# 生成式AI的著作權法律風險——以RAG應用為中心

蔡毓貞＊

## 壹、導論：從生成式AI的挑戰到RAG的興起

生成式AI技術雖發展迅速，卻面臨「幻覺」、「不透明」與「知識時效性不足」等根本挑戰[1]。例如，美國已發生多起律師在書狀中引用生成式AI虛構裁判的事件[2]，導致律師受到裁罰。為此，「檢索增強生成」（Retrieval-Augmented Generation，下稱RAG[3]）技術應運而生[4]，透過結合大型語言模型（Large Language Models, LLM）（下稱大模型）的強大生成能力與外部知識庫的即時檢索能力，實現「先查證、再生成」，以提升回應的準確性與即時性[5]。

＊本文作者係執業律師，理慈國際科技法律事務所合夥律師。
（本文為作者個人意見，不代表理慈國際科技法律事務所之立場。）

註1：Gao, Y., Xiong, Y., Gao, X., Jia, K., Pan, J., Bi, Y., Dai, Y., Sun, J., Wang, M., & Wang, H. (2023). Retrieval-augmented generation for large language models: A survey. *arXiv preprint arXiv*:2312.10997. https://doi.org/10.48550/arXiv.2312.1099

註2：Mata v. Avianca, Inc., No. 22-cv-1461 (PKC), Opinion and Order on Sanctions (S.D.N.Y. June 22, 2023). United States v. Cohen, No. 1:18-cr-00602-JMF, Opinion and Order (S.D.N.Y. Mar. 20, 2024). *Stephanie Wadsworth v. Walmart Inc. & Jetson Electric Bikes, LLC*, 2:23-CV-118-KHR, Order on Sanctions and Other Disciplinary Action, United States District Court for the District of Wyoming (Feb. 24, 2025).

註3：Facebook AI研究員Patrick Lewis受訪時曾提及，「RAG」在英文裡有抹布的意思，他們也想過取個更稱頭點的名字，但當時沒料到這個技術會如此受到歡迎，又忙於發表論文，實在沒時間想其他的名字。Alex G. (2023, December 19). From RAG to Riches: Retrieval-Augmented Generation Explained. Medium. https://medium.com/@alexgnibus/from-rag-to-riches-retrieval-augmented-generation-explained-2f55efdc7fa6.

註4：Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W., Rocktäschel, T., Riedel, S., & Kiela, D. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. *arXiv preprint arXiv:2005.11401*. https://doi.org/10.48550/arXiv.2005.11401.

註5：劉育維（2023），《RAG 檢索增強生成──讓大型語言模型更聰明的秘密武器》，載於：https://blog.infuseai.io/rag-retrieval-augmented-generation-introduction-a5854cb6393e（最後瀏覽日：2025年6月19日）。

然而，RAG的廣泛應用已引發著作權訴訟，如美國Perplexity[6]案及Cohere[7]案，使其法律風險評估成為迫切課題。美國著作權局在2025年5月的報告中指出，RAG是許多AI產品的重要功能，其應用也成為新聞媒體業者關注的議題[8]。日本文化廳早在2024年5月發布相關指引[9]，明確將AI訓練過程納入「非享受」著作的例外情形，即依照日本著作權法第30條之4「非以享受著作中所表現出之思想或感情為目的之利用」，可評價為通常不會損害著作權人利益之類型。該指引認為RAG應用不屬於「非享受」類例外[10]。

雖然國內對於生成式AI在「預訓練」與「微調」的著作權議題已有相當討論[11]，但對RAG應用所衍生著作權法律風險的關注仍屬有限[12]。鑑於RAG技術發展迅速且可能為我國廠商普遍採用，本研究擬深入探討其著作權法律風險與相應的合規策略。

美國訴訟實務顯示，原告多採取「分階段評價模式」，主張單是RAG在建置索引階段的大規模複製行為，就足以構成侵權。本研究認為此模式忽略RAG作為整體技術系統的本質，無法準確評估其對著作權人利益的實質影響。因此，本文旨在建構並論證一套適用於RAG應用的「混合評價模式」。此模式整合不同思維，主張先進行分階段的表面侵

註6：2024年10月，華爾街日報及紐約郵報母公司控告Perplexity AI公司提供的「perplexity」服務侵害其著作權，這是全球首件針對RAG架構AI服務的著作權訴訟。

註7：2025年2月，包括富比士、衛報和洛杉磯時報等十多家知名新聞、雜誌和數位出版商控告Cohere公司侵害其原告的著作權等。

註8：U.S. Copyright Office (2025, May). *Copyright and artificial intelligence: Part 3: Generative AI training (Pre-publication version)*. https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf ( “We note that RAG is an important feature of many AI products, and that RAG-related uses are of particular concerns for news media stakeholders.”).

註9：Agency for Cultural Affairs, Japan (2024, May). *AI and copyright in Japan: Overview*. Legal Subcommittee under the Copyright Subdivision of the Cultural Council, Japan Copyright Office. https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf

註10：林欣儀（2024），〈簡介日本文化廳關於AI及著作權之看法〉，《萬國法律》，第258期，第76-87頁。

註11：章忠信（2025），〈著作權──生成式AI的加速器或絆腳石？〉，《金融科技法律》。章忠信（2024），〈人工智慧訓練與著作之合法利用〉，《智慧財產權月刊》，304期，第5-26頁。陳俞安（2025），〈生成式AI與著作權議題之國際趨勢〉，《智慧財產權月刊》，316期，第5-29頁。徐龍、鄭冠宇（2023），〈論機器學習之著作權困境與應對〉，《臺大法學論叢》，第52卷第2期，第391-475頁。葉奇鑫、許斌（2024），〈AI大語言模型訓練與著作權合理使用之思考──以紐約時報對OpenAI訴訟案為中心〉，《全國律師》，28卷第6期，第18-19頁。陳家駿（2023），〈從美國人工智慧擴散模型訴訟案---談生成式AI圖像之著作權侵權議題〉，《智慧財產權月刊》，298期，第6-35頁。陳家駿（2022），《AI人工智能vs智慧財產權》，元照。陳家駿、許正乾、林宜柔合著（2024），《AI/ChatGPT v. 智慧財產權美國生成式AI案例評析》，元照。

註12：廖先志、陳鍾誠（2025），〈大型語言模型在訓練階段與使用檢索增強生成的著作權風險挑戰及案例研究〉，《智慧財產權月刊》，317期。

權判斷，再從系統整體評價合理使用等抗辯事由的適用性，期能在鼓勵創新與保護著作間取得平衡。

本研究採文獻分析法與比較法研究方法，探討混合評價模式在美國、歐盟及我國法制下的適用性。

## 貳、RAG運作機制與發展

為準確進行法律評價，須先深入理解RAG技術。

### 一、RAG運作機制

RAG運作可細分為以下步驟：

**（一）資料擷取階段：**RAG應用的基礎，此階段涉及：

1.文檔解析（Parsing）：讀取不同格式的檔案。

2.文本分塊（Chunking）：將長文本切分成較小的、語義連貫的片段。

3.嵌入生成（Embedding Generation）：使用嵌入模型將文本塊轉換為數值向量，以捕捉其語義。

4.向量存儲與索引（Vector Storage and Indexing）：將向量化的文本塊存入專門的向量數據庫，並建立索引以便快速搜索。

**（二）檢索（Retrieval）：**當收到使用者查詢時，系統將查詢同樣轉換為向量，並在向量數據庫中進行語義搜索，找出與查詢最相關的文本塊。

**（三）增強（Augmentation）：**系統將檢索到的相關文本塊，連同原始使用者提示，一起打包成一個「增強提示」。

**（四）生成（Generation）：**大模型接收此增強提示，並基於其中豐富的上下文資訊來生成最終回答。

### 二、RAG的演進：從原生到代理

隨著技術發展，RAG的架構已從簡單走向複雜，主要類型包括：

**（一）原生RAG（Naive RAG）[13]：**最基礎的線性流程，執行容易但精準度有限。

**（二）高級RAG（Advanced RAG）[14]：**引入「查詢擴展」或「重排序」等技術以提升檢索精準度。

**（三）模塊化RAG（Modular RAG）[15]：**將系統拆解為搜索、記憶、路由等多個可動態配置的模塊，提升靈活性。

**（四）代理式RAG（Agentic RAG）[16]：**最新的發展是結合能規劃、思考和執行多步驟任務的自主「代理」（Agent），能主動分解複雜問題、進行多輪搜索與評估。如OpenAI及Gemini推出的Deep

註13：See *supra* note 1.

註14：*Id.*

註15：*Id.*

註16：Singh, A., Ehtesham, A., Kumar, S., & Khoei, T. T. (2025). Agentic retrieval-augmented generation: A survey on agentic RAG. *arXiv preprint arXiv:2501.09136*. https://doi.org/10.48550/arXiv.2501.09136

Research[17]，即為典型範例，能生成類似人類分析師所作的全面研究報告。

## 參、RAG應用的著作權法律風險

RAG應用對傳統著作權侵權評價模式構成挑戰。

### 一、既有評價模式的觀察與檢討

#### （一）分階段評價模式

在*Perplexity*[18]案與*Cohere*[19]案中，原告媒體集團均採取「分階段評價」的訴訟策略。他們主張，被告的RAG服務在建置索引或擷取資料的「輸入階段」，就未經授權大規模複製其受著作權保護的新聞內容[20]，此行為本身即構成侵權[21]，無須證明最終的「輸出內容」與原著作構成實質近似[22]。

此模式對原告而言，訴訟上較為便利，因其僅需聚焦於前端明確的複製行為，而無須證明難以捉摸的「輸出實質近似」。然而，此種觀點存在明顯割裂技術的缺點，完全忽略RAG作為一個整合系統的轉化性用途與社會價值。若採此模式，任何在前端複製受保護資料的RAG應用，都可能被直接認定為侵權，這將扼殺許多有益的創新。

#### （二）整體評價模式

與分階段模式相對的，是將RAG應用視為一個不可分割的整體，從其最終目的與功能進行法律判斷的「整體評價模式」。此模式的優點在於契合RAG技術各階段功能上緊密整合的特性，能從系統的最終產出與社會價值（如促進知識發現）進行宏觀評估，避免過度拘泥於前端的複製行為。

然而，其最大缺點在於可能完全忽略前端行為的法律性質。由於評價重點完全集中在

註17：OpenAI. (2025, February 2). Introducing Deep Research. https://openai.com/index/introducing-deep-research/

註18：Dow Jones & Co. v. Perplexity AI, Inc., No. 24-cv-7984 (PKF), United States District Court for the Southern District of New York, filed October 21, 2024.

註19：Advance Local Media LLC et al. v. Cohere Inc., No. 1:25-cv-01305 (S.D.N.Y. Feb. 13, 2025).

註20：原告主張Cohere標榜以RAG技術提供「值得信賴」、「可驗證」的答案，事實上，用戶透過「Chat」功能，可以取得與原告著作幾乎相同的新聞報導或付費文章。

註21：Id, Complaint, at 4 ( “Perplexity's actions at the input stage-copying without authorization massive amounts of Plaintiff's copyrighted works for inclusion into Perplexity's RAG index-constitute completed and massive copyright violations without even a colorable fair use. The illegality of this massive copyright violation at the input stage does not depend on whether the particular outputs of Perplexity's so-called ‘answer engine’ are sufficiently similar in each instance to the copyrighted works of Plaintiffs as to constitute identical reproductions of those works. It is sufficient that Perplexity makes copies of Plaintiffs' works on a grand scale to create reproductions and/or derivative content that is designed as a substitute for Plaintiff's works.” )

註22：原告主張Cohere標榜以RAG技術提供「值得信賴」、「可驗證」的答案，事實上，用戶透過「Chat」功能，可以取得與原告著作幾乎相同的新聞報導或付費文章。Cohere. (2023, September 28). Introducing Chat with Retrieval-Augmented Generation (RAG). https://cohere.com/blog/chat-with-rag

系統最終的抽象「目的」，著作權人將難以就其著作在前端被大規模、系統性複製的明確行為有效主張權利。這種作法可能導致「目的正當即可不問手段」的道德風險，削弱著作權法對重製權的基本保護。

## 二、針對RAG應用建構混合評價模式

鑑於前述兩種模式的缺點，本研究主張採用「混合評價模式」，為RAG這項兼具「明確前端行為」與「整體創新目的」的特殊技術，建構一個更務實及衡平的法律分析方式。

### （一）混合評價模式的結構

#### 1.階段一：表面侵權之分階段判斷

此階段旨在釐清RAG應用的各個技術環節是否涉及著作權法所管制的行為，構成表面上的侵權（prima facie infringement）。例如，在資料擷取階段，若未經授權系統性地複製他人著作以建立知識庫（如爬取公開網頁），即可能構成表面上的重製權侵害[23]。在檢索階段，系統根據查詢從知識庫檢索相關片段，此處涉及的複製行為通常是暫時性、技術性的，需判斷是否符合「暫時性重製」的例外要件。在生成階段，若系統回應的內容與原著作構成「實質近似」，則可能同時涉及重製權與改作權或公開傳輸權的侵害；若僅為少量引用或提供摘要，則爭議程度相對較輕，需個案判斷。

#### 2.階段二：抗辯事由之整體評價

當RAG的某一階段被認定可能構成表面侵權時，便進入是否存在合理使用等抗辯的判斷，此時不再割裂看待技術環節，而是將RAG應用作為一個「整體」來綜合考量。例如，一個輔助學術研究的RAG，若在輸出端採取了有效措施（如限制輸出長度、避免直接複製、提供來源標註）以降低市場替代效應，其被認定構成合理使用的可能性便會提高。

### （二）各種評價模式的比較

| 比較面向 | 分階段評價模式 | 整體評價模式 | 混合評價模式 |
|---|---|---|---|
| **分析起點** | 從「單一行為」出發，逐一檢視資料擷取、檢索等各階段的獨立行為是否侵權。 | 從「整體目的」出發，直接評估RAG系統的最終功能、社會價值與市場影響。 | 從「分階段行為」出發，再到「整體目的」。第一步判斷表面侵權，第二步才從整體評價抗辯事由。 |
| **對前端複製行為的處理方式** | 作為核心侵權事實，將前端大規模、未經授權的複製行為直接作為主要的侵權主張。 | 可能忽略或淡化，可能因其「目的良善」而將前端的複製行為輕易地合理化。 | 明確承認與審視，第一步即正面處理前端的複製行為，承認其可能構成表面侵權。 |

註23：在我國，可能構成著作權法第22條重製權的侵害。此階段的法律風險主要在於大規模複製他人著作建立知識庫。

| 比較面向 | 分階段評價模式 | 整體評價模式 | 混合評價模式 |
|---|---|---|---|
| **對著作權利人的保障** | 主張侵權上較便利，但可能因評價片面，無法反映真實損害。 | 較弱。權利人難以就著作被明確複製的事實有效主張權利。 | 較強。此模式先確認權利可能受侵害，再將舉證責任轉移給利用方證明其行為可構成合理使用等抗辯。 |
| **法律分析的邏輯** | 割裂式分析，將連續的技術過程拆解成獨立的法律事件，可能與技術現實脫節。 | 一步到位的宏觀衡量，但可能忽略了侵權行為構成要件的判斷。 | 兩步驟的結構化分析，先判斷「請求權基礎」（是否侵權），再判斷「阻卻違法事由」（是否有合理使用抗辯），邏輯嚴謹。 |

### （三）混合評價模式與直接合理使用分析之差異

混合評價模式看似與直接合理使用原則進行分析無異，但兩者在結構與側重上存在根本不同，此差異對於RAG至關重要。兩步驟的混合評價模式是有意識地「矯正及整合」分階段與整體的兩種極端思維，提供一個「結構化的中間路徑」，首先正視前端複製行為（階段一），隨後將視角拉高至系統整體來評估其創新價值與市場影響（階段二）。

### （四）混合評價模式之理論基礎

#### 1.著作權侵權判斷的基本邏輯

著作權侵權的判斷邏輯，本質上就是一個二階段的過程。無論在英美法系還是大陸法系，都包含兩個層次：首先是表面侵權行為（prima facie infringement）的認定，其次是抗辯事由（如合理使用、法定例外）的檢視。此種分析架構為建構「混合評價模式」提供堅實的法理基礎。

#### 2.混合評價模式才能準確掌握RAG技術的核心特徵

RAG技術的核心特徵在於其資料擷取、檢索及生成三個階段的緊密整合與功能上的不可分割性，共同達成經外部知識源驗證、更為可靠資訊的最終目的。由於大模型基於這些被外部知識「增強」過的提示生成最終回答，部分學者因此視RAG為一種高階提示詞工程（advanced prompt engineering）[24]。此種「先查證、再生成」的運作機制，本質上即要求從一個連續且完整的系統功能角度進行審視，而非將各環節孤立評價。

分階段評價在「表面侵權判斷」中的必要性：RAG在資料擷取、檢索與生成階段，涉及不同的技術行為與法律評

註24：Venkatesh, K., Dalva, Y., Lourentzou, I., & Yanardag, P. (2024). Context Canvas: Enhancing text-to-image diffusion models with knowledge graph-based RAG. *arXiv preprint arXiv:2412.09614*. https://doi.org/10.48550/arXiv.2412.09614（“Retrieval Augmented Generation (RAG) is a prompt engineering technique that improves the relevance and accuracy of a generative model's response, while reducing hallucinations.”）

價。例如，資料擷取階段的大規模複製與檢索階段的暫時性重製，在法律性質上有本質差異。採用分階段分析，有助於精確識別各環節是否落入著作權法所管制的行為範疇（如重製權、改作權），並為不同類型的RAG應用（處理公開網路資料vs.使用者私有資料）提供差異化的風險評估基礎。

整體評價在「抗辯事由判斷」中的重要性：合理使用等抗辯事由的判斷，本質上即要求進行綜合性的利益衡量。美國最高法院在指標性的*Campbell*[25]案中即強調，合理使用分析需要「個案的、整體的」（case-by-case, holistic）判斷。將此原理應用於RAG，意味著在判斷其是否構成合理使用時，不應割裂地看待各技術環節，而應從系統的整體功能、社會價值與市場影響進行綜合評估。

**3.混合評價模式符合RAG技術發展方向**

針對RAG應用為降低著作權風險而持續演進的技術解決方案，例如旨在透過控制資訊處理與內容生成的整體流程，結合私有資料庫共同資訊並丟棄獨特可識別部分，以確保最終輸出能兼顧資訊利用與著作權保護的CPR（Copy-Protected Generation with Retrieval）[26]方法，其設計理念亦著重於對RAG應用整體運作進行合規管理與風險控制，此與整體評價模式重視系統性設計、最終產出效果及整體影響的精神不謀而合。

## 三、RAG與基礎模型採用不同評價模式的必要性

雖然一般的生成式AI（如GPT、Gemini等基礎模型）的著作權爭議常被簡化為「輸入」（訓練資料）與「輸出」（生成內容）兩端的評價[27]，但RAG技術之所以需要採用更複雜的「混合評價模式」，其根本理由在於RAG的技術架構與運作目的，與基礎模型有著本質上的不同，分述如下：

### （一）RAG的技術整合性使其不宜被割裂評價

RAG的核心特徵在於資料擷取、檢索及生成三個階段的「緊密整合與功能上的不可分割性」。與基礎模型的「訓練」和「生成」在時間與功能上可以區分不同，RAG的前端

註25：Souter, D. H., & Supreme Court of the United States. (1994). *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569. Retrieved from https://www.loc.gov/item/usrep510569/

註26；A. Golatkar, A. Achille, L. Zancato, Y.-X. Wang, A. Swaminathan, and S. Soatto, "CPR: Retrieval augmented generation for copyright protection," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2024, pp. 12374-12384. See also N. Vyas, S. Kakade, and B. Barak, "On provable copyright protection for generative models (Version 2)," arXiv preprint arXiv:2302.10870, 2023. [Online]. Available: https://doi.org/10.48550/arXiv.2302.10870.

註27：徐龍、鄭冠宇（2023），〈論機器學習之著作權困境與應對〉，《臺大法學論叢》，第52卷第2期，第399頁。

「資料擷取」是為了後端「生成」更可靠的內容而服務的，兩者共同達成一個「先查證、再生成」的單一、連續的系統目標。此種「先查證、再生成」的運作機制，本質上即要求從一個連續且完整的系統功能角度進行審視，而非將各環節孤立評價。因此，純粹的將RAG分階段評價，將此一體化過程割裂，與RAG技術的運作現實完全脫節。

**（二）RAG的輸出可追溯性使其與基礎模型有本質區別**

基礎模型採用輸入與輸出分開評價的一個重要原因，就是輸入端的訓練資料過於龐大，與輸出端的內容難以進行侵權比對，甚至難以追溯輸出的資料來源。相對地，RAG的輸出並非像基礎模型那樣從一個龐大、抽象的參數空間中生成，而是直接被檢索到的具體資訊片段所「增強」（Augment），並且可以追溯資料來源。亦即，RAG輸出內容與特定原著作的關聯性更強、更直接，也更容易進行侵權比對。從而，RAG應用者在技術上也有採取技術措施（如限制輸出長度、避免生成與單一原著作實質近似的內容、設置引用頻率上限等）以避免侵權的可行性。

**（三）「混合評價模式」是唯一能兼顧行為與目的之評價方案**

若只採「分階段評價」，可能陷入「見樹不見林」的困境。此模式雖然能精確指出「資料擷取」階段的複製行為構成表面侵權，但卻完全忽略這個複製行為的最終目的是為實現一個可能具有高度社會價值的整體功能（例如，輔助醫療診斷、加速科學研究）。導致任何RAG應用只要在前端複製受著作權保護的資料，就直接被認定為侵權，將扼殺所有真正有益的創新。

若只採「整體評價」，將陷入「目的正當即可不問手段」的盲點。此模式雖然看到RAG應用的整體創新價值，但卻可能完全忽略前端「建庫」行為對著作權人重製權的直接侵害。這會讓權利人難以就其著作被明確複製的事實主張權利，從而過度向技術開發者傾斜，違反著作權法的保障著作權著作權益的基本理念。

## 四、RAG與基礎模型之法律分析差異

**（一）RAG與基礎模型的合理使用比較**

RAG應用與基礎模型雖然共享部分法律原則，但審查的重心完全不同，基礎模型的分析焦點是前端「訓練行為」的合法性（因為生成行為的侵權證明不易），而RAG的分析則聚焦於後端「應用服務」之整體目的、功能與市場影響。因此，基礎模型是否侵權，未必適用於RAG應用，兩者的法律分析並非命運共同體，應依照個案情形分別獨立評價，分析如下：

**1.若基礎模型被判定侵權，RAG未必隨之敗訴**

若法院認定基礎模型構成侵權，其理由可能是該訓練行為設計對海量、未經篩檢的網路資料進行全面複製，其目的是為了打造一個通用的商業模型，該行為直接損害內容市場。然而，一個設計良好的RAG應用，其合理使用的主張是建立在「利用模型進行檢索與分析」，因此抗辯的理由會側重於明確的轉化性目的（如進行科學研究、輔助醫療診斷），以及有效的風險控制（例如採限制輸出、提供來源標註等措施，以降低對原著作市場的替代效應）。

2.若基礎模型成立合理使用，RAG未必隨之過關

反之，即便法院認為基礎模型創造前所未有的工具，具有高度轉化性而構成合理使用，一個設計粗糙的RAG應用仍可能構成侵權。例如，若RAG服務的主要功能僅是抓取最新新聞報導並生成近乎原文的摘要，直接與新聞網站競爭，則既便基礎模型是合法的，該RAG應用本身也可能因為缺乏轉化性且對市場造成替代性衝擊，而無法成立合理使用。

**（二）混合評價模型才能準確掌握RAG的核心特徵**

RAG的法律分析在本質上與基礎模型有顯著不同，因此有其獨特的論述空間，例如「事實與表達二分法」的應用。此原則在RAG的特定應用場景中，成為一個有力的抗辯。

以「事實查核」或研究性RAG應用為例，其法律分析與基礎模型有所區別。當使用者向基礎模型詢問一個事實性問題，其生成的答案是基於從龐大訓練資料中學習的統計規律，此過程可能無可避免地複製受著作權保護的「表達方式」，由於其內部運作的不透明性，基礎模型開發者很難主張他只是在處理不受保護的「事實」。然而，RAG的運作機制則使其能更清晰地在「事實」與「表達」之間劃出界線：

1.目的精準性：一個為事實查核而設計的RAG，其明確的系統目標是驗證事實，而非重現表達。例如用於生醫研究或新藥開發的RAG系統，其知識庫可能包含數萬篇受著作保護的期刊論文。

2.過程的可追溯性：RAG輸出內容的依據是具體的、被檢索到的文本塊，使得開發者可以從技術上證明，氣筒只是將這些文本塊作為驗證事實的證據，並透過設計（如僅輸出最終事實、提供多個來源連結、限制引用長度）以確保未侵害原著作的表達。

3.轉化性用途的體現：在此類應用中，RAG並非原著作的替代品，而是一個研究工具或驗證工具，將原著作從「供讀者閱讀欣賞」的性質，轉化為「供機器分析驗證的數據源」，這種用途的轉變，正是合理使用中「轉化性」的核心精神。

## 肆、混合評價模式的比較法實踐分析

混合評價模式為RAG應用這項新興技術上提供了一個結構化且可預測的分析框架，以下針對美國、歐盟與我國的法律框架，分別運用「混合評價模式」進行分析。

### 一、美國法下RAG應用的混合評價分析

**（一）依循混合評價模式，在美國法制下對RAG應用進行分析**

1.第一步（分階段判斷表面侵權）：

首先，在資料擷取階段，若涉及對受保護作品（如新聞報導、書籍）的複製以建立索引資料庫，無論是從公開網路爬取或是從其他來源獲取，均可能構成對著作權人重製權的侵害。Perplexity案與Cohere案的原告即持此主張。在生成階段，若輸出內容與原著作構成實質近

似，則可能進一步構成侵權。

**2.第二步（整體評價合理使用四要素）：**

當表面侵權可能成立時，進入美國著作權法第107條的合理使用四要素判斷。此時應採整體評價：

(1)利用之目的與性質：轉化性（Transformative Use）是核心關鍵。一個RAG應用的轉化性高低，取決於其整體功能。以Deep Research為例，其目的並非複製單篇論文，而是綜合數十篇科學文獻，進行多步驟推理，以識別研究模式或提出新見解。這種用途創造全新的知識價值，遠超原文獻的簡單呈現，轉化性程度高。一個RAG應用若主要功能是提供與原新聞報導高度近似的即時摘要，且可能直接取代使用者對原始新聞來源的需求（如Perplexity案的爭議），其轉化性就較低。

(2)著作之性質：RAG處理的內容類型會影響判斷。處理事實性、資訊性的內容（如新聞報導、科學數據、財務報表），相較於處理高度創作性的作品（如小說、詩歌），在合理使用判斷上整體可能較為有利。

(3)所利用之質量及其在整個著作所占之比例：判斷重點不應只看輸入端複製多少，而應更側重於最終輸出內容與任何單一原著作的關係。

(4)利用結果對著作潛在市場或價值之影響：此項被視為「最重要的一環」。評估應是整體的，而非片段的。若RAG應用直接與原內容市場競爭，不利於合理使用主張。例如，若一個RAG新聞摘要服務導致原新聞網站流量劇減、訂閱收入下降，其市場損害是顯而易見的。反之，若RAG應用能與內容產業合作，或為原作帶來新的價值，則有利於合理使用認定。

承前分析，在美國法下應用混合評價模式具有可行性，能避免一開始就被前端複製行為綁架，而是能將重點放在RAG作為一個整體服務是否具備「轉化性」這一合理使用的核心精神上，從其整體應用場景（Use Case）出發，全面評估其是否構成轉化性使用、是否採取充分的保護措施，以及是否會不成比例地損害著作權市場，而非僅因為其在技術過程中進行複製，就斷然認定其構成侵權，從而在保護著作權與鼓勵技術創新之間取得平衡。

### （二）美國著作權局意見與混合評價模式

美國著作權局（U.S. Copyright Office）在2025年5月9日公布的「著作權與AI第三部分：生成式AI訓練」意見[28]，對RAG的轉化性持相對保守立場，指出RAG應用主要目的係將資料庫內相關著作以摘述方式呈現，與原著作提供資訊之目的相似，故轉化性程度較低。但報告同時承認，若AI業者實施適當的輸出限制措施，避免生成與原著作實質近似內容，應用的轉化性程度將顯著提高。此觀點支持整體評價的重要性，即不能僅看RAG

註28：See *supra* note 6.

技術本身，須結合具體實施方式綜合判斷。

美國著作權局認為，RAG涉及重製他人著作，可能構成表面侵權（prima facie infringement）[29]。無論AI開發者將資料複製到其檢索資料庫，或系統從外部來源取得資料，系統在生成回應時均會複製檢索內容以增強輸出，此等複製即便短暫，若對話系統保留歷史記錄則可能儲存檢索結果。著作權局特別關注RAG對新聞媒體的影響，因生成的摘要可能替代原作或驅離流量。著作權局以Google Books案為例，強調Google採用關鍵措施（significant safeguards）降低取代原著作的可能性。此觀點實質上已超越對RAG技術本身的片面評價，而是著眼於該應用的整體設計與市場影響。

### （三）Google Books案等對混合評價模式的啟示

美國已有數十件針對生成式AI的著作權訴訟[30]，包括2023年12月，紐約時報對OpenAI及微軟公司提出的著作權侵害訴訟[31]等案。這些案件的被告多數引用Google Books案以主張合理使用。

#### 1.Google Books案

*Authors Guild v. Google Inc*，案[32]為RAG應用的合理使用提供了重要先例。第二巡迴上訴法院將Google Books應用作為整體進行分析，認定其建立可搜索圖書資料庫的整體目標具高度轉化性，創造了全新圖書使用方式。法院高度評價Google採取的綜合保護措施，如嚴格限制片段（Snippet）[33]顯示限制，頁面屏蔽及對特定類型圖書的特殊處理，此系列保護體系確保Google Books不成為購書替代品。

此案啟示RAG應用若能從整體系統設計上採取有效的輸出限制措施（如限制長度、避免生成核心部分），將有效地增強其合理使用主張。

#### 2.Warhol案

*Andy Warhol Foundation for Visual Arts, Inc. v. Goldsmith*案[34]代表美國最高法院轉化性使用最新立場，強調判斷轉化性須考慮使用具體目的和前後文。即使Warhol對照片進行藝術化處理，但用

---

註29：*Id.*

註30：ChatGPT is Eating the World. (2024, August 27). *Master list: Copyright lawsuits v. AI companies in U.S.* Retrieved May 30, 2025, from https://chatgptiseatingtheworld.com/2024/08/27/master-list-of-lawsuits-v-ai-chatgpt-openai-microsoft-meta-midjourney-other-ai-cos/（最後瀏覽日：2025年6月9日）（截至2025年3月13日，累積共有39件案例）。

註31：New York Times Co. v. Microsoft Corp., No. 1:23-cv-11195 (S.D.N.Y. Aug. 12, 2024).

註32：Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).

註33：該案中對摘要的限制措施包括：最多顯示三個摘要，每個約八分之一頁，無論使用者搜尋多少次都只顯示相同的三個摘要；Google也永久阻止顯示所有頁面的一部分以及每十頁中的一整頁；對於食譜、字典等某些類別，摘要功能被完全禁用，因為摘要本身可能就足以滿足使用者需求。

註34：Supreme Court of the United States. (2023). *Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith et al.*, 598 U.S. ___ (No. 21-869). https://www.supremecourt.gov/opinions/22pdf/21-869_87ad.pdf

於雜誌封面時，與原照片的商業用途相同，故缺乏轉化性。此判決提醒RAG開發者，技術創新本身不足以確保轉化性，須確保整體用途確實不同於原著作。

Warhol案亦突顯市場替代效應及商業授權市場存在的重要性。若RAG應用導致使用者不再需要原內容或規避既有授權機制，將嚴重削弱合理使用主張，啟示產業應積極探索與內容產業的合作模式。

## 二、歐盟法制下RAG應用的混合評價分析

### （一）依循混合評價模式，在歐盟法制下對RAG應用進行分析

#### 1.第一步（分階段判斷表面侵權）：

RAG在資料擷取和索引過程、檢索及生成階段對受保護作品進行複製，原則上仍落入會員國著作權法所規範的重製權範圍，因此需要進一步探討是否有TDM例外規定的適用。

#### 2.第二步（整體評價是否符合TDM目的）：

歐盟法制關於生成式AI[35]的規範核心是2019年通過「數位單一市場著作權指令」（Directive on Copyright and related rights in the Digital Single Market，下統稱CDSM指令）中的「文字與資料探勘」（Text and Data Mining，下統稱TDM）例外規定[36]。

(1)科研目的TDM例外：CDSM指令第3條允許研究及文化遺產機構為科學研究目的進行TDM，前提是具「合法管道」（Lawful Access）接觸著作，權利人不得以契約排除。

(2)一般目的TDM例外：CDSM指令第4條允許任何人為任何目的（含商業目的）進行TDM，前提亦為「合法管道」接觸著作，但權利人可透過「適當方式」（如機器可讀格式）明示「選擇退出」（Opt-out）以排除例外適用，若未明示保留則可進行TDM。

CDSM指令第2條第2款將TDM定義為「任何自動化分析技術，旨在分析數位形式之文字與資料，以產生包括但不限於模式、趨勢和關聯性之資訊」。此定義本身即帶有目的導向性，強調TDM活動是為了「產生資訊」而非僅是複製。若一個RAG主要功能是分析而非單純呈現，就較可能適用；反之則可能被排除。此外，此模式也會要求從整體上審視RAG服務是否尊重權利人的「選擇退出」（Opt-out）機制。

然而，RAG的輸出（如特定問題的答案或文章摘要）是否完全符合CDSM指令對TDM所產出「包括但不

註35：同前註26，第418頁（「雖然並未專門於條文主文部分強調機器學習一詞，但資料探勘之高效實現離不開機器學習，二者關係密切。」）

註36：高嘉鴻（2023），〈資料探勘著作權限制及例外規定國際立法趨勢研究〉，《智慧財產權月刊》，298期，第36-56頁。

限於模式、趨勢和關聯性之資訊」的定義，並非沒有疑義。若對此定義採嚴格的文義解釋，單純的摘要或問答可能被排除在外。此種解釋忽略了TDM例外的立法精神，即鼓勵利用自動化技術從既有資料中創造新價值。RAG的核心正是一種「自動化分析技術」，透過對檢索到的資料進行篩選、整合與提煉，最終生成一個比原始資料更有用的答案。此過程本身就是一種「產生資訊」的行為。因此，對TDM的定義應採更為寬鬆的「功能性解釋」，只要RAG應用的整體目的在於「分析」而非單純「呈現」，其產出就應被視為TDM定義下廣義的「資訊」。

前述說明突顯本研究「混合評價模式」的分析優勢。若孤立看待R-A-G中的「G」（生成）環節，其輸出內容確實不像「趨勢」或「模式」。但若從整體評價RAG作為一個「先查證、再生成」的完整分析系統，則其整體運作為「產生包括但不限於模式、趨勢和關聯性之資訊」而進行的分析過程[37]，有機會落入TDM例外的保護傘下，從而化解了僅從輸出結果進行判斷的困境。

### （二）德國法院LAION案判決對混合評價模式的啟示

雖然歐盟在生成式AI適用TDM規定的相關案件已繫屬於歐洲法院（ECJ）[38]，但目前尚無判決。不過，德國漢堡地方法院的「LAION案」判決，為觀察歐洲各國法院如何在生成式AI領域適用TDM例外規定，提供了重要的線索。

LAION案是歐洲首件針對AI訓練資料集的著作權侵權問題作出實體判決的案例。案情為一名攝影師控告非營利組織LAION（Large-scale AI Open Network），主張其在用於訓練AI模型的大規模圖像資料集LAION-5B[39]中，收錄了他受版權保護的照片。

漢堡地方法院於2024年9月27日駁回原告訴訟[40]，其重點有二：

1.**符合科研目的TDM例外**：法院認定LAION為一研究機構，其建立資料集是為了促進科學研究，符合非商業目的，因此其行為適用德國著作權法第60d條「為科學研究目的的文字和資料探勘」

註37：章忠信（2024），〈人工智慧訓練與著作之合法利用〉，《智慧財產權月刊》，304期，第5-26頁。

註38：陳家駿（2025），《歐洲首宗生成式AI著作侵權官司──德國音樂仲團GEMA起訴OpenAI和Suno》，載於 https://iknow.stpi.niar.org.tw/post/Read.aspx?PostID=21624，陳家駿（2025），《從法國首宗生成式AI之Meta被告著作侵權訴訟案──兼談歐盟人工智慧法》，載於 https://iknow.stpi.niar.org.tw/post/Read.aspx?PostID=21781

註39：LAION-5B是一個包含數十億張圖片和其文字描述的公開資料集。

註40：Hamburg Regional Court. (2024, September 27). *Robert Kneschke v. LAION e.V.*, Case No. 310 O 227/23. https://www.wipo.int/wipolex/en/judgments/details/2381

豁免（此條為依據CDSM指令第3條增訂）。

2.**關於一般目的TDM例外**：法院補充說明，雖然LAION的行為也符合德國著作權法第44b條「一般資料探勘」之目的（對應CDSM指令第4條），但因該攝影師（權利人）已依法明示退出（Opt-out），故此項例外無法適用。

值得注意的是，法院在判決時的思考路徑，並非孤立地看待「建立資料集」這一行為，而是從行為的整體目的出發，將LAION作為一個組織的整體宗旨（促進科學研究）與資料集的最終用途納入綜合考量。法院的此種判決思路，即在認定表面侵權行為後，從整體目的與功能來審視抗辯事由（TDM例外）。此種做法與本研究提倡的「混合評價模式」中，第二階段對抗辯事由進行整體評價的精神完全契合。

## 三、我國法制下RAG應用的混合評價分析

### （一）依循混合評價模式，在我國法制下對RAG應用進行分析

1.**階段一（表面侵權判斷）**：RAG應用若未經授權對他人享有著作權的數位內容（如網路文章）進行複製以建立知識庫，此行為可能落入我國著作權法第22條重製權的範圍[41]。其在檢索階段的暫時性複製，則需檢視是否符合第22條第3項「過渡性或附帶性」、「不具獨立經濟意義」等要件。生成階段若與原作實質近似，亦可能觸犯重製權或第28條的改作權。

2.**階段二（我國著作權法第65條第2項合理使用四要素之整體適用）**：在認定表面侵權可能成立後，便進入合理使用的整體評價。

(1)利用之目的及性質：若RAG應用能證明其整體目的並非單純再現原著作，而是透過對大量資訊的分析、整合與提煉，產生具有附加價值的新資訊或新功能（例如，輔助學術研究、進行複雜問題解答、提供個人化知識管理等），則較有機會被認為具有「轉化性」。

(2)著作之性質：若RAG處理的主要是資訊性、事實性的內容（如新聞報導、科學數據），相較於處理高度創作性、虛構性的作品（如小說、詩歌），在合理使用判斷上整體可能較為有利。但這並非絕對，關鍵仍在於具體的利用方式是否合理。

(3)所利用之質量及其在整個著作所占之比例：傳統上關注的是利用部分在原著作中的占比。但對於RAG這類以處理、整合大量資訊為特性的技術，判斷重點或應更側重於最終輸出內容與任何單一原著作的關係，以及輸出內容是否包含了原著

註41：智慧財產局著作權組（2022），電子郵件1111212號函釋（111年12月12日）（「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』」）。取自 https://www.tipo.gov.tw/copyright-tw/cp-407-916892-c036b-301.html

作最核心、最具創作性的部分。

(4)利用結果對著作潛在市場與現在價值之影響：此為合理使用判斷中極為重要的考量因素。應從RAG應用對整體內容生態系統的影響進行評估，不僅包括對個別著作權人直接的經濟影響，也應涵蓋對整個產業結構的潛在改變。若RAG應用導致原創內容的生產誘因降低，長期而言將損害社會的文化創造力；但同時也應考量其是否可能帶來正面的市場效應，例如增加內容的可發現性、擴大潛在讀者群等。

著作權法第65條第2項規定除臚列4項判斷基準外，並規定應審酌「一切情狀」，即包含利用結果對於人類智識文化資產之整體影響，以及其他情狀，綜合各判斷基準及主觀因素與客觀因素之衡量[42]。整體而言，我國著作權合理使用規定強調需就一切情狀進行綜合考量，而非僅就資料複製的單一行為進行判斷，這為RAG應用在我國法下尋求合法性依據時，應從整體角度論究提供明確方向。

除第65條第2項的概括性合理使用條款外，我國著作權法亦設有多項法定例外規定（第44條至第63條），如第49條「為時事報導者」或第52條「為報導、評論、教學、研究或其他正當目的之必要」的引用，這些條款的適用多採目的導向設計，其解釋適用亦應考慮RAG應用的整體目的與行為樣態是否符合各該條款的立法本旨與要件。

### （二）賴和編輯著作案判決對混合評價模式的啟示

我國目前尚無生成式AI侵害著作權的訴訟，故從轉化性使用司法案例中選取與生成式AI性質較接近的賴和編輯著作案[43]，以探求我國法院對於生成式AI案件的可能審理趨勢。

本案事實是賴和基金會等人起訴主張聯合百科公司未經授權將賴和手稿集、賴和影像集等系列叢書收錄於聯合百科電子資料庫，侵害其所享有賴和手稿集、賴和影像集等系列叢書之編輯著作。本案主要爭點包括系爭電子資料庫對於系爭叢書之編輯著作的使用，是否具有轉化性使用及轉化之程度？是否成立合理使用[44]？

本案歷經數個審級，前後共有五個民事判決[45]及五個刑事判決[46]，其中有兩個判決詳細

註42：蔡惠如（2016），〈著作權合理使用概括規定之回顧與前瞻〉，《智慧財產權月刊》，209期，第15-16頁。

註43：蔡嘉裕（2021），〈著作權「轉化性使用」之我國本土案例分析〉，《智慧財產權月刊》，271期，第47-77頁。

註44：同前註。

註45：智慧財產法院101年民著訴字第37號民事判決、智慧財產法院102年民著上字第18號民事判決、最高法院104年台上字第1139號民事判決、智慧財產法院104年民著上（一）字第2號民事判決、最高法院108年台上字第1135號民事判決。

註46：臺灣臺北地方法院102年度智訴字第24號刑事判決、智慧財產法院104年刑智上訴字第47號刑事判

論斷是否構成合理使用，有無轉化性，其中一則認定具有轉化性[47]、另一則認定不具有轉化性[48]。值得注意的是，此兩則判決論斷合理使用的思考路徑，並非孤立地看待掃描轉存數位化複本行為，而是從行為整體目的出發，將前階段行為（將手稿影像紙本掃描轉存為數位化複本），與後階段行為（將數位化複本重新選擇編排，新增電子全文檢索之功能，供使用者以電腦網路等電子設備，高效率搜尋、比對賴和手稿影像之內容）合併評價，論究是否成立合理使用。此種做法與本研究提倡的「混合評價模式」中，第二階段對抗辯事由進行整體評價的精神完全契合。

## 伍、結語

### 一、基於混合評價思維的整體合規策略

對產業而言，應將著作權合規置於核心地位，以下基於「混合評價模式」思維提供合規策略建議：

**（一）資料來源的合法性優先（對應階段一）**

1.**優先採用授權資料**：盡可能使用已獲合法授權的資料庫、專有內部資料或開放授權內容。

2.**尊重選擇退出機制**：在擷取公開網路資料時，必須設計能夠識別並尊重robots.txt[49]、TDM保留聲明等權利人選擇退出信號的機制。

3.**詳細記錄來源與過程**：對所有資料來源、擷取時間與處理方式進行詳細記錄，以備合規審查。

**（二）提升應用的轉化性價值（對應階段二：目的與性質）**

1.**專注於「分析」而非「呈現」**：系統設計應致力於提供經分析、整合或賦予新功能的資訊（如趨勢分析、複雜問答、洞見提取），而非實質替代原著作的內容。

2.**從服務提供者轉向工具提供者**：思考將商業模式從直接提供內容，轉型為提供分析工具或平台服務，讓使用者在自己的資料上運行RAG。

**（三）設計降低市場衝擊的技術與管理措施（對應階段二：市場影響）**

1.**實施輸出限制**：積極採用如限制輸出長度、避免生成與單一原著作實質近似的內容、設置引用頻率上限等技術措施。

2.**提供清晰來源標註**：為所有引用的資訊提供清晰的來源標註和連結。這不僅能增強可信度，也能在合理使用分析中證明並未試圖將他人著作冒充為己有，並

決、最高法院106年台上字第2093號刑事判決、智慧財產法院107刑智上更（一）字第1號刑事判決、最高法院108年台上字第224號刑事判決。

註47：智慧財產法院104年刑智上訴字第47號刑事判決（105年11月24日刑事第二審判決）。

註48：智慧財產法院107刑智上更（一）字第1號刑事判決（107年10月19日刑事第二審更一審判決）。

註49：robots.txt是一個放在網站根目錄下的文字文件，用來告知網路搜尋引擎的爬蟲，哪些內容可以被爬取，哪些內容應該被忽略主要作用是控制網站的爬蟲行為，例如哪些網頁可以被索引，哪些網頁不應該被索引。

可能為原作者導流。

3.**建立有效的過濾與下架機制**：建立快速回應的內容過濾與權利人下架（Takedown）請求的處理機制。

## 二、RAG的未來軌跡、法律挑戰與應對之道

RAG技術仍在快速演進，其未來趨勢將帶來新的法律挑戰。首先，隨著「代理式RAG」（Agentic RAG）[50]的發展，AI代理將具備更強的自主推理和任務執行能力，其行為的法律定性（是工具還是代理人？）以及責任歸屬勢將成為新的焦點。與此同時，「多模態RAG」（Multimodal RAG）[51]將處理範圍從文本擴展到圖像、音訊與視訊，這使其與美術著作、錄音著作等發生更為複雜的著作權交集。此外，「實時RAG」（Real-Time RAG）[52]從社群媒體、新聞推送等實時數據流動態檢索資訊的能力，將使侵權行為的認定變得更加困難與即時。最後，「設備端RAG」（On-Device RAG）[53]的出現，雖然能透過在使用者本地設備運行來保護隱私，卻也可能將侵權的重製行為轉移到使用者端，從而引發新的共同侵權或幫助侵權責任問題。

從當前發展趨勢來看，對RAG的法律評價需要保持動態和前瞻性，「混合評價模式」提供一個靈活的分析框架，使其能夠適應未來更複雜的技術形態。不同類型的RAG應用在法律風險與合理使用空間上存在差異，因此，產業介若能依循混合評價的合規思維，透過審慎的系統設計與商業模式規劃，將有機會在技術創新與法律規範間取得動態平衡。展望未來，RAG技術的持續演進將不斷帶來新的法律議題，唯有透過立法者、司法者、產業與學界的持續對話與共同努力，才能在鼓勵創新的同時，有效保護著作權人的正當權益，共同塑造一個AI賦能且法制健全的知識社會。

（投稿日期：2025年6月16日）

註50：*See supra* note 14.

註51：Gautam75. (2024, May 22). Multi-Modal RAG: A practical guide. *Medium*. https://gautam75.medium.com/multi-modal-rag-a-practical-guide-99b0178c4fbb

註52：Chen, J., Shen, E., Bavalatti, T., Lin, X., Wang, Y., Hu, S., Subramanyam, H., Vepuri, K. S., Jiang, M., Qi, J., Chen, L., Jiang, N., & Jain, A. (2024). Class-RAG: Content moderation with retrieval augmented generation. *arXiv preprint arXiv:2410.14881*. https://doi.org/10.48550/arXiv.2410.14881arXiv. https://doi.org/10.48550/arXiv.2410.14881

註53：Wang, Z. J., & Chau, D. H. (2024). MeMemo: On-device retrieval augmentation for private and personalized text generation (arXiv:2407.01972). *arXiv*. https://doi.org/10.48550/arXiv.2407.01972