元件各自適用的授權條款
- 模型或套件升級時，授權條款是否也有更異，而需重新審查

(二) 建立類似軟體物料清單的「AI元件清冊」以便利盤點

1. 不同技術形式的模型在法律意義上並不完全相同

以客戶訂單規格解析以及語文翻譯為例，可能涉及不同技術形式的微調模型，包括：完整微調模型、LoRA或Adapter、特定系統提示詞、RAG搭配固定工作流程、Few-shot範例以及不同推論參數或模型路由。而不同技術形式的模型，在法律意義上並不相同，例如：

- RAG主要涉及知識庫來源與檢索權限，誤用恐有著作侵權爭議；
- Prompt與工作流程：則更可能涉及企業自身受到營業秘密、著作權或契約保護之資訊。

因此，企業應建立AI元件清冊，至少臚列：模型名稱、版本、來源、授權條款、用途及部署環境，以根據不同的技術態樣區分應用及治理之方式。此外，清冊宜另記載元件之資料流向、是否可將使用者輸入或輸出保留、是否用於模型改良、資料處理地點、次處理者、更新與停用程序，以及發生資安或授權爭議時之通知與修補責任。對於企業自行建置之RAG系統、模型、向量資料庫、OCR工具、外部API與監控工具等，均可能構成獨立元件，不宜只登錄基礎模型。

2. 雲端模型、跨境資料與出口管制

若製造商處理半導體、航太、精密機械、通訊設備或受客戶限制的技術文件，將資料上傳至境外AI服務商，讓境外工程師閱覽、或由境外企業處理，可能涉及個資、技術移轉或出口管制風險。涉及相關技術資料之企業應先確認AI應用的資料處理地點、可存取人員、次處理者及模型訓練政策；必要時應採分

區部署或禁止輸入特定資料類別之方式，避免未經授權之跨境技術轉移。

(三) 專利與營業秘密：企業AI資產的雙軌保護

對多數企業而言，在此階段真正形成競爭優勢的未必是基礎模型本身，而是經過長期累積的專業語料、知識庫結構、任務流程、評測資料及人工校正紀錄、錯誤案例集。這些資料集可能同時受到營業秘密或者著作權之保護。臺灣對著作權雖採創作主義保護，惟仍應視其表達是否具備足夠原創性，且臺灣並未對「資料庫」特予立法保護，實務上對企業更可行的防線經常是採取必要的保密措施、權限控管、員工或供應商契約及版本之管理。

另一方面，對於可由外部產品功能觀察、易於被競爭者逆向推知，且確實具有具體技術貢獻的AI技術方案，企業仍應評估申請專利的必要性。美國USPTO近期在*Ex parte Desjardins*案認定，涉及機器學習模型訓練的方法，如將數學概念整合至實際應用，並具體改善模型的儲存效率、系統複雜度或持續學習能力，可符合專利適格性之要求，並撤銷原依美國專利法第101條所為之核駁，雖然該案不代表所有與AI或機器學習相關的請求項都當然適格(註9)。此外，英國最高法院也在2026年2月於*Emotional Perception* 案中重整電腦實作發明的判斷方法(註10)。總體而言，近期案例顯示：人工神經網絡雖可能構成電腦程式發明，但判斷時仍需辨識請求項是否具有對技術特徵作出貢獻的內容；僅屬抽象規則、商業方法或非技術性結果的特徵，仍不足以支持專利保護。

因此，企業應把AI的具體技術貢獻與資產保護策略合併觀察，倘若是可公開、可逆向且可具體描述之技術問題、技術手段或技術效果：例如降低模型訓練所需儲存量、提高特定資料格式的辨識準確性、改善設備故障診斷流程，或使製造設備控制系統產生可驗證的技術效果，較適合評估以專利加以保護。反之，若競爭優勢主要來自未公開的專業語料、評測集、提示詞、工作流程和人工校正紀錄，且公開專利反而使競爭者容易重建其作法，則透過營業秘密、契約與存取控制通常更合適。

(四) 小結：在此一階段的治理重點在於透過先盤點「AI元件清單」以確認其相關技術性、可公開性與保密可行性等，以決定透過何種權利工具加以保護管理。

五、AI之部署、輸出責任與風險控制

將AI系統落地到日常使用流程，涉及實際應用之責任與風險控制。以下仍以A企業為例，試列AI實際部署時的分層治理及各項內控評測考量點，並根據可能產生的法律風險對應建議平日即宜留存之日誌等證據資料：

(一) 依用途決定控制的強度：

1. A企業將其AI之用途分為三層級，並對應根據不同層級之用途搭配不同程度的管理措施：

使用層級	舉例	控制重點
內部輔助	摘要、格式轉換、文件比對	人工抽樣覆核與錯誤回報
工程或專業工作底稿	客戶指示規格解析、翻譯、以往工作集整理	具資格人員逐項覆核資料來源、版本與結論
對外專業成果或可能影響安全、品質或商業決策者	設計變更圖、客戶企劃報告書	明確指定最終核准人員，並保留核准前後版本及判斷依據
Agent/自動化行動	預測性維護與派工、動態產線排程調度、品質異常追因與改善、供應鏈與採購自動化以及設備故障排除指引	設定授權門檻、雙重核准、金額/設備/客戶資料範圍限制及緊急停用機制

2. **AI不能替代核心的設計變更與品質控制**

對於涉及建議替代零件、設計變更、調整設備操作參數、維修指引或故障原因分析的項目，所涉及之風險為製造業核心的產品安全、品質責任、保固與合約責任。此類核心業務項目中，AI宜定位為輔助分析工具、不應取代既有之工程審查、品質驗證、變更核准及客戶確認程序；如有應用AI生成項目，應保存AI輸出之版本、引用依據、測試結果、人工修改與最終核准紀錄，以備追溯查核。

3. **代理式(agentic)AI與工業系統**

如代理式AI可呼叫ERP、MES、PLM、SCADA或採購系統，治理問題即由輸出內容之正確性擴大為系統行動權限；有鑑於目前技術上對於代理式AI行為之可控性及風險控管仍有疑義(註11)，宜採最小權限、唯讀優先、工具呼叫白名單、雙重核准、可撤銷設計與緊急停用等較高等級治理機制。

(二) AI部署前的評測考慮點

對智慧製造業的應用而言，AI部署前可考量的評測要素包括：

- 技術內容正確性?
- 引用來源是否可追溯?
- 翻譯術語之一致性?

- 對不同文件版本的辨識能力?
- 是否可能揭露其他案件或客戶資訊?
- 面對不確定資訊時，是否會產生幻覺或者捏造答案?

(三) AI部署後應留存的日誌或證據資料

- 使用者之身分及權限
- 所使用的模型與版本
- 檢索到的文件來源
- 重要Prompt或工作流程版本
- 人工覆核者與修改內容
- 錯誤及申訴紀錄
- 模型或知識庫更新紀錄
- 日誌的設計應遵循目的特定、最小必要、分級存取與保存期限原則；對於含有個資、客戶機密或受保護技術資料的prompt、附件與輸出，宜區分一般營運日誌與可供稽核之證據紀錄，並設定遮罩、加密、調閱權限及刪除程序。對非必要的完整prompt、附件原文或高度機密輸出，不宜為了可稽核性而無限制保存，可改以索引號、雜湊值、去識別化摘要或版本識別碼保留可追溯性(註12)。

(四) RAG的「品質、安全與責任」風險

1. RAG技術在企業AI治理中具有雙重意義。一方面，透過限定檢索範圍、呈現引用來源、保存檢索紀錄及搭配人工覆核，RAG有助於降低模型無依據生成內容的機率，並可作為企業已採取輸出品質控制與合理注意措施的證據(註13)。另一方面，RAG的資料匯入、切分、向量化、儲存、檢索與摘要，本身仍可能涉及著作權、契約、營業秘密、個資及資安風險。除「直接Prompt injection(提示詞注入攻擊)」外，外部或內部文件本身也可能夾帶惡意指令，於檢索後形成「間接Prompt injection」; 此外，向量/嵌入層亦可能發生存取控制失效、跨用戶資料洩漏、資料污染或檢索偏移、敏感資訊洩漏以及向量資料庫或檢索內容遭污染等風險(註14)。
2. 因此，RAG雖可改善AI生成資料之可靠性與可追溯性，降低幻覺風險，但仍非侵權或責任的安全港；是否構成侵權，將分別取決於資料取得與利用方式、輸出用途、控制措施與應用之司法領域，企業應用RAG技術架構時仍有需同時對應治理「資料來源之權利」與「輸出責任與可追溯性」議題。以本文的A公司為例，可將前述兩治理問題合併為以下治理表：

RAG問題	主要智財及法律風險	建議保留之治理證據
供應商規格書可否向量化	授權使用範圍、保密義務範圍、營業秘密	資料來源與可用範圍審核表
不同供應商資料能否共用檢索	跨供應商保密、競爭資訊與資料隔離	向量資料庫namespace、權限矩陣
系統引用是否為最新版本	品質、產品責任、決策風險	文件版本、有效日期、檢索與引用紀錄
RAG是否降低錯誤輸出	供應商的合理注意義務、品保義務、責任追溯	評測結果紀錄、來源呈現、人工覆核紀錄
文件是否夾帶惡意指令	Prompt injection、資料污染與資安	文件清洗、信任來源分級、內容掃描與輸入過濾

(五) 小結：目前生成式AI技術之發展有目共睹，治理的問題不在於「能不能用」，而在於「如何負責」。因此，在AI落地使用後之環結，治理的核心應由法律以及技術專業人員協作，具體識別風險發生在哪個技術環節，從而對應採取風險降低措施，以部署可追溯、覆核的AI系統。此外，AI系統上線不是治理的終點，而是持續改善、運作維持以及更新的起點，模型、資料來源、文件版本、供應商條款與使用情境均可能持續變動，企業應保留持續監測、更新調整與停用的機制。

六、結語：如何建立成熟的AI治理模式

AI之導入需要從架構、資料、管理監督及人員能力同步準備，而不是單一附加購買的IT軟體。因此，企業對於涉及AI導入的智財治理對象，也應由單一作品成果或單一模型，擴大為整套AI資訊供應鏈之治理。這有需整合企業內部之法務、資訊、採購、品質與研發業務單位，就資訊流向之各層次資料所涉權利、契約、資安與內控等進行AI生命週期的跨部門統合參與，而非外包給AI系統供應商處理。

數發部在2026年7月發布的「人工智慧風險分類框架」倡導「先盤點應用情境，再識別、評估與應對風險」(註15)，企業可借用其流程作為內控邏輯。此外國際上亦有各種標準管理規範可供參照，例如： 美國國家標準暨技術研究院(National Institute of Standards and Technology，NIST)發布的「人工智慧風險管理框架(Artificial Intelligence Risk Management Framework)與ISO/IEC 42001，NIST強調從治理、情境盤點、衡量到管理的

持續風險控制流程(註16)；ISO/IEC 42001、42005則把AI治理納入組織政策、責任、資料治理、績效評估及持續改善的管理系統。

本文建議企業以AI使用情境為起點，根據使用情境決定控制強度，並沿著資訊與工作流程追溯資料來源、模型選擇、權限配置、人工覆核與輸出責任的資訊供應鏈建立可追溯、可驗證的分級智財治理模式。以製造業為例，可分為以下幾種治理等級(註17)：

等級	企業內的狀態	智財治理方式
第1級：零散使用	員工各自使用工具	無資料清冊、無統一使用規則
第2級：基本控管	有核准工具及使用規範	使用政策及臚列禁止輸入清單、基本教育訓練
第3級：標準化治理	建立受管理的AI 系統與關鍵資產清冊	來源、授權、版本及責任均可追溯。例如：使用單位清冊、資訊來源、模型與元件清冊、權限層級、人工覆核流程
第4級：可驗證治理	可證明運作受到控制，並持續評測、監控與改良	部署前評測、輸出及覆核紀錄、日誌、事件處理紀錄、定期複查及管理階層檢視紀錄

整體而言，目前主流法域對於生成式AI治理的共同方向，在於提升系統運作的透明度、可追溯性與可靠性，並建立相應的人類監督與責任歸屬機制(註18)。AI可協助企業處理資料、檢索資訊、產生初稿或提供分析建議；但對於核心業務、關鍵程序、服務品質以及重大風險，企業仍應保有實質審查、最終決策與責任承擔能力。因此，成熟的AI治理不在於企業使用多少AI工具，而在於企業能否就每一項高影響應用，說明資料從何而來、經過哪些技術與人員處理、輸出如何被覆核，以及錯誤發生時如何追溯、修正與負責。

※ 註釋

1. 根據WIPO與Luiss Business School於2025年7月共同發布的World Intangible Investment Highlights 2025報告指出，無形投資涵蓋研發、軟體、資料、品牌、設計與組織資本，且近年無形投資持續高於有形投資的成長趨勢，可說明資料、軟體與組織資本已成為企業無形投資的重要部分。該篇報導之介紹可參考聖島官網「WIPO：無形資產驅動全球經濟成長」一文。
2. 數發部2026年7月推出的「人工智慧風險分類框架」v1.0主要定位為協助目的事業主管機關識別、評估與應對AI風險，但企業仍可借用其情境識別及風險導向流程建立內部AI治理程序，其餘關於此框架之介紹，可參閱聖島官網近期「AI風險分類框架上路: 企業如何應用四步驟盤點及應對風險」報導。
3. U.S. Copyright Office, Copyright and Artificial Intelligence, Part3: Generative AI Training (pre-publication version, 2025). 有關此篇美國官方報告之介紹，另可參見聖島官網「美國著作權局報告- 訓練生成式AI對著作權的影響」。

4. 以*Thomson Reuters v. Ross Intelligence, Inc.*案為例，Westlaw曾拒絕Ross Intelligence之商業授權邀約，且其網站使用條款亦明文禁止商業利用，Ross Intelligence其後繞道透過第三方LegalEase Solutions付費訂閱Westlaw帳號，間接利用 Westlaw的內容製作法律備忘錄據以開發競爭性的法律研究AI工具，經美國德拉瓦州聯邦地院以即決判決(summary judgment)認定構成著作權侵權，並駁回「合理使用」之抗辯，因此付費或可閱覽的資料庫內容，仍須另行確認是是否可被大量複製、轉換、建置資料集或用於競爭性AI服務。本案詳細討論可參考聖島官網「美國首件判決 - 駁回AI開發商的合理使用抗辯(Westlaw法訊摘要爭議案)」報導。
5. 同前註3。
6. 延伸閱讀：未留意開源軟體之授權條款逕行利用作為AI之訓練材料在臺灣造成之訟爭，可參見聖島官網「近期開源軟體涉及的著作權爭議探討」一文。
7. Google AI for Developers，其中Gemma4 Model Card/Model Overview提供Gemma 4 31B的模型資訊，最後瀏覽日:2026年8月10日。
8. Gemma Terms of Use網頁顯示Gemma 4 31B的適用條款，最後瀏覽日:2026年8月10日。
9. *Ex parte Desjardins,* Appeal 2024-000567, Appl. No. 16/319,040 (P.T.A.B. Sep. 26, 2025)。USPTO已公告將*Desjardins*案指定為先例(precedential)。本所先前就此議題曾進行分析，參見聖島官網「USPTO降低機器學習專利適格性審查門檻：Desjardins先例」一文。
10. Emotional Perception AI Ltd v. Comptroller General of Patents, Designs and Trademarks UKSC3(11 Feb. 2026)。英國政府的UKIPO 審查指引亦已明示依本案判決更新相關審查方式。本案的細節可參考聖島官網「英國最高法院認定AI人工神經網路的專利適格性及其影響（Emotional Perception案）」報導。
11. 關於代理式AI在近期於全球造成的資安議題，可參考聖島官網「失控的代理?－從OpenClaw熱潮論AI代理之治理」報導。
12. AI 提示詞、上傳資料、輸出與對話紀錄，可能同時涉及營業秘密、個資、訴訟證據保全及法律專業保密等問題；企業宜預先建立輸入限制、存取權限、保存期限與刪除程序。此議題之討論可參閱聖島官網「AI不是樹洞? - 從美國近期裁決論AI對話紀錄的訴訟證據風險」報導。
13. 一件中國大陸杭州網路法院審理的「AI幻覺提供錯誤資訊」的民事侵權案件中，因為平台設有「內容可能不準確」的告知，並採用RAG等業界常用技術措施提升內容準確性，法院據此認為平台已盡合理注意義務、欠缺主觀過錯；該案係就特定錯誤資訊及平台注意義務所為判斷，不能推論採用RAG即當然免除其他著作權、契約、保密或資安責任。本案進一步之討論可參照聖島官網「中國大陸首例AI幻覺侵權判決帶來的省思」。
14. OWASP，Top 10 for Large Language Model Applications，最後瀏覽日: 2026年8月11日。
15. 同前註2。
16. NIST，Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile，NIST AI RMF Playbook，最後瀏覽日:2026年8月4日。
17. 本文所提四級AI治理模式，係筆者參考數發部提出以應用情境為起點之AI風險管理流程框架、NIST AI RMF的Govern、Map、Measure、Manage功能所提出的例示性企業自我評估工具，並非法律意見或法定分級標準，業界仍宜根據具體情境選擇適宜合法的治理模式。
18. 有興趣研究者，可參閱聖島官網「美、歐、中、臺現階段對AI的治理模式」一文，整理迄至2026年初世界主流法域的AI治理模式。

* 以上網址若無法瀏覽請使用其他瀏覽器。

本期內文

以Amarin Pharma, Inc. v. Hikma Pharmaceuticals USA Inc.案探討美國最高法院對於學名藥仿單瘦身(skinny labeling)是否涉及誘導侵權之認定標

❖劉家宏 專利師❖

一、前言

美國於1984年制定了「藥價競爭及專利期間回復法(Drug Price Competition and Patent Term Restoration Act)」(即Hatch-Waxman Act)，允許學名藥廠在原廠新藥的專利權期滿前，提交簡易新藥上市申請(Abbreviated New Drug Application, ANDA)，但為事先釐清學名藥可能的專利侵權爭議，學名藥廠需提出四類聲明中之一者，或是選擇提出「section viii聲明」，將原廠藥仿單中仍受專利保護之適應症或使用方法剔除(即仿單瘦身(skinny labeling))，以避免落入專利侵權之風險。惟，學名藥廠採用仿單瘦身策略，是否即當然足以排除專利侵權的疑慮，仍有待商榷。特別是，實務上不乏出現「跨仿單(仿單外)使用(Off-label Use)」之狀況，根據美國專利法35 U.S.C. § 271(b)，倘若學名藥廠有積極鼓勵、指導或促使他人將該學名藥物用於受專利保護之適應症或用途，便有可能被認定為「誘導侵權」。

針對學名藥仿單瘦身及其可能涉及之誘導侵權的認定方式的議題，本所前曾介紹美國聯邦巡迴上訴法院(United States Court of Appeals for the Federal Circuit，下稱CAFC)於Amarin v. Hikma一案(註1)之判決，其中CAFC認定，基於學名藥廠Hikma之仿單內容及其公開新聞稿與網站行銷等內容構成誘導他人侵害原廠藥廠Amarin之系爭專利。此案後經Hikma上訴後，最高法院於2026年6月4日以全票通過的方式，推翻CAFC的判決，其中進一步闡明了原廠藥廠必須提出何種證據，才能基於學名藥的瘦身仿單提出誘導侵權之有效主張。以下將就最高法院判決(註2)做進一步介紹。

二、案件背景與爭議

本案在地方法院的審理階段中，地方法院認為Hikma的仿單不會合理地誘導侵權行為，且Amarin提出的陳述均不構成鼓勵侵權的積極行為。隨後，CAFC推翻了地方法院的判決，認為對於醫師可將Hikma之仿單、網站與公開新聞稿等相關陳述解讀為指示或鼓勵將學名藥開立用於仿單標示外且仍受專利保護之適應症，這種可能性至少是合理的(註1)。

由此可見，本案的核心爭點在於：當醫療照護提供者將學名藥的瘦身仿單、網站資訊及新聞稿等內容理解為可將該學名藥用於受專利保護的適應症(仿單外使用)時，能否視為學名

藥廠已積極的誘導第三方侵害原廠藥的專利？即，Amarin是否已提出Hikma積極鼓勵侵權行為之合理指控，而不僅僅是醫師是否可能合理地將上述相關陳述解讀為侵權的指示。

三、美國最高法院的見解

首先，最高法院依據先前三件專利判決，闡明主張誘導侵權的三個要件：

1. 必須存在第三方所為的直接侵權行為(註3)；
2. 誘導者必須知道誘導行為構成專利侵權(註4)；
3. 誘導者必須「採取積極措施(active steps)」以鼓勵直接侵權行為(註5)。

在本案中，由於Hikma並未爭執前兩項要件，因此最高法院聚焦在第三項要件--積極措施。最高法院指出，「**誘導行為必須涉及採取積極措施(非被動措施)以促成所期望的結果(即專利侵權)**」。換言之，要認定積極誘導侵權結果的成立，必須有會導致侵權結果的直接性表示或行動，而且不論該表示或行動是以隱喻或明喻的方式進行，且對該表示或行動的接受者來說，該誘導是屬於「明確(affirmative)」且「積極」的行為。因此，第三項要件的成立不是第三人是否「可能」將被告的相關表示理解為侵權指示或建議，而是被告「**是否有蓄意，且可歸責的積極誘導表示或行動**」。換言之，即便被告提供的資訊被第三人解讀為「鼓勵進行侵權行為」，仍不會被認定為觸犯美國專利法之誘導侵權責任。又，為避免「干涉正常商業活動」，產品分銷過程中的正常行為並不足以構成法律責任。

就本案而言，最高法院指出，Hikma是否構成誘導侵權的關鍵在於：「誘導侵權的認定不能僅以醫師在接收Hikma提供的訊息後是否可能將其理解為Hikma有指導或鼓勵將學名藥用於仿單指示以外的用途，而是Hikma**是否有採取主動積極的行為鼓勵侵權**」。然而，Amarin用以指控Hikma積極誘導侵權的主張(包括Hikma的學名藥仿單、患者資訊單、官方網站及新聞稿等內容)均未能「超出純粹可能性」，且未提出足夠具體之事實證明Hikma有積極誘導侵權的行為。

具體而言：

1. 最高法院認為Hikma刪除仿單中的心血管使用限制係為符合「學名藥仿單須與原廠仿單相同」之法定要求，不能因此推定Hikma有促成侵權之意圖，且Hikma將其學名藥產品描述為「通用的Vascepa®」或「Vascepa®的通用等效品」，僅是如實的描述學名藥與品牌藥相當，屬於一般產業慣例，不能單憑此即認定其有誘導侵權之行為。因此，Amarin上述主張具有「顯而易見的替代解釋」，若以此認定Hikma侵權，等同將遵守法規及產業慣例的行為認定為違法行為，會使學名藥製造商無所適從。

2. 最高法院未否定Amarin所主張之可能會有人從Hikma的瘦身仿單上遺漏了「心血管適應症的使用限制」，以及新聞稿未「提及Hikma學名藥的核准用途僅限於SH適應症」而得出不當結論的可能性，但再次強調誘導侵權之成立要求必須要有積極的表示或行為，此是為了避免這類「需視情況而定的」的事件鏈干預正常商業活動的進行，否則這種「無論與違法者的關係有多麼微弱，都可能因其商品或服務的任何濫用而需承擔責任」的情況，將使合法商業活動過度暴露於責任風險之下。因此，最高法院強調不能僅依據「單純的遺漏、不作為或未履行職責」作為積極誘導之指控。
3. 就Amarin主張Hikma在其學名藥的資訊單上列出了心血管疾病患者的潛在副作用，並指出藥物有時會被開立用於標籤上未明確指明的用途，醫療服務提供者「很可能會理解」該仿單上的患者資訊單是在鼓勵侵權用途，最高法院認為，以患者資訊單的方式作為誘導侵權的手段係過於迂迴且難以令人信服，若採信此主張而認定有侵權事實，那將來即使是警告人們勿將此藥物用於已獲得專利之使用方法的陳述，都可能被視為積極教唆侵權。此外，針對Amarin主張Hikma官網上將其學名藥的治療類別標示為「高三酸甘油酯血症(hypertriglyceridemia)」，並指出其學名藥的評級為AB，使得所標示的治療類別包含比瘦身仿單中之SH適應症更廣的範圍，最高法院認為，藥物的治療類別並非開立處方的指示，其學名藥的評級為AB僅意謂該學名藥在其仿單所列適應症下與原廠藥相當，且仿單上已排除用於已核准之專利上，因此Amarin針對資訊單及網站內容的主張皆不足以成為Hikma誘導他人侵權的合理理由，因為**不能僅以不明確的用語結合猜測他人可能會有什麼行為來判斷**。
4. 最後，針對Amarin主張Hikma發佈的新聞稿中關於Vascepa在美國的銷售數據同時包含了SH和CV兩項適應症的銷售數據，以此來指控Hikma鼓勵以其學名藥用於CV適應症，最高法院認為此主張最不明確，且有過多未加詳述的推論。同時，法院也指出，新聞稿的主要受眾是投資者，而非醫師或藥師，而醫師和藥師還需要具備藥物銷售相關背景知識去理解新聞稿內容，並將其解讀為可將學名藥用於CV適應症。當然，法院也不否認這條事件鏈所描述的情景確實「可能」發生，但也「僅是可能」，不能據此認定主動誘導行為一定會發生。

綜上所述，最高法院認為，Amarin的主張僅是基於Hikma各種與學名藥相關的表示來提出一套合乎情理的事件鏈，說明Hikma的各項表示「有可能」促使醫療照護提供者開立處方或調配Hikma的藥物以用於降低患者的心血管風險。但不論將這些表示單獨或結合進行檢視，都無法證明Hikma有採取任何具體的「積極誘導」的主動行為鼓勵第三方侵害Amarin的CV適應症專利。

四、結語

由上述判決結果可知，對於學名藥廠採取仿單瘦身之策略是否涉及誘導侵權之爭議，美國最高法院強調原廠藥廠需提出「積極、具體且可歸責於被告的表示或行為」，來證明被告有誘導第三方侵權，若僅僅知道產品有侵權可能，並不能據此認定誘導侵權成立。因此未來在相關訴訟中，原廠藥廠若要主張學名藥廠有誘導侵權的行為，必須更明確提出學名藥廠有**具體且合理的積極鼓勵侵權行為之**證明，而無法僅憑推測性、可能性之主張。對於學名藥廠而言，雖然最高法院肯認瘦身仿單的合法性，但在學名藥的後續推廣及銷售過程中仍需更加審慎留意避免任何可能被認定為構成誘導侵權的作為或表示。

※ 註釋

1. 聖島國際專利商標聯合事務所，實務報導2025年第27卷01期：
   以Amarin Pharma, Inc. v. Hikma Pharmaceuticals USA Inc.案探討美國學名藥仿單瘦身(skinny labeling)制度及其涉及之誘導侵權認定。
2. Hikma Pharmaceuticals USA Inc. v. Amarin Pharma, Inc., No. 24–889, 608 U.S. _ (2026).
3. Limelight Networks, Inc. v. Akamai Technologies, Inc., 572 U. S. 915, 920–921 (2014).
4. Global-Tech Appliances, Inc. v. SEB S. A., 563 U. S. 754, 766 (2011).
5. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U. S. 913, 937 (2005).

聖島國際法律事務所
SAINT ISLAND INTERNATIONAL LAW OFFICE
聖島國際專利商標聯合事務所
SAINT ISLAND INTERNATIONAL PATENT OFFICE

總所 台北市松山區105403南京東路三段248號7樓 TEL:(02)2775-1823 FAX:(02)2731-6374
法律 台北市松山區105403南京東路3段248號12樓之2 TEL:(02)2775-1823 FAX:(02)8773-6131
台北 台北市中山區104451敬業一路99號2樓 TEL:(02)7702-8299 FAX:(02)7702-8289
台中 台中市西區403406臺灣大道二段220號32樓 TEL:(04)2328-8218 FAX:(04)2328-8318
台南 台南市東區701024裕農路375號11樓 TEL:(06)274 - 2266 FAX:(06)238 - 0527
嘉義 嘉義市西區600001垂楊路505號6樓之1 TEL:(05)285 - 1586 FAX:(05)285 - 1595
高雄 高雄市前金區801301中正四路211號14樓 TEL:(07)216 - 3721 FAX:(07)216 - 2588