

# AI 走向國界後，需要重新思考什麼？

文／洪為靈

在過去十年，人工智慧（AI）從新興技術轉變為具備高度經濟、政治與戰略意義的關鍵基礎能力。生成式 AI 與大型語言模型（LLM）的成熟，除了改變企業的營運模式與創新節奏，也逐漸深刻影響國家政策、社會治理、資訊安全與資料主權等核心議題。AI 不僅只是提升效率的工具，更將成為左右國家競爭力與產業版圖的重要資產。

從美國、歐盟到亞洲與中東，各國政府正透過政策與資金加速 AI 能力建置，避免在科技競爭中落後。Reuters（2026）報導指出，新加坡在宣布投入超過 7.7 億新加坡元（約 5.7 億美元）發展公有 AI 研究與基礎設施，而沙烏地阿拉伯國家基礎設施基金和該國人工智慧公司 Humain，宣布以高達 12 億美元的融資協議，擴展 AI 人工智慧基礎設施，推動經濟結構轉型。

這些動向反映了明確的趨勢：AI 是逐步受到法規、政策與國家戰略所形塑的「數位主權力量」。

在此背景下，企業所面臨的挑戰不只是「如何導入 AI」，而是必須思考如何維持競爭力、彈性與風險可控性。過去依賴雲端平台與開源模型的 AI 採用模式，正面臨資料跨境、算力依賴與治理透明度不足等結構性風險，使得「主權 AI（Sovereign AI）」與「開放 AI（Open / Open-source AI）」成為企業無法忽視的兩大發展方向。

這兩種看似對立、實則彼此補充的發展方向已成為企業必須理解與策略性整合的關鍵議題。因此，本篇文章將探討：

- 主權 AI 是什麼？
- 為何企業對主權 AI 感到遙遠？

## •主權 AI 與開放 AI 的發展方向

### 主權 AI 是什麼？

主權 AI 並非單指一套 AI 模型，而是具備控制權、治理能力與資安防護能力的完整 AI 生態系。其核心在於，國家或經濟體能在 AI 供給鏈的關鍵環節中保持自主性，不被單一的外部平台、法律體系或技術供應商所全面制約。

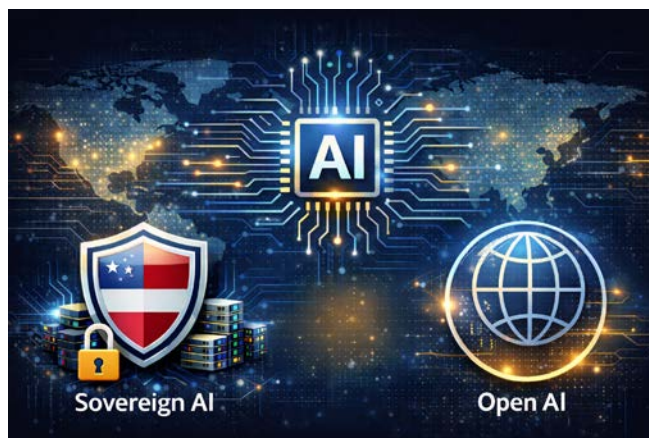
其中，資料主權是主權 AI 的基礎。資料不再只是模型訓練的燃料，而是需要納入治理與策略思維的核心資產。透過資料在地留置、依本地法律管理，能降低國安、商業機密與個資外洩的風險。近期，台灣數位發展部推動「主權 AI 訓練語料庫」，集合超過 200 個政府機關資料集、逾 6 億 Tokens，目的是希望讓 AI 模型能理解台灣在地語言與文化脈絡，避免價值觀與決策邏輯由外部平台主導。

另一個關鍵則是算力自主。大型模型的訓練與推理高度依賴 GPU 與異構運算資源，算力逐漸成為數位主權的重要基石。台灣未來將 AI 算力納入「AI 新十大建設」，提出打造世界級算力中心的願景，其中反映出政府高度重視對於降低單一雲端的依賴。

此外，主權 AI 也包括 AI 治理與跨國協作機制。在國際層面，放言(2024)報導指出輝達(Nvidia)執行長黃仁勳在不同的國際場合積極推廣主權 AI 的重要性，認為各國必須運用自己的基礎建設、資料與模型能力來避免過度依賴科技平台。

因此，主權並不等於封閉，各國需在資料治理、倫理與永續發展上協調合作。主權 AI 的本質，在於建立開放與自主之間的平衡。

簡而言之，主權 AI 是一種技術戰略，將 AI 放在國家安全、資安保護、社會治理與產業競爭力的核心位置。主權 AI 不僅影響國家層面的數位主權，更進



一步影響企業在全球 AI 生態系統中的定位及風險治理策略。

### 為何企業對主權 AI 感到遙遠？

雖然主權 AI 在政策層面備受重視，但對多數企業而言顯得抽象而難以落地。原因在於，其核心價值與企業營運的決策邏輯存在落差。

首先，技術與資源門檻過高。關於模型訓練、算力建置及資料治理需龐大投資與專業人才，對多數企業而言難以回收成本，因此傾向採用付費雲端服務與成熟的開源模型，而非自行搭建完整的主權 AI 平台。

其次，企業已高度依賴現有開放的 AI 生態。許多大型平台如 Meta LLaMA、OpenAI 等提供成熟、易整合的工具，使企業能快速部署 AI 應用，而無需掌握底層架構。

第三，法規與治理仍在持續演進中。各國對資料跨境、隱私與 AI 監管的立場不一，企業難以預測未來合規要求，因此採取觀望態度，避免投入不確定性的 AI 基礎建設。

最後，企業的 AI 投資仍以短期效益為導向，但主權 AI 屬於長期基礎建設，較難立即反映在營收上。這使主權 AI 常被視為「重要但不急迫」。然而，當資料流動受限、合規成本上升或供應鏈不穩時，缺

乏前瞻布局的企業，將更容易失去競爭彈性。

雖主權 AI 不易落地，TechRadar (2025) 報導德國已推出名為「OpenAI for Germany」的主權 AI 平台，專注於在政府與公共機構中部署符合歐盟資料主權要求的 AI 解決方案，這意味歐洲政府正積極尋求與大型科技企業合作，在不違反法規的前提下建立主權 AI 能力。

此外，Reuters (2026) Microsoft 與 OpenAI 聯合推出的「OpenAI for Countries」計畫，目的在降低全球不同地區使用 AI 的落差，擴大 AI 在教育、醫療與公共服務領域的普及性。跨國企業策略既是技術擴散動能，也展現出企業如何在全球主權與開放 AI 機制之間找到平衡。

## 主權 AI 與開放 AI 的發展方向

在全球 AI 競賽中，主權 AI 與開放 AI 並非對立，而是代表兩種互補的發展路徑。主權 AI 由國家或區域推動，強調安全、可控與治理能力，適用於核心資料、公共服務與關鍵產業的場景。其目標是確保 AI 能力不因外部政治、商業或技術等因素而中斷。

在主權 AI 的路徑之下，企業能理解這不僅是政府的責任，也需要企業本身在資料治理、模型透明度、合規操作等相關面向投入力量。主權 AI 強調本地資料留置與治理，使模型訓練貼近本土語言、法律管理與社會背景。例如台灣主權 AI 訓練語料庫的建置，除了提供政府資料的訓練集，同時也讓企業共享本地化的資料資源，進而提升 AI 於在地場景下的識別與品質。

開放 AI 則源自開源社群精神，能讓任何開發者與企業使用、修改與改進 AI 模型，促進技術迭代速度與多樣性，使企業可用低成本試驗與部署 AI 的應用。開放 AI 的優勢在於快速創新與低門檻採用，企

業能夠透過開源模型建立 AI 的解決方案，並快速整合到現有系統中，加速數位轉型。

此外，跨國社群的技術合作能推動模型迅速演進，使性能與應用場景逐漸擴大。然而，開放 AI 也伴隨治理與資安風險。當模型深入核心業務系統，若缺乏資料治理與風險控管，將衍生合規與安全問題。

因此，許多國家在鼓勵開放創新的同時，也加強監管框架。對多數企業而言，關鍵不在於二選一，而是建立不同層面共存，並分工合作的整合性生態。在高創新、低敏感場景中善用開放 AI，並在涉及關鍵資料與決策的領域導入主權 AI 架構。

## 結語

當 AI 開始走向國界，其影響已遠超越技術層次，成為產業結構與治理模式重塑的關鍵力量。主權 AI 的興起提醒企業，在追求效率與創新的同時，也必須同步思考資料主權、資安韌性與治理責任。

未來忽視 AI 國界化趨勢的企業，可能在法規、算力與資料流動限制下承受更高風險。反之，提早整合主權 AI 與開放 AI 的企業，將更有能力在不確定環境中保持競爭優勢。

AI 的未來，不只屬於技術領先者，更屬於能在效率、治理與風險之間做出平衡抉擇的企業。當國界再次成為 AI 發展的重要背景條件時，企業需重新思考的，已不僅只是是否使用 AI，而是在誰的規則下、以何種方式、承擔多少風險來使用 AI，這將是下一個十年競爭力的分水嶺。



作者洪為璽博士，現為國立政治大學資訊管理學系教授兼CINTES研究中心主任，專長為資訊策略管理、資訊安全管理與大型資訊系統導入與應用。