財團法人理律文教基金會

專題報告

淺談我國發展主權 AI 之可能性：以歐盟為比較中心*

李建融**

* 本文係為申請財團法人理律文教基金會所撰寫之專題報告。

** 世新大學法律學系碩士班二年級。

目錄

壹、 緒論 4
一、問題之提出：自 DEEPSEEK 事件說起 4
二、語料結構之不對稱 5
三、研究目的及問題意識 5
貳、 主權 AI 之概念釐清 6
一、自數位主權至主權 AI 之概念演進 6
二、概念之商業起源與語彙區辨 8
三、定義困境及其法律後果 9
四、主權 AI 之四大面向 10
五、小國之策略選擇：可控的相互依賴 13
六、本文之界定：三項判斷標準 15
七、小結 17
參、 我國主權 AI 及相關治理法制之現況與挑戰 18
一、政策架構與法制架構之落差 18
二、可信任 AI 對話引擎（TAIDE）計畫 18
三、臺灣主權 AI 訓練語料授權條款 20
四、四大結構性挑戰 21
五、小結 25
肆、 比較法觀點：以歐盟為中心 25
一、歐盟之雙軌回應 26
二、技術主權之政策藍圖：EUROSTACK 倡議 26
三、人工智慧大陸行動計畫 28
四、資料聯盟策略 29
五、數位綜合法案對一般資料保護規則（GDPR）之修正 30
六、歐盟主權 AI 之其他論述 31
七、歐盟路徑之歸納 32
伍、 我國主權 AI 法制建構之初步構想 32
一、三項移植原則 32
二、資料供給面：促進資料創新利用發展條例之立法定位 33
三、資料利用面：著作權法之相關問題 34
四、基礎設施：AI 新十大建設推動方案之法制化 36
五、管轄與問責：人工智慧基本法之修正 37
六、小結 38
陸、 結論 39
參考文獻

摘要

我國語料於全球訓練資料庫中居弱勢，此一情況將導致公共領域所仰賴之語言模型，其價值取向與管轄恐繫於他國法域。模型偏差既源於語料輸入之內容而非傳播行為，規範重心即應自輸出端之事後管制前移至訓練資料之供給。本文將主權 AI 界定為國家對技術堆疊各層依賴關係之安排，並以透明性、可替代性與有效法律支配三項判準，說明我國可行者為可控的相互依賴而非全技術堆疊主權。

檢視現況，可見政策與法制密度之落差：算力匱乏、開放資料授權不明、著作權風險之寒蟬效應與基本法之規範闕如，四者彼此增強。比較法上以歐盟作為參照，文末提出相關修法方向：著作權法之資訊分析例外、人工智慧基本法就資料供給與依賴治理之增訂，及政府資料流通與算力設施之法制化。

關鍵字

主權 AI、數位主權、人工智慧基本法、歐盟、可控的相互依賴

壹、緒論

一、問題之提出：自 DeepSeek 事件說起

2025 年初，中國大陸發布之 DeepSeek 模型以顯著較低之訓練成本與取得前沿模型之表現，在全球科技與政策社群引發連鎖反應。就技術層面而言，其意義在於模型效能與資本投入之間的線性關係遭到動搖；就治理層面而言，其所揭示者更為根本，即一國之論述、知識生產與行政決策所仰賴之語言模型，其訓練資料、價值取向，均可能落於他國法域之支配範圍。國內學者即指出，全球科技治理之關注已自個人資料保護、跨境資料流動等傳統「資料主權」議題，逐步擴展至涵蓋資料、模型、基礎設施與價值觀治理之「主權 AI」新領域[1]。

主權 AI 之所以在短時間內成為各國政策語彙，其動力來源有二。其一為對技術依賴所生之管轄落差。當公共服務、國防情報與關鍵基礎設施之運作日益仰賴少數境外供應商所提供之模型與雲端服務時，形式上之法律管轄權與實質上之技術控制之間，即出現落差。其二為對文化主體性之維繫。語言模型並非中立之工具，其輸出之內容反映訓練資料庫所承載之價值判斷；當一國之語言在全球語料中僅佔極小比重，且該語言之主要語料來源受他國支配時，模型之輸出即可能系統性地偏離該國之社會共識。大型語言模型若由他國企業或不同文化背景國家主導，易生「價值觀偏誤」（value bias），與本土文化或社會價值相衝突，甚至面臨政治操弄或內容不當審查之風險[2]。除此之外，NVIDIA（輝達）共同創辦人暨執行長黃仁勳亦表示，各國必須擁有獨立的 AI 基礎建設，他認為建立 AI 基礎建設對國家而言已是「絕對必要」，是贏得全球競賽的關鍵[3]。

回到臺灣，2023 年國慶前夕，中央研究院所釋出之繁體中文模型於測試中回答「我國領導人為習近平」、「國慶日為 10 月 1 日」[4]，此一事件並非模型設計者之疏失，而是基礎模型過度依賴簡體中文訓練資料之必然結果，使得中研院隨

---

[1] 陳譽文，從 DeepSeek 事件觀察主權 AI 治理趨勢與我國法制回應，當代法律，41 期，頁 68-78，2025。

[2] 林佳瑩，從國際 AI 發展趨勢探析我國主權 AI 推展策略，經濟研究（國家發展委員會經濟發展處），26 期，頁 10，2026 年。

[3] Brian Caulfield, *NVIDIA CEO: Every Country Needs AI*, NVIDIA BLOG (Feb. 12, 2024), https://blogs.nvidia.com/blog/world-governments-summit/. 另可參：楊蕙如，主權 AI 發展相關問題研析——以數據資料與大型語言模型之建立為例，立法院法制局議題研析，編號 R02904，2025 年 10 月，https://www.ly.gov.tw/Pages/List.aspx?nodeid=46869（最後瀏覽日：2026/09/05）。

[4] 林志成，國慶日是 10 月 1 日？中研院語言模型出錯急下架，工商時報，2023 年 10 月 9 日，https://www.ctee.com.tw/news/20231009700630-431401（最後瀏覽日：2026/09/05）。

即做出相關澄清[5]。該事件在我國公共討論中之意義，在於它以極為具體之方式，將抽象之「文化主體性」問題轉化為可觀察之現象。

此二事件分居問題之兩端：DeepSeek 事件所呈現者為管轄之外部化，中研院事件所呈現者為我國價值流失之風險。二者雖表現形態不同，其共同之結構成因則為我國語料在全球訓練資料庫中之結構性弱勢。

二、語料結構之不對稱

語料結構之不對稱，得自投資結構與模型產出兩端分別觀之。就投資結構而言，世界經濟論壇與貝恩公司之聯合白皮書指出，美國與中國合計掌握全球 AI 價值鏈總投資逾六成，其投資版圖橫跨基礎設施、資料、基礎模型、應用與服務各環節，展現多數經濟體難以匹敵之投資規模[6]。

就我國語料之規模而言，數位發展部於 2025 年 12 月 24 日發布「臺灣主權 AI 訓練語料庫」，動員逾 200 個政府機關，上架逾 2,000 筆資料集，累計超過 6 億 tokens[7]。該數字在國內政策脈絡中屬重大成果，惟若與當代前沿模型動輒數兆 tokens 之訓練規模相較，其相對比重不言可喻。國家投入全部行政動能所能集結之本國語料，在全球語料池中所佔之比例，正是主權 AI 問題意識之量化表現。

若模型偏差之成因為語料結構而非傳播行為，則因應之道即不在於傳播管制，而在於語料供給。國家所應建立者，係使本國語言、文化與法律秩序得以充分進入訓練語料之制度條件。據此本文之論證重心將自「規制什麼」轉向「供給什麼」，此一轉向具有雙重意義。就規範對象而言，其將討論自對模型輸出之事後管制，前移至對訓練資料之事前供給，而供給之法律工具即為著作權法上之利用例外與資料法制上之開放義務。就規範形態而言，管制以禁止與制裁為手段，供給則以授權、給付與組織建置為手段，二者所受之法律保留密度與正當程序要求並不同。

三、研究目的及問題意識

據此，本文之研究目的有三。其一，釐清「主權 AI」作為法律概念之可能內涵。「主權 AI」一語源自產業論述而非學術傳統，其在政策文件中之流通速度遠快於其概念之澄清速度。概念之不確定性在法學上並非單純之用語問題：當立法者欲以「主權 AI」作為政策發展目標時，行政機關即取得高度之形成空間，法律

---

[5] 中央研究院，中研院資訊所對 CKIP-Llama-2-7b 之回應（民國 112 年 10 月 9 日），https://www.sinica.edu.tw/news_content/70/1850（最後瀏覽日：2026/09/05）。

[6] World Economic Forum & Bain & Company,Rethinking AI Sovereignty: Pathways to Competitiveness through Strategic Investments 6-8 (2026).

[7] 數位發展部，「臺灣主權 AI 訓練語料庫」上線！數位發展部攜手 200 個機關打造本土語料資源，2025/12/24，https://moda.gov.tw/press/press-releases/18314（最後瀏覽日：2026/09/07）。

授權明確性之審查亦因而失其基準。

其二，檢驗我國現行法制回應主權 AI 課題之能力。我國人工智慧基本法全文 20 條未見「主權」二字，而行政部門所推動之「AI 新十大建設推動方案」則已就算力與語料設定具體目標。政策先行而法制落後，其後果不僅為規範之不足，更在於以行政計畫支撐之制度欠缺存續保障，並使承辦機關與人員陷於責任不確定之狀態。

其三，提出與我國法秩序相容之制度建構方向。本文所採之比較對象為歐盟。選擇歐盟之理由並非其制度最為成功。恰相反，歐盟之政策密度為全球之最而技術依賴程度仍屬嚴重，而係其同時提供了制度設計之來源與失敗模式之樣本，得以使我國具有可比較參考之重要性。因此，本文之待答問題得歸納為以下：
首先，我國現行法（人工智慧基本法、著作權法、政府資訊公開法等）就主權 AI 所生之課題，其規範缺口何在？該等缺口彼此之間是否具有結構性之關聯？再者，在我國之法秩序、財政規模與立法資源之限制下，何種制度設計具有可行性？

四、研究方法及限制

本文之研究方法採文獻分析法，參閱中文及外文重要文獻與實務見解，檢視不同學者對於人工智慧法中關於主權 AI 之相關解釋並進行比較。

本文之研究範圍設有下列限制。第一，本文所處理者為主權 AI 之「供給端」課題，即資料、算力與模型之取得與支配；至於人工智慧輸出所生之侵權責任、演算法決定之正當程序保障、自動化行政處分之救濟等「適用端」課題，雖同屬人工智慧法之重要議題，惟其規範邏輯不同，非本文所能兼顧。第二，本文不處理國防與情報領域之人工智慧應用，該領域另有其特殊之保護法制。第三，本文所稱「主權」，不涉及國際法上關於我國國際法地位之爭議。

貳、主權 AI 之概念釐清

一、自數位主權至主權 AI 之概念演進

（一） 主權概念之數位轉譯

網際網路曾被期待終結國家主權。Barlow 於 1996 年宣稱「工業世界的政府們，你們這些血肉與鋼鐵構成的疲憊巨人，在我們聚集之處，你們沒有主權」[8]。然而，Chander 與 Sun 於〈主權 2.0〉一文中指出，該預言業已落空，並以 2020

[8] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 18 DUKE L. & TECH. REV. 5, 5-7 (2019)

至 2021 年間一連串「國家反擊」之事例為證：中國滴滴（Didi）於紐約證券交易所掛牌後隨即遭啟動網路安全審查並令其應用程式下架[9]、歐盟對大型科技公司處以鉅額反壟斷與資料保護罰款[10]、美國聯邦貿易委員會與司法部同時對主要平臺提起反壟斷訴訟[11]。

自國際法之角度觀之，其轉變之核心在於管轄權基礎之再建構。1648 年西發里亞和約所確立、以「領土」與實體「管轄」為核心之傳統主權概念，於網路空間之匿名性、跨境性與去中心化特質下遭遇挑戰；判斷「何人」應就虛擬空間中之行為負責、如何加以規制，成為學界必須面對之核心問題。Usman 等人則以「侵蝕、強化」雙重命題貫穿其分析，指出學界對 AI 與國家主權之關係結論分歧：一方主張 AI 因得以跨越國界、規避國家權威而侵蝕主權，另一方則主張 AI 因提升政府監控能力而強化主權[12]。此一雙重性正是主權 AI 論述在法律上必須首先處理之問題。若同一技術既侵蝕又強化主權，則「發展主權 AI」政策目標本身即不足以指引規範設計；真正需要界定者，係主權之何種面向受侵蝕、何種面向被強化，以及此消長是否符合憲政秩序之要求。

（二） 數位主權之雙面刃

Chander 與 Sun 就此提出一項對本文具重要性之觀點。其援引國際人權法學者 Henkin 之警語，指出「主權」一詞最常見之用法或許正是主權豁免，即免於法律、免於審查、免於正義；即數位主權對保護隱私、消費者權益、市場競爭與執法確有其重要性，論者往往忽略主權亦可能成為政府逃避外部監督、侵害人權之屏障。其將此稱為「數位主權之雙面刃」：數位主權既能保護居民，亦能用以控制居民[13]。本文以為，該觀察於規範層面尚得再進一步。數位主權之意義同時承載兩種可能，其一為保護公共能力、國家安全、民主自治與基本權，其二為正當化大規模監控、內容審查、歧視性行政與市場封閉。有學者則自另一角度提出警告，指出將主權 AI 界定為國家控制之增強，恐僅是以政府權力集中取代企業權力集中[14]。

---

[9] Anupam Chander & Haochen Sun, *Sovereignty 2.0*, 55 VAND. J. TRANSNAT'L L.283, 313 (2022). 滴滴於 2021 年 6 月 30 日已完成紐約證券交易所掛牌。然而，中國國家網際網路信息辦公室於同年 7 月 2 日啟動網路安全審查、7 月 4 日令其應用程式下架。

[10] *Id.*at 3.

[11] Anupam Chander & Haochen Sun , *Supra* note9, at 4.

[12] Hazrat Usman, Bushra Nawaz & Saiqa Naseer, *The Future of State Sovereignty in the Age of Artificial Intelligence*, 5 J.L. & SOC. STUD. 142, 144 (2023).

[13] Anupam Chander & Haochen Sun, *Supra* note9 at 26.

[14] Lucía Bosoer & Daniel Innerarity, *Unpacking AI Sovereignty*, STG POL'Y PAPERS, Issue 2025/18, at 5 (Eur. Univ. Inst. Sch. of Transnat'l Governance, Nov. 2025).

Roberts 認為僅以「控制」界定數位主權在規範上是有所不足的，其固然能豐富地描述行為者如何競爭、合作以掌控數位技術，卻無法提供評價這些行動正當性之機制；數位主權應被理解為聚焦於「權威」，亦即正當之控制規範性概念。依此檢視，大型科技公司雖具高度事實控制，卻欠缺輸入正當性、其輸出正當性亦有疑義，至多僅得評價為 AI 之「準主權者（Quasi-sovereign）」[15]。就公法而言，後者方為核心。國家對 AI 技術堆疊之控制主張，其正當性並非源自控制之事實，而係源自憲法所賦予之權限及其所受之拘束。

（三） 主權與國際主義之結構性悖論

亦有學者提出「主權—國際主義悖論」之概念，用以描述 AI 治理領域之結構性張力：國家一方面需要對演算法系統維持主權控制，另一方面卻又必須參與跨國合作以因應無國界之技術挑戰。並明確區辨該悖論與既有理論工具之異同，指出其不同於 Krasner 所稱之「有組織的偽善」，亦不同於 Keohane 與 Nye 之複合相互依賴理論，而係專指演算法治理領域所生之獨特規制張力。作者以歐盟與中國為對比個案，將歐盟人工智慧法（AI Act）定性為「風險導向」之超國家規制模式，將中國社會信用體系定性為「國家中心」模式，並提出「數位聯邦主義」作為整合地方、國家與全球層級規制協調之治理模型，主張其保留階層式協調[16]。此分析對我國之意義有二。其一，主權 AI 之制度設計必須預留國際互通與司法互助之媒介，否則主權主張將因無法與他國協調而自我孤立。其二，歐盟模式所呈現之「監理不對稱」現象，亦即執法責任下放至會員國層級所生之落差，對我國亦具警示意義。

二、概念之商業起源與語彙區辨

須辨明者，係「主權 AI」一詞之流通，其源頭並非學術界，而係硬體供應商之市場論述。NVIDIA（輝達）將主權 AI 界定為「一國運用其自身之基礎設施、資料、勞動力與商業網絡，生產人工智慧之能力」[17]，並將此概念與其「AI 工廠」產品緊密結合。該定義之特徵在於，其將「主權」實質等同於在地擁有特定供應商之運算設備。若援用相關語彙而未先行辨明其論述來源，將使主權之法律定義被簡化。

企業論述其後有所精緻化。國際商業機器公司（International Business

---

[15] Huw Roberts, *Digital Sovereignty and Artificial Intelligence: A Normative Approach*, 26 ETHICS & INFO. TECH., art. 70, at 5-6 (2024).

[16] Artur Ishkhanyan, *The Sovereignty–Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control*, 5 DISCOVER A.I.,art. 123, at 6 (2025).

[17] NVIDIA, *What Is Sovereign AI?*, NVIDIA Resources (last visited Aug. 21, 2026), https://resources.nvidia.com/en-us-telco-ai-factories-mc/en-us-telco-ai-factories/what-is-sovereign-ai.

Machines Corporation,IBM）之論述區分「AI 主權」與「主權 AI」，前者指組織或國家對其 AI 生態系（資料、模型、運作、治理）之控制權限，後者指其直接建置並控制之基礎設施與技術能力，並主張後者為前者之技術基礎[18]。EnterpriseDB 則提出三階遞進架構，主張資料主權是基礎、混合式 AI 基礎設施是設計、主權 AI 是結果[19]。

本文採 IBM 所提之二階區分，理由在於公法所關切者為前者之權限層次，基礎設施之所有權僅為其實現手段之一。惟須限定者，本文所採者僅為該區分之分析形式，即「權限層次」與「技術層次」之二分，而非其實質內涵。供應商論述之利益結構決定其定義之偏向：無論係輝達之「在地擁有運算設備」或 IBM 之「直接建置並控制之基礎設施」，均以採購其產品為主權之實現途徑，其偏向於法學分析上不具規範拘束力。準此，本文於下文建立判斷標準時，將「境內所有權」與「領域內在地化」明確排除於決定性要件之外，其原因即在於此。

三、定義困境及其法律後果

因此，如何定義主權 AI，則是一件困難的事，Pava 等人以「為 AI 主權下定義猶如試圖將果凍釘在牆上」為喻，歸納四項定義困境。其一，主權 AI 承接網路主權、資料主權與數位主權之未決辯論，其模糊性在政治上具有動員效果，同時亦使威權政府得援引以正當化審查與監控。其二，國家層次之硬性主權觀（追求完全自給自足）與軟性主權觀（框架為戰略自主）相互對立，而企業層次所追求之營運控制又與地緣政治意義之主權相混淆。其三，主權主張反應至技術堆疊各層時，各層本身另有自完整之詮釋光譜。其四，國家安全、經濟競爭力、監理監督與文化對齊四類目標彼此衝突，嚴格資料本地化雖可強化監理權限，卻可能抑制創新、限制國際研究協作並產生新的弱點。該文並將我國與智利並列為投資自主開源模型以追求文化自主作為相關案例[20]。

Bosoer 與 Innerarity 則提出三重憂慮：其一，將主權概念套用於數位領域，將類比世界之制度與邏輯強行移植進嶄新社會技術生態系統之風險，因 AI 就其本質具有跨國性，供應鏈之每一層均仰賴跨境互動與相互依賴，即便美國亦無法

---

[18] Stephanie Susnjara & Ian Smalley, *What is AI Sovereignty?*, IBM THINK (Feb. 4, 2026), https://www.ibm.com/think/topics/ai-sovereignty.

[19] EnterpriseDB, *Data and AI Sovereignty*, EDB (last visited Aug. 21, 2026), https://www.enterprisedb.com/what-is-sovereign-ai-data-sovereignty.

[20] Juan N. Pava, Caroline Meinhardt, Elena Cryst & James Landay, *AI Sovereignty's Definitional Dilemma*, STANFORD HAI (Feb. 17, 2026), https://hai.stanford.edu/news/ai-sovereigntys-definitional-dilemma.

完全掌控整條 AI 堆疊（AI Stack）[21]；其二，將主權 AI 界定為國家控制之增強，恐僅是以政府權力集中取代企業權力集中；其三，主權論述之模糊性使其易於被各種相互衝突之政策目標所徵用[22]。

上開分析於法律上之後果，在於概念之不確定性直接影響法律授權明確性原則之判斷。當立法者以「主權 AI」為政策目標而未界定其構成要件時，行政機關即取得高度之形成空間。

四、主權 AI 之四大面向

（一）資料、模型、基礎設施與價值對齊

綜合上開分析並參酌國內外既有研究，主權 AI 之內涵得劃分為四個面向。此分類並非逕自既有定義移植而來，而係綜合前述學說爭議與我國制度現況所為之整理；國際組織之定義得為部分佐證，惟其涵蓋範圍較本文為窄。世界經濟論壇將主權 AI 界定為「國家透過規劃及建立人工智慧基礎設施、核心能力與產業，藉此增強國家競爭力，並提振未來發展[23]」，而經濟合作暨發展組織之補充見解則強調，主權 AI 除資料主權外，尚須包含模型訓練與「計算主權」（Compute Sovereignty），亦即自主高效能運算與雲端推理架構[24]。二者合計涵蓋本文所稱之資料、模型與基礎設施三面向，至於價值對齊一面向，則為我國制度實踐所應著重者，故本文另立為第四面向。因此，主權 AI 之四大面向可大致劃分如下：

1. **資料**：關切重點在於訓練語料之取得、品質與合法性。其法律爭議集中於著作權法上之文字與資料探勘、個人資料保護法上之處理合法性基礎，以及政府資料開放之授權密度。
2. **模型**：關切重點在於模型權重之可取得性、可檢視性與可修改性。專有模型、開放權重模型與符合開放原始碼倡議定義之開源模型，三者在可支配性上存有本質差異[25]。則該差異直接決定國家對模型之法律支配是否可能。

---

[21] AI 堆疊係指涵蓋基礎架構、資料處理、模型開發、部署、應用及治理各層級的技術整合架構，用以支撐 AI 系統從研發到運行的端到端生命週期。詳參：Cole Stryker，*What is an AI Stack?*, IBM THINK (Nov. 29, 2024)，https://www.ibm.com/think/topics/ai-stack（最後瀏覽日：2026/09/05）。

[22] Lucía Bosoer & Daniel Innerarity,*Supra* note 14,at 4-5.

[23] Muath Alduhishy，*Sovereign AI: What it is, and 6 strategic pillars for achieving it*, WORLD ECON. F. (Apr. 25, 2024),https://www.weforum.org/stories/emerging-technologies/sovereign-ai-what-is-ways-states-building/(last visited Sept. 5, 2026).

[24] OECD, *A Blueprint for Building National Compute Capacity for Artificial Intelligence*, OECD DIGITAL ECONOMY PAPERS, (Feb. 27, 2023),https://doi.org/10.1787/876367e3-en(last visited Sept. 5, 2026).

[25] Gregory Smith, *Open Models, Digital Sovereignty, and the Future of AI: Why This Debate Matters for Trinidad and Tobago*, UNDP (Aug. 13, 2026), https://www.undp.org/trinidad-and-tobago/blog/open-models-digital-sovereignty-and-future-ai-why-debate-matters-trinidad-and-tobago (last visited Sept. 5,

3. **基礎設施（即計算主權）**：關切重點在於算力之所在地與其管轄歸屬。數位發展部部長林宜敬就此提出極為精確之表述：「算力中心在哪裡，就受哪個國家的法律管轄。」其並以打詐經驗為例，說明社群平臺伺服器位於美國或新加坡、通訊軟體伺服器位於日本時，我國法律難以直接管轄之困境[26]。
4. **價值對齊**：關切重點在於模型輸出是否符合本國之社會共識與法律秩序。此層面在我國具有特殊重要性，其操作化即為後述 AI 產品與系統評測中心之「臺灣價值觀」評測指標[27]。

（二）三層結構：實體層、程式碼層、資訊層

四大面向之分類，其功能在於界定主權主張之標的；欲進一步處理干預強度與法律依據密度之問題，尚須引入分層控制之架構。該架構之學術淵源，得追溯至 Chander 與 Sun 所整理之數位主權定義光譜[28]。該文列舉四種學說：Woods 將資料主權界定為傳統國家主權三要素之延伸，並區分「令企業遵守之權力」與「決定遵守方式之權力」；Ke Xu 將網路空間之主權區分為實體層、程式碼層與資料層三層次；Luciano Floridi 自個人主權出發，將數位主權定義為對資料、軟體、標準與協定、程序、硬體、服務及基礎設施之控制；Paul Rosenzweig 則將問題化約為管轄權問題，並提出「地理即命運」之推論。

此外，Mügge 就歐盟脈絡亦採相同之三分：數位主權涵蓋對實體層（基礎設施、裝置）、程式碼層（標準、規則、設計）與資訊層（內容、資料）之控制需求[29]。未來社會智庫則進一步將此架構與治理工具相連結，主張須透過投資與採購、規則標準及認證、外交、能力建設四項工具，分別對三大技術層次行使控制[30]。本文以下採 Mügge 之用語，即實體層、程式碼層與資訊層；Ke Xu 所稱之「資料層」與本文之「資訊層」指涉相近，惟後者兼含內容與資料，範圍較廣，併此敘明。

2026).

[26] iThome，數發部揭主權 AI 策略：算力中心必須在臺灣、模型需具備 3 大理解力，另看好主權 AI 服務出海，2026/07/01，https://www.ithome.com.tw/news/177017（最後瀏覽日：2026/09/05）。

[27] TechNews，AI 評測中心公布模型評測，Gemini 2.5 Flash 最具「台灣價值觀」，2025/10/03，https://infosecu.technews.tw/2025/10/03/aiec-unveils-its-first-model-benchmark-results/（最後瀏覽日：2026/09/05）。另參見：數位發展部數位產業署，AI 產品與系統評測中心(AIEC)公布最新語言模型評測結果，強化 AI 在地能力與可信任發展，數位產業署網站，民國 115 年 5 月 4 日，https://moda.gov.tw/ADI/news/latest-news/19588（最後瀏覽日：2026/09/10）。

[28] Anupam Chander & Haochen Sun ,*Supra* note9 at 9-10.

[29] Daniel Mügge, *EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?*, 31 J. EUR. PUB. POL'Y 2200, 2200-01 (2024).

[30] Nick Moës et al., *Beware of Geeks Bearing Gifts: Building True EU Frontier AI Sovereignty*, THE FUTURE SOC'Y, Apr. 17, 2026, https://thefuturesociety.org/wp-content/uploads/2026/04/Beware_of_Geeks_17April26.pdf (last visited Sept. 10, 2026).

臺灣方面，李建良教授則就主權 AI 所提出之「客體思維法」與「主體思維法」，與上開分層架構得相互補充。前者著重於支配力所及之客體，如資料、基礎設施、網際網路與運算能力；後者則追問主權者為何，究係國家、企業抑或個人[31]。客體思維法為主權 AI 提供物質基礎之分析框架，主體思維法則為其民主正當性與問責機制提供規範依據。

分層控制架構之作用有二：其一為適合性審查之精確化。主權措施若未與其所欲控制之技術層次相對應，即難通過比例原則中適當性之檢驗。以資料在地化為例，若僅要求資料儲存於境內，而未同時要求加密金鑰之管理與營運控制在地化，則資料仍可能為境外主體所實質取用。此即「資料落地提供的是位置，主權需要的則是控制。」此一落差並非靜態，反而隨技術演進而擴大。代理式 AI 使存取不再限於人類使用者與傳統應用程式，AI 代理得自主檢索資訊、觸發工作流程並跨平臺交換內容，形成所謂「影子資料移動」，傳統以人類使用者為中心之存取控制模型可能因而失效[32]。其於適合性審查上之意義在於，僅及於實體層（儲存位置）之措施，對發生於程式碼層與資訊層之存取行為不生控制效果；以實體層手段追求資訊層目的者，其手段與目的間欠缺實質關聯。其二為授權密度之分級。各層之干預強度不同，所要求之法律依據密度亦應有別。實體層之算力建置之法律依據密度得較低；資訊層之語料徵集涉及著作權與個人資料，須有明確之法律授權；程式碼層之標準制定與認證則具有事實上之市場准入效果，應受法律保留之較高要求。

（三）面向與層次之對應

四大面向與三層結構並非同一分類之兩種說法，而係兩個相互交錯之維度：前者回答「主權主張之標的為何」，後者回答「該主張作用於技術堆疊之何處」。二者交錯之結果如下表，其實益在於使干預手段與法律依據密度得以逐格檢視。

面向	主要落點	干預手段之典型	法律依據密度
資料	資訊層	語料徵集、開放義務、利用例外	高（涉著作權與個人資料，須明確法律授權）
模型	程式碼層	權重取得要求、透明義務、評測認證	高（認證具市場准入效果，受法律保留較高要求）
基礎設施	實體層	算力建置、在地化要求、採購條件	中低（涉差別待遇者仍受平等原則拘束）

[31] 李建良，數位社會的智慧治理法制：思維框架的建構，收於：數位社會的智慧治理，元照，頁 9 以下，2026 年。

[32] Andrea Benito, *Sovereignty Beyond Residency: Why Gulf Governments Must Rethink AI Control*, COMPUTER WEEKLY, Aug. 12, 2026, https://www.computerweekly.com/news/366648672/Sovereignty-beyond-residency-Why-Gulf-governments-must-rethink-AI-control (last visited Sept. 10, 2026).

價值對齊	資訊層與程式碼層之交界	評測指標、採購加分、標示義務	高（涉價值認定權限，應以法規命令定之）

上表末欄之判斷，於第參章將以我國現況逐項檢驗，於第伍章則為各項修法建議之規範形式選擇依據。

五、小國之策略選擇：可控的相互依賴

（一）全技術堆疊主權之不可行性

分層架構之實益，在於使「全技術堆疊主權」之不可行性得以具體呈現。布魯金斯學會與歐洲政策研究中心之聯合報告將主權 AI 界定為「一系列旨在強化一國對關鍵 AI 基礎設施之部署、使用與採用作成獨立決策能力之策略光譜，而非字面意義上之自給自足」[33]，並指出對幾乎任何國家而言，全堆疊主權 AI 在結構上均屬不可行，因 AI 是一套具跨國性質之技術堆疊，於礦產、能源、運算硬體、網路、數位基礎設施、資料資產、模型、應用，以及人才與治理等要素上，均存在集中化之樣貌。該報告並提出四分類架構，將主要行為者區分為「廣域堆疊領導者（Broad system leaders）」如：美國、中國、歐盟、「協調型堆疊建構者（Stack builders）」如：印度、日本、英國、「策略層次專家（Layer specialists）」如：臺灣、加拿大、德國、新加坡、南韓與「其他起步中之 AI 部署國（Other countries）」[34]。

Jurgens 則自另一角度提出質疑，其以台積電亞利桑那廠為例，指出美國政府依晶片法所給予其 66 億美元補助設廠，然生產之晶片仍落後臺灣廠一個世代，理由在於「產線得以遷移，學習曲線無從遷移」；復以中國估計投入約 1,500 億美元試圖投資電路產業，然整體規模而仍落後數個世代為例，主張即令中央集權、資本充足且市場龐大之大國，亦受制於戰略速度瓶頸[35]。本文並不全盤接受其「主權技術堆疊係根本性戰略誤判」之觀點，該結論係自產業效率之角度立論，未考慮主權措施尚承擔管轄權維持與民主正當性之功能，二者不能以效率單一標準衡量，惟認為其對「控制戰略資源等同於控制結果」此預設之拆解，正是主權 AI 論述在法學上必須通過之第一道檢驗。其於法學上之意義在於：主權措施之適當性審查，不得以「取得所有權即達成目的」為當然前提。

---

[33] Brooke Tanner, Cameron F. Kerry, Andrew Wyckoff, Nicoleta Kyosovska, Andrea Renda & Elham Tabassi, *Is AI Sovereignty Possible? Balancing Autonomy and Interdependence* 1 (Brookings Inst. & Ctr. for Eur. Pol'y Studies, Report, Feb. 2026), https://www.brookings.edu/wp-content/uploads/2026/02/20260217_AI_sovereignty_final.pdf (last visited Sept. 10, 2026).

[34] *Id.*at 5.

[35] Jeremy Jurgens, *The Myth of AI Sovereignty*, FOREIGN POL'Y (Mar. 9, 2026), https://foreignpolicy.com/2026/03/09/artificial-intelligence-ai-sovereignty-taiwan-semiconductor-manufacturing-tsmc-chip-supply-chain-united-states-china/ (last visited Sept. 10, 2026).

（二）可控的相互依賴作為替代方案

可行之替代方案，係透過繪製依賴關係、優先處理可行之干預點、多元化供應商與夥伴，並藉技術標準、政府採購及治理機制嵌入互通性與可攜性，將依賴關係置於本國法律管轄之下[36]。該路徑於政策研究中另有數種表述，其共同特徵在於以「條件之設定」取代「連結之切斷」。

同一路徑於政策研究中另有數種表述。Joshi 以 2026 年 2 月阿聯酋與印度所簽署之主權 AI 基礎設施協議為例，指出該協議之資金來自阿聯酋、技術來自美國晶片與美阿雙方之硬體專業，卻須受印度治理框架與資料本地化要求管轄，並據以主張「戰略自主」或「可控的相互依賴」構成美中二元依賴以外之第三條路[37]。Chapman 等人則主張，AI 主權在實踐上更宜理解為「AI 自主性（AI agency）」，亦即一國依其國家利益執行選擇之能力；各國多採混合策略，即在確保獲得外國人工智慧模型和硬體的同時，努力實現國內能力的多元化和發展（採用自主研發或修改後的外國開源軟體），以應對此類取得中斷的情況。該文並指出，主權 AI 計畫普遍存在雄心與執行能力之落差，其待決問題在於辨別何種使用情境得以較低階模型滿足，何種情境須確保前沿模型之取得[38]。

Chapman 等人另指出一項對我國具警示意義之觀察：多數中等強國與新興經濟體之主權討論，主要由依賴、掠奪性經濟模式、市場集中度與地緣政治從屬地位等所驅動，而非由跨境大規模風險所驅動[39]。這個觀察提醒我國，主權 AI 之政策論述若僅停留於產業競爭力，將難以與國際上以風險為核心之治理規範接軌，我國人工智慧基本法第 16 條所欲「與國際介接」之目標亦將落空。

（三）利基型主權與我國之典型定位

世界經濟論壇與貝恩公司之白皮書提出「完整的 AI 主權遙不可及，持久的優勢並非如此」之核心觀點，並將 AI 主權界定為「各經濟體依其自身價值觀形塑、部署與治理 AI 生態系統之能力，同時透過在地化投資與可信賴之國際合作相結合，確保策略性與營運性之控制、彈性，並最終獲得韌性」。該報告指出，「AI 主權」已與「AI 基礎設施」及資料中心過度混為一談，儘管 AI 基礎設施確

---

[36] Brooke Tanner, Cameron F. Kerry, Andrew Wyckoff, Nicoleta Kyosovska, Andrea Renda & Elham Tabassi,*Supra* note33,at 6.

[37] Shreya Joshi, *Early Lessons in the Pursuit of Sovereign AI*, Carnegie Endowment for Int'l Peace (June 17, 2026), https://carnegieendowment.org/research/2026/06/early-lessons-in-the-pursuit-of-sovereign-ai.

[38] Conor Chapman, Jon Bateman, Andrew Grotto, Colin Kahl, Arthur Nelson & Lakshmee Sharma, *AI Sovereignty, Diffusion, and Risk: Strategy in a Contested Landscape* (Stanford Program on Geopolitics, Tech. & Governance & Carnegie Endowment for Int'l Peace, Policy Brief, Aug. 12, 2026),https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2026-08/gtg-ceip_ai_sovereignty_2026-08.pdf (last visited Sept. 10, 2026).

[39] *Id.*

為迫切課題，卻非唯一之決定性因素[40]。

就我國之定位而言，該報告指出約九成之全球晶圓代工營收集中於台積電、聯電、三星晶圓代工與中芯國際四家公司[41]。該結構使我國在 AI 價值鏈中居於特殊地位。Jurgens 以荷蘭艾司摩爾（ASML）為例，指出荷蘭本身不設計晶片、不製造晶片、亦不訓練 AI 模型，惟該公司作為全球唯一能製造最先進極紫外光微影系統之企業，使荷蘭取得對全球 AI 生態之實質影響力[42]。

此一「不可或缺性」模式，相較於「全技術堆疊主權」模式，對我國具有更高之可移植性，因我國台積電之晶片供給，為各國迫切所需。惟須補充一項前提：供應鏈上之不可或缺地位，其本身為經濟事實而非法律地位；該事實得轉化為規範影響力者，係以我國具備可供他國依循之法制內容為條件。荷蘭之影響力所以得以行使，係因其得透過出口管制法制與歐盟共同貿易政策之參與而具體化。本文據此主張，我國主權 AI 之法制設計，其重心應置於如何將供應鏈上之不可或缺地位轉譯為規範制定與國際協商之籌碼，而非投注於難以達成之全技術堆疊建置。國內有研究指出臺灣發展主權 AI 需採取「以應用為中心」戰略，強化數位基礎設施和培養 AI 人才[43]，惟本文認為，應用自主化尚須以規範參與能力為後盾，否則我國仍將處於規則接受者之地位。

六、本文之界定：三項判斷標準

（一）選擇性主權：自國家層次至組織層次之操作化

IBM 企業價值研究院之研究報告，將 AI 主權自國家層次移至組織層次，並提出一項對本文具直接操作價值之定義：「AI 主權不等於擁有整條技術堆疊，而是在條件變化時仍保有控制力。[44]」該報告依據一項於 2026 年 2 月至 4 月間對全球 16 個地理區域、17 個產業、1,000 位高階主管所做之調查，發現僅 9%之高階主管自認對其 AI 供應商、模型與基礎設施之依賴關係具優異理解，71%表示若今日必須更換其主要 AI 供應商或模型將面臨困難，而 72%之高階主管願意接受 20%之成本增加，以維持多家 AI 供應商所帶來之戰略彈性；在 AI 堆疊各面向具備最強控制力之組織，較控制力較弱之組織多保護 55%之營運利潤免受 AI 之營運中斷影響。

---

[40] World Economic Forum & Bain & Company, *Supra* note 6,at 4.

[41] World Economic Forum & Bain & Company, *Supra* note 6,at 8

[42] Jeremy Jurgens, *Supra* note35.

[43] 廖明輝、洪尉淳，各國發展主權 AI 策略對我國的啟示，經濟前瞻，215 期，頁 88，2024 年。

[44] IBM Institute for Business Value, THE CALCULUS OF AI SOVEREIGNTY: BALANCING CONTROL, FLEXIBILITY, AND RISK 3 (June 16, 2026), https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-sovereignty (last visited Sept. 10, 2026).

該報告最具制度設計價值者，為其以五項要素定義 AI 主權之具體內涵，**可見性（Visibility）**：掌握依賴關係、暴露風險與鎖定點、**治理（Governance）**：執行政策、合規與存取邊界、**可攜性（Portability）**：跨境移動資料、**可替代性（Substitutability）**：於需要時更換模型或供應商，以及**持續性（Continuity）**：於中斷或效能劣化期間維持營運[45]。該報告並指出，AI 將依賴延伸至模型層及其周邊服務，引入新型態之波動性：模型可能在無正式發布週期之情況下改變行為，服務條款與安全控管可能在毫無預警之情況下更新；過去 24 個月間，高階主管回報之非預期變化包括價格大幅上漲、使用限制、模型或服務停用、隱私與資料處理條款變更、效能劣化，以及新的地理存取限制[46]。

此五項要素雖以企業治理為對象，惟其對法律之意義甚為直接。行政機關若使用 AI 執行公權力時，其所面臨之依賴風險與企業並無二致，而其後果更為嚴重：企業之營運中斷造成財產損失，行政機關之營運中斷則造成公共服務停擺與人民權利無從實現。惟企業治理之五要素不得逕予移植為公法判準。其理由在於，企業之控制力係為維護營運利益而設，其正當性來源為所有權與契約；行政機關之控制力則係為履行憲法所課予之公共職能而設，其正當性來源為法律授權，並須受法律保留與比例原則之拘束。故本文於下文所提之判準，係就該五項要素為規範性之再建構，而非其翻譯。

（二）本文之界定與三項判準

在上開基礎上，本文將主權 AI 界定為：國家為維持其憲政秩序下之公共職能，就人工智慧技術堆疊各層之依賴關係，建立透明化、可替代性與有效法律支配之制度安排。

1. **透明性**：要求依賴關係本身得被識別與描述，包括供應商之法域歸屬、可取用之模型資訊範圍與營運持續安排。此判準對應 IBM 五要素中之「可見性」；前文所示僅 9%之高階主管自認對其依賴關係具優異理解，正說明透明性並非自然狀態，而須以制度強制之。
2. **可替代性**：要求存在實際可行之退出路徑，其內容包括契約上之轉換與退出條款、技術上之互通性與可攜性，以及市場上之供應商多元化。該判斷標準對應 IBM 五要素中之「可攜性」與「可替代性」。Ren Ito 就此主張，判斷標準應自「是否擁有」轉為「是否保有選擇權」，並將多元化提升至另一層次，亦即依賴多個模型而非單一供應商本身即構成一種威懾，因其降低脅迫之有

---

[45] *Id.*at 10

[46] IBM Inst. for Bus. Value, *Supra* note 44,at 8.

效性[47]。

3. **有效法律支配**：要求本國法律對該依賴關係具有實際之規範效力，其核心為管轄權連結之建立。該判準對應 IBM 五要素中之「治理」與「持續性」，亦即政策執行、合規邊界之劃定，以及中斷期間公共行政之運作。依前述 Roberts 之區分，本判準所要求者為「權威」而非單純之「控制」：控制之事實不生正當性，其正當性須來自憲法所賦予之權限，並以該權限所受之拘束為界。

境內所有權與領域內在地化雖屬相關因素，惟均非決定性。以此三項判準衡量，主權 AI 之達成程度得以分層評估，而非陷於「有主權或無主權」之二元判斷。三項判準之間並非彼此獨立，而具有階層關係。透明性為其餘二者之前提：依賴關係未經識別者，無從評估其可替代性，亦無從判斷本國法律是否及於該關係。可替代性則為有效法律支配之實效條件：欠缺退出路徑者，縱有管轄權連結，其規範之執行仍將因轉換成本過高而受制於受規範者。

七、小結

本章之分析得歸納為三點。第一，主權 AI 係數位主權之次概念，其範圍涵蓋資料、模型、基礎設施與價值對齊四個方面，而各面向又分別落於實體層、程式碼層與資訊層之技術結構中；分層控制架構之實益，在於使干預強度與法律依據密度之分級成為可能。第二，全技術堆疊主權對我國並不可行，可行者為可控的相互依賴，亦即以法律機制設定依賴條件，而非切斷對外連結；就我國之特殊處境而言，艾司摩爾（ASML）式之「不可或缺性」較之「全技術堆疊」更具可移植性。惟其轉化為規範影響力，仍以我國具備可供他國依循之法制內容為條件。第三，主權論述本身具有雙面性，其既得回復民主自我統治之能力，同一套語彙亦得為監控、審查與市場封閉提供正當化基礎，故主權措施必須回歸一般法律之審查。

據此，本文提出透明性、可替代性與有效法律支配三項判斷標準。該三項判準係就企業治理研究所提之可見性、治理、可攜性、可替代性與持續性五項要素為規範性之建構，並非其移植；其相互關係為階層而非平行，即透明性為其餘二者之前提，可替代性為有效法律支配之實效條件。以下第參章即以此三項判準檢視我國現況。

---

[47] Ren Ito, *AI Sovereignty Is About Options, Not Ownership*, TAIPEI TIMES, June 25, 2026, https://www.taipeitimes.com/News/editorials/archives/2026/06/25/2003859687 (last visited Sept. 7, 2026).

參、我國主權 AI 及相關治理法制之現況與挑戰

一、政策架構與法制架構之落差

我國主權 AI 之政策落點，主要集中於「AI 新十大建設推動方案」。該方案於 2026 年 1 月核定[48]，計畫期程為民國 114 年至 117 年（2025 年至 2028 年），其中第七項即為「主權 AI 及算力建設」[49]，主辦機關為國家科學及技術委員會。方案揭示 AI 時代「算力即國力」，記載我國於 2025 年 11 月全球算力排名第 13、亞洲排名第 4，並就算力建設設定「至 2028 年完成累計能耗約 20MW、至 2029 年約 23MW」之目標；另於「鞏固主權 AI」之項目下，設定完成算力建置之目標。

方案就語料庫之規劃分為四項：打造臺灣主權 AI 訓練語料平臺、訂定授權條款、強化公私部門語料釋出動能、促進主權 AI 模型之應用發展[50]。其中第二項明載「偕同經濟部智慧財產局及專家學者，共同研擬《臺灣主權 AI 訓練語料授權條款》及相關使用規範，並請經濟部智慧財產局針對政府機關持有之中文語料是否可授權供 AI 訓練使用，研提相關授權適用說明」。

與此政策密度相對照者，為法制規範密度之不足。我國人工智慧基本法全文 20 條，未見「主權」二字，亦未就算力、模型權重與跨境管轄設有任何規範。該法第 13 條雖規定「政府應建立資料開放、共享及再利用機制，以提升人工智慧使用資料之可利用性」，並要求「致力提升我國人工智慧使用資料之品質與數量，確保訓練及產出結果足以展現國家多元文化價值與維護智慧財產權」，惟其規範形態為對政府之綱領性作為要求，欠缺構成要件與法律效果之對應，亦未指定主管機關與完成期限。政策先行而法制落後，形成本文之核心問題意識。

二、可信任 AI 對話引擎（TAIDE）計畫

為保護在地文化、確保我國數位主權，國科會自 2023 年 4 月起推動「可信任 AI 對話引擎」（Trustworthy AI Dialogue Engine，TAIDE）之開發[51]，其技術路

---

[48] 行政院，AI 新十大建設推動方案(114 年至 117 年)，國家發展委員會網站，民國 115 年 1 月 28 日行政院核定，https://www.ndc.gov.tw/Content_List.aspx?n=EF80A54FA6A63200（最後瀏覽日：2026/09/10）。

[49] 行政院，AI 新十大建設推動方案（核定本），頁 86，民國 115 年 1 月。

[50] 同上註，頁 87。

[51] 行政院（國家科學及技術委員會提供資料），完善臺灣 AI 基礎建設—打造可信任 AI 對話引擎 TAIDE，行政院全球資訊網「重要政策」，民國 113 年 6 月 11 日，https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/582206fe-26fc-4184-b911-aa6e4569ff3e（最後瀏

線為在既有開源模型基礎上進行微調與持續訓練：初期以 Meta 之 Llama 2 或 Llama 3 為基礎，加入具臺灣主體性之內容資料進行訓練；其後轉以 Google 之 Gemma-3 為基礎進一步訓練[52]。

價值對齊之評測，則由數位發展部、工業技術研究院與國家資通安全研究院共同成立之「AI 產品與系統評測中心」（AIEC）辦理。該中心於 2025 年 10 月 3 日首次公布語言模型基準評測結果，採用三項指標，即「高中學測國文科」、「高中學測社會科」與「臺灣價值觀」，受測模型共 42 款[53]。「臺灣價值觀」指標之設計方法，據數位發展部說明，係以 50 道「臺灣藍綠白政黨有共識，但與中國共產黨沒有共識」之題目測試[54]。

就最新（2026 年 8 月語言模型，9 月 2 日所公布）評測結果而言，最新一期受測模型已增至 188 款，總分係三項指標正確率之加總。居前者依序為 GPT-5.6-Sol（274.00%）、Claude-Fable-5（271.96%）與 Gemini-2.5-Pro（270.71%）；「臺灣價值觀」獲滿分者則為雅婷智慧 Yating-FedGPT-1.10.18 與亞太智能機器 ACE-1-24B-2604，均屬國內業者之中小型模型。惟學科能力與價值對齊未必同向，Gemini-3.5-Flash 兩科學測正確率分居前列（96.76%、89.46%），臺灣價值觀正確率僅 14.00%，總分退居第 61 名。以 188 款模型計算，兩科學測正確率之相關係數為 0.94，學科平均與臺灣價值觀正確率之相關係數則僅 0.22[55]。

暫不論具體分數，此評測機制之建立仍具三重制度意義。其一，為本土模型之能力評估提供客觀基準。其二，「臺灣價值觀」指標之設計，將抽象之文化主權轉譯為可操作、可驗證之技術指標，此為主權 AI 論述在我國最具體之制度成果。其三，評測結果得作為政府採購決策與模型認證之參考依據，從而使價值對齊自政策宣示轉為具有法律效果之判準。

惟須指出者，該指標以政黨共識為設計基礎，其於價值多元社會中之正當性基礎為何，以及由行政機關認定何謂「臺灣價值觀」是否逾越其權限，均為尚待

覽日：2026/09/10）。

[52] 國家科學及技術委員會，TAIDE——推動臺灣可信任生成式 AI 發展，計畫重點研發與活動歷程，TAIDE 官方網站，https://taide.stpi.niar.org.tw/（最後瀏覽日：2026/09/10）。

[53] AI 產品與系統評測中心（AIEC），開源／指標模型測試結果，AIEC 官方網站，2026 年 9 月 2 日更新，https://www.aiec.org.tw/web/guest/result（最後瀏覽日：2026/09/10）。

[54] iThome，同註 26。

[55] 需註明者，該評測指標其後有所擴增。2026 年 6 月 30 日公布之版本於三項基礎指標外增列兩岸議題（陸委會）與銀行、保險、證券（金管會）題組，7 月 27 日之版本再納入政治學、地方自治及法務部出題之法務指標，受測模型 32 款。法務指標區分「一般民眾」與「司法人員」兩種題型，各模型於後者之正確率普遍低於前者，如 Claude-Opus-4.8 為 92.22%對 78.33%，GPT-5 為 92.78%對 67.50%。

處理之課題。該疑慮並非我國所獨有。Chander 與 Sun 所指出之「數位主權雙面刃」，其在價值對齊評測上之具體形態，即為國家如何認定「正確價值」之權限[56]。本文認為，評測指標之設計程序、指標內容之公開性，以及模型提供者對評測結果之爭議管道，應審慎考慮台灣多元價值文化。

三、臺灣主權 AI 訓練語料授權條款

數位發展部與經濟部智慧財產局於 2025 年 12 月共同推出《臺灣主權 AI 訓練語料授權條款——第 1 版》（Taiwan Sovereign AI Training Corpus License - Version 1）[57]。就法律性質而言，該條款屬定型化之著作財產權授權契約，其功能在於「讓語料釋出有明確的授權依據，降低個別著作權商議所要付出的龐大行政成本，減少 AI 訓練資料可能產生的著作權爭議」。該條款有兩項設計，就降低合規行政成本而言具有實質進步性。

其一為授權撤回不溯及既往原則。條款明定，被授權人依訓練所得之成果，包括所產出之模型、權重與生成程式碼、文件或其他型態之輸出成果，若具著作權保護要件，應歸屬於被授權人或模型操作者所有；即使原語料資料後續停止提供使用，不影響已完成之訓練成果[58]。該設計所處理者，為 AI 訓練之不可逆性問題。模型一經訓練完成，其權重即無法將特定語料之影響單獨移除；若允許授權人事後撤回而溯及影響已完成之模型，則被授權人將面臨無法履行之義務。該原則在法律上之意義，在於其將授權關係之風險分配，自「授權人得隨時回復原狀」調整為「授權人得終止未來之利用，但不影響已生之法律效果」。

其二為簡化標示義務。條款要求被授權人於產出模型、權重等工具或輸出平臺時，應標示語料平臺及相關識別資訊，包括資料集名稱、版本號、資料集提供者、發布年份、資料集申請頁面或官方網站；惟明定「鑒於人工智慧訓練涉及多元來源之語料資料混用，授權人同意就本授權條款發布之語料資料進行識別資訊標示時，被授權人僅需就語料平臺提供之語料資料庫或資料集名稱及其他相關識別資訊進行標示，毋須就本授權語料資料內含個別素材進行逐項標示」[59]。該設計直接回應了 AI 訓練場景中逐項標示在技術上不可行之現實，並調整為「集中

---

[56] Anupam Chander & Haochen Sun , *Supra* note9 at 36-37.

[57] 數位發展部，「臺灣主權 AI 訓練語料庫」上線！數位發展部攜手 200 個機關打造本土語料資源，行政院國家永續發展委員會網站，民國 114 年 12 月 24 日，https://ncsd.ndc.gov.tw/Fore/News_detail/31d6cb25-fe44-4550-b9ea-5b0d33b63b97（最後瀏覽日：2026/09/10）。

[58] 數位發展部、經濟部智慧財產局，臺灣主權 AI 訓練語料授權條款——第 1 版（Taiwan Sovereign AI Training Data License, Version 1.0），2025 年 12 月，第二點授權同意。

[59] 數位發展部、智慧財產局，同上註，第三點標示義務。

標示」。

上開兩項設計值得肯定，惟該條款作為制度工具仍有三項限制。第一，其效力僅及於授權人自身管理之語料，無從解決對既有著作進行文字與資料探勘之合法性問題。第二，條款所定「被授權人應就語料資料之使用成果，於合理範圍內設置適當防護機制，以避免與原語料資料產生實質近似」[60]，其中「實質近似」之認定標準與「合理範圍」之界限，在生成式 AI 領域中之操作可行性尚待驗證。第三，條款第二點明定授權「不得再授權與轉讓」，惟在多階段訓練、模型設計及開放權重發布等技術場景中，其限制之實際效力仍有爭議。尤須指出者，該限制與國家自身之政策目標存有內在衝突：主權 AI 之政策既以開放權重模型為推動方向，而以主權語料訓練所得之模型若受不得再授權之拘束，其權重之公開釋出即生疑義。政策工具之間欠缺一致性，其成本終將由使用者承擔。

最根本之限制在於，以此私法契約安排無從創設行政機關取得或使用資料之公法權限，亦無從對抗未參與該授權關係之第三人。授權條款所能達成者，係在既有法律框架內降低交易成本；其所不能達成者，係填補法律框架本身之空白。

四、四大結構性挑戰

（一）公部門算力匱乏與實質法律管轄權之喪失

依 2026 年 3 月之報導，數位發展部現有可提供業者使用之 GPU 約 40 片，係於 2024 年購入。規劃再添購約 100 片，若預算通過，整體可提供業者使用之 GPU 數量將達 140 片。部長林宜敬並說明，因 2025 年相關預算遭刪減，導致算力擴充進度受到影響[61]。該數字之意義，一為於 GPU 之規模，二為則在於其導致之管轄後果。當公部門與本國業者無從於境內取得足夠算力時，模型之訓練與部署即向境外遷移；模型一旦於境外運行，我國法律對其之規範效力即大幅減損。部長林宜敬所稱「算力中心在哪裡，就受哪個國家的法律管轄」[62]，正是此一因果鏈之簡明表述。

算力匱乏於本文三項判準上各有其對應之後果。就透明性而言，境外運行之模型，其訓練紀錄與運作日誌不在我國機關可取得之範圍。就可替代性而言，一旦公共服務建立於特定境外平臺，其轉換成本將隨時間累積而趨於不可承受；

---

[60] 數位發展部、智慧財產局，同註 58，第四點使用政策。

[61] 蘇文彬，數發部今年擬增購 100 片 GPU 擴大產業免費可用 AI 算力資源，與金管會討論開放保險業投資 AI 算力，iThome，2026 年 3 月 4 日，https://www.ithome.com.tw/news/174181（最後瀏覽日：2026/09/10）。

[62] 陳佳鑫、張梓嘉，數發部長指算力中心建在台灣才能有效掌握 AI 主權，公視新聞網 PNN，2026 年 6 月 30 日，https://news.pts.org.tw/article/815472（最後瀏覽日：2026/09/10）。

IBM 企業價值研究院之調查即顯示，75%曾嘗試更換 AI 供應商之高階主管表示，因資料可攜性、模型重新驗證、合規要求與技術鎖定等因素，該過程極為困難，本應屬簡單調整之事項，往往演變為長達數月之營運中斷[63]。就有效法律支配而言，管轄權連結之欠缺使我國法上之調查權、處分權與救濟途徑均難以實現。須補充者，算力在地化本身並非充分條件。如前所述，措施之技術層次須與其所欲控制之對象相對應；算力之所在地屬實體層，而營運控制屬程式碼層，前者之在地化不當然及於後者。算力中心設於境內而其營運、管理與系統維運仍由境外主體掌控者，管轄權連結仍屬形式。有研究即指出，購買商業主權方案者，雖得到在地資料管理、監理合規與在地基礎設施，實則加深對該國（如：美國）供應商之依賴；即令標榜主權之非美國供應商方案，亦鮮少完全在地化[64]。準此，算力建設之法制配套，應同時處理營運主體之在地化、關鍵人員之可接觸性保障，而非僅止於機房座落地點。

（二）政府開放資料之不足

我國人工智慧基本法第 13 條第 1 項課予政府建立資料開放、共享及再利用機制之義務。惟就實際運作而言，我國政府開放資料在授權標示與資料品質兩方面均存在系統性問題。該判斷之基礎，並非單一之統計數字，而係下列三項可查證之制度性事實。

第一，《AI 新十大建設推動方案》就語料平臺之規劃，明載須「建立標準化資料上架機制」，並「優先推動中央二級機關釋出具自然語言特性、語意連貫、結構完整，或具臺灣語言與文化特色之文本資料」。此表述之反面推論，即現行政府資料多不具備語意連貫與結構完整之特性，難以直接供模型訓練之用。第二，要求「請經濟部智慧財產局針對政府機關持有之中文語料是否可授權供 AI 訓練使用，研提相關授權適用說明，提供各機關參考，協助加速資料盤點與合法釋出」[65]。此項規劃之存在，正說明各機關就其所持有資料得否供 AI 訓練使用，普遍欠缺明確之判斷依據。第三，語料庫上線時所集結之逾 2,000 筆資料集、超過 6 億 tokens，係動員逾 200 個機關之成果[66]；以此規模除以參與機關數，平均每機關所釋出者約 10 筆資料集，其單位產出之低落，反映的並非機關怠惰，而是制度上欠缺明確之授權依據與品質標準。

---

[63] IBM Institute for Business Value, *Supra* note 44,at 10.

[64] Shana Lynch, *The AI Sovereignty Paradox: Should Countries Buy, Build, or Lease to Maintain Strategic Control of Their AI?*, STANFORD HAI (July 14, 2026), https://hai.stanford.edu/news/the-ai-sovereignty-paradox-should-countries-buy-build-or-lease-to-maintain-strategic-control-of-their-ai (last visited Sept. 10, 2026).

[65] 行政院，同註 49，頁 87。

[66] 數位發展部，同註 7。

此一失能於法制上之根源有二。其一為政府資訊公開法之立法目的在於保障人民知的權利[67]，其規範對象為個案之申請與提供，並非為大規模機器可讀之資料再利用而設計。其二為現行法未就政府所持有資料之著作權歸屬與授權方式設有一般性規定，各機關因而各自為政。後續所提及之促進資料創新利用發展條例之立法，即應以填補該空白為核心任務。

（三）合規焦慮之寒蟬效應

我國於 2025 年間發生之兩起案件，就國內 AI 資料利用之法律風險提供了極為具體之說明。**其一為臺灣新北地方法院 111 年度智訴字第 8 號刑事判決。**該院判決被告郭○彥犯著作權法第 91 條第 2 項意圖銷售而擅自以重製之方法侵害他人著作財產權罪，處有期徒刑 4 年；被告謝○雅處有期徒刑 2 年；被告七法股份有限公司科罰金新臺幣 150 萬元。法院認定，被告謝○雅撰寫程式，於 107 至 108 年間自動複製並下載法源法律網內容，共 98,068 筆法規沿革、102,520 筆法規內容及 130,936 筆法規附件，作為該公司法學資料庫之資料庫內容，侵害著作人之編輯著作權，並另構成刑法第 359 條無故取得他人電腦電磁紀錄罪。本案得上訴於智慧財產及商業法院[68]，另有民事損害賠償部分併行進行[69]。

該判決之爭點有二。第一，資料庫內容之編輯著作保護範圍。法規沿革與法規內容本身屬不受著作權保護之標的（著作權法第 9 條第 1 項第 1 款），其可受保護者僅為資料之選擇及編排具有創作性之編輯著作（同法第 7 條）；本案之關鍵，在於大規模擷取是否即構成對編輯著作整體之重製。第二，刑事責任之發動。以刑法第 359 條處理網路爬蟲行為，其「無故」要件之解釋，將直接決定公開網站之自動化存取行為之刑事風險邊界。

其二為中央通訊社對臺灣大學生之著作權爭議。據報導[70]，臺灣大學電機工程學系博士生鍾 o 霖彙整名為「fineweb2-zhtw」之繁體中文語料集並公開釋出，其中包含多家臺灣媒體之內容；中央社復於 2025 年 7 月提告，雙方其後達成和解。中央社董事長李永得表示「內容有價」，並稱「如果他有來跟我們申請，我們一定全部免費，重點是，他沒有事先來」；該社媒體實驗室主任宋育泰則指控

---

67 政府資訊公開法第 1 條。

68 臺灣新北地方法院 111 年度智訴字第 8 號刑事判決。判決要旨參見司法院，臺灣新北地方法院 111 年度智訴字第 8 號違反著作權法等案件新聞稿，https://www.judicial.gov.tw/tw/cp-1888-1350821-0ca41-1.html（最後瀏覽日：2026/09/07）。

69 臺灣新北地方法院 112 年度智重附民字第 1 號民事判決

70 謝馥伊，和解案後，未解的台灣主權 AI 語料困局：開發者和內容方能否終結授權衝突？，報導者 The Reporter，2026 年 3 月 22 日，https://www.twreporter.org/a/taiwan-sovereign-ai-zhtw-llm-copyright-conflict（最後瀏覽日：2026/09/07）。

其行為損害該社付費歷史新聞檢索服務之收益。本案雖以和解終結，其對語料建置者所傳遞之訊號並不因此減弱。

上開兩起事件之共同效果，在於其向所有潛在之語料建置者傳遞了明確訊號：於現行法下，未經個別授權而利用他人著作進行 AI 訓練，其法律風險並非僅止於民事賠償，更可能觸及刑事責任。將造成以下後果：

首先為創新之窒礙。學術研究與開源社群所建置之繁體中文語料集，其規模與品質本已不足；在刑事風險下，個別研究者將傾向於避免公開釋出，語料之集體累積因而中斷。中央社案之當事人為博士生，其行為經其自陳係非營利性質，即令如此仍遭提告，該事實對研究社群之嚇阻效果甚為顯著。再者為政策路徑之被動化。數位發展部部長林宜敬曾表示「未來 5 年內不會推相關修法」，而係推動臺灣主權 AI 訓練語料庫，採「避開爭議的深水區，把沒問題的部分開放出來」之策略[71]。此策略在短期內確能累積成果，惟其代價在於，真正具有高訓練價值之語料（新聞、出版品、學術著作）恰恰位於爭議區內；避開爭議之結果，即為語料庫之品質與規模長期受限。

須特別指出者，主權 AI 之推動與著作權之保護，在我國現行制度下被設定為零和關係，該設定本身即為制度設計之失敗。TAIDE 計畫透過事前洽談向內容單位取得授權，支付每家約新臺幣 100 至 200 萬元，占計畫預算不到一成；這數字說明，問題之核心並非授權金之高低，而係交易成本與法律不確定性。若有一項得以同時降低交易成本並提供合理報酬之制度設計，可能為解方之一。

（四）人工智慧基本法之規範缺口

前述三項挑戰，最終均指向同一制度根源，即我國人工智慧基本法未就主權 AI 設有任何規範。李建良教授就該法所提出之結構性課題，亦以「基本法」為我國特有立法模式之規範效力為核心，並指出該法第 1 條後段「本法未規定者，適用其他法律之規定」為行政院版、國科會版及各立法委員提案版本所無，其增訂意旨未見說明[72]。

該法就資料所設之規定僅有二條。第 13 條課予政府建立資料開放、共享及再利用機制之義務，並要求提升資料之品質與數量；第 14 條則規定各目的事業主管機關會商個人資料保護主管機關，於研發及應用過程避免不必要之個人資料蒐集、處理或利用，並促進將個人資料保護納入預設及設計。二者均為綱領性條款，欠缺構成要件、法律效果、完成期限與違反效果。該法第 11 條第 1 項後段規定：「相關法規之解釋與適用，如與其他法規扞格，在符合本法第四條基本原

---

[71] 報導者，同上註。

[72] 李建良，人工智慧基本法的基本課題，台灣法律人，48 期，頁 64，2026 年。

則之前提下，以促進新技術與服務之提供為優先原則。」該解釋準則具有跨法域之效力，其形式上以「符合第 4 條基本原則」為前提，惟第 4 條所定七項原則本身即為綱領性條款，其密度不足以在具體個案中形成有效之限制。其結果為，凡涉及 AI 之法規解釋，均傾向於作出有利於技術與服務提供之解釋。此設計，與同法第 5 條第 1 項所定政府應避免 AI 應用侵害人民生命、身體、自由或財產，破壞社會秩序、國家安全或生態環境之要求，形成緊張關係。

組織法上之問題同樣顯著。該法第 2 條定中央主管機關為國家科學及技術委員會，地方主管機關則為直轄市、縣（市）政府，並就涉及各目的事業主管機關職掌者，明定由各該機關辦理，第 5 條第 2 項將高風險應用之認定交由中央目的事業主管機關會商數位發展部，第 16 條第 1 項將與國際介接之風險分類框架交由數位發展部推動，第 14 條將個人資料事項交由各目的事業主管機關會商個人資料保護主管機關，另於第 6 條在行政院設置國家人工智慧戰略特別委員會。權限之高度分散，使 AI 輔助行政決定所生之損害，在組織法上難以歸屬於特定義務主體。

五、小結

綜上分析，我國主權 AI 之推動，其政策密度已達相當水準，惟法制密度顯著不足，二者之落差構成當前之核心課題。我國於透明性、可替代性與有效法律支配三者均有缺口：公部門算力匱乏、政府開放資料之授權狀態不明，使國家自身所持有之語料難以進入訓練；而兩起 2025 年之著作權案件所可能形成之寒蟬效應，將使民間與學術社群退出語料建置。尤須指出者，上開三項缺口彼此影響。算力不足使模型向境外遷移，境外模型之語料需求無從以本國語料滿足；語料不足使本土模型難以在價值對齊上取得優勢；價值對齊之弱勢又削弱了政府採購本土模型之正當性，進而使本土算力需求無從累積。

肆、比較法觀點：以歐盟為中心

在全球人工智慧技術發展與地緣科技競爭激烈之格局下，「主權 AI」之發展已從產業技術競爭升格為國家安全與憲政防禦之核心命題。各國政府皆意識到，過度依賴境外的大型語言模型與雲端基礎設施，不僅將導致法律管轄權的實質喪失，更可能在關鍵決策、社會認知與資訊流動上遭受境外地緣政治力量滲透與制約。然而，面對該通用技術所帶來之深層衝擊，全球各主要司法轄區因其自身之產業利基、法治傳統與國家治理需求，發展出截然不同的政策模式與法制防禦體系。本章專就歐盟為考察對象，採單一法域深度考察而非多國並列之理由有三。其一，歐盟係迄今唯一同時完成規範立法（人工智慧法）與產業政策部署（人工

智慧工廠、資料聯盟策略）之政策，其雙軌並行之結構，恰可用以檢驗本文所關切之核心問題，即政策文件是否已轉化為具拘束力之義務。其二，歐盟與我國同屬成文法傳統，其以指令、規則與標準契約條款分層配置規範密度之立法技術，較諸判例法法域對我國更具可移植性。其三，歐盟之政策密度為全球之最，而其技術依賴程度仍屬嚴重，此一落差使其兼具制度設計來源與失敗模式樣本之雙重身分；多國並列之泛覽，難以呈現此種張力。

一、歐盟之雙軌回應

就歐盟而言，其回應不循單一法律工具展開，而係同時推動兩條軌道。其一為法律規範，以人工智慧法（EU AI Act）為核心，對模型提供者課予透明與問責義務[73]；其二為產業與基礎設施軌，以通訊、資金工具與契約範本為手段，補強其在算力、資料與模型上之弱勢。然而二者並非各自獨立，而係互為條件：規範軌之義務必須有可供規制之歐洲業者始具實益，產業軌之投資亦須有法律確定性始能吸引私部門參與。

該雙軌結構對我國之比較法意義，在於其揭示了主權 AI 之法制工作並不限於立法。投資與採購、標準與認證、契約範本之發布，同屬治理工具，且其對依賴關係之調整效果，往往較管制規範更為直接。本節即循此思路，先處理產業軌之三份政策文件（EuroStack 倡議、人工智慧大陸行動計畫、資料聯盟策略），再回到規範軌之兩項制度（訓練內容摘要義務、個人資料處理合法性基礎之調整），繼而處理主權 AI 之概念深化，最後檢討歐盟主權論述之內在張力。

二、技術主權之政策藍圖：EuroStack 倡議

2025 年 2 月 13 日，Francesca Bria、Paul Timmers 與 Fausto Gernone 公佈其共同撰寫之 EuroStack 報告[74]。該報告之問題診斷極為直接：歐洲逾八成之數位基礎設施與技術仰賴進口，此一比例所造成者並非個別產業之競爭劣勢，而是系統性之脆弱[75]。

該問題之意義在於其將「依賴」自經濟問題重述為治理問題。當基礎設施之絕大部分由境外供給時，歐盟縱使在規範層面享有立法管轄權，其規範之實效仍

---

[73] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L 1689), https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (last visited Sept. 11, 2026).

[74] Francesca Bria,Paul Timmers &Fausto Gernone, EuroStack – A European Alternative for Digital Sovereignty (Bertelsmann Stiftung 2025), https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/EuroStack__2025_final__1_.pdf (last visited Sept. 11, 2026).

[75] *Id.*at 8.

取決於境外供應商之配合意願。EuroStack 所提出之對策，不是加強管制，而是建立歐洲自身之技術堆疊，使規範對象得以在歐洲法秩序之內存在。因此，EuroStack 報告所揭示之七項原則[76]，各自對應不同之法律領域：

（一）**主權與安全（Sovereignty and security）**：要求歐洲之關鍵數位基礎設施處於歐洲管轄之下，並以安全設計與隱私設計加以保護。其法律意涵為管轄權連結之建立，具體手段包括雲端服務之在地化義務與營運主體之適格要求。本文先前已指出，單純之資料儲存在地化不足以建立實質支配，該原則所稱之「處於歐洲管轄之下」，其內涵應包含管理、營運控制與稽核可及性。

（二）**去專有化與互通性（De-proprietarization and interoperability）**：要求推動開源與聯邦式技術堆疊之整合，並降低對大型科技公司專有解決方案之依賴。其法律意涵橫跨競爭法與採購法：於競爭法上，對應市場支配地位濫用與封鎖效果之規制；於採購法上，對應互通性規格之強制與避免單一供應商。

（三）**永續性（Sustainability）**：要求建立節能且資源具韌性之系統，以符合歐洲環境與氣候目標。其法律意涵在於使算力建設與碳中和義務相互銜接，該連結於我國尚未見於法制討論，惟以資料中心之耗電規模而言，其遲早將成為許可與環評程序上之討論重點。

（四）**資料作為公共財（Data as common good）**：要求將資料視為共享資源，於釋放創新之同時維護社會利益與基本權利。此一原則就我國《促進資料創新利用發展條例》草案之立法定位具有直接啟示：政府所持有之資料，其開放之正當性基礎並非行政裁量，而係其本即以公共資源產生。

（五）**去中心化之主權基礎設施（Decentralized sovereign infrastructure）**：要求結合邊緣運算與集中式系統，以提升效率與資料主權。其法律意涵在於提醒立法者，主權之實現未必以集中化為必要；過度集中之基礎設施本身即構成失效之風險。

（六）**包容性治理（Inclusive governance）**：要求確保法規之協調一致、問責機制之建立，以及短期韌性與長期自主之間的平衡。權限分散所導致之問責稀釋，正是治理包容性之反面。

（七）**強健民主（Strong democracy）**：要求數位技術不僅不造成危害，更應從根本上強化民主社會。該原則之規範地位最高，亦最抽象；其於具體個案中之作用，應為前述六項原則之解釋準則，而非獨立之請求權基礎。

---

[76] Francesca Bria、Paul Timmers &Fausto Gernone, *Supra* note74,at 25-26.

七項原則之整體結構顯示，歐盟之技術主權論述並未將主權化約為所有權。原則一所要求者為管轄，原則二所要求者為可替代，原則四與原則七所要求者為公共利益與民主。以本文三項判準對照，原則一相當於有效法律支配，原則二相當於可替代性，二者之對應堪稱緊密。惟七項原則中並無與「透明性」相對應者，此一缺漏並非偶然：EuroStack 報告之性質為產業政策藍圖，其所關切者為歐洲技術堆疊之建置，而依賴關係之揭露義務屬規範端之課題，於歐盟法上係由人工智慧法所承擔。準此，本文三項判準與歐盟制度之對應關係，須跨越產業端與規範端二者方能完整。

三、人工智慧大陸行動計畫

2025 年 4 月 9 日，執委會發布人工智慧大陸行動計畫（The AI Continent Action Plan）[77]，設定五項行動領域：建立跨歐洲之大規模資料與運算基礎設施、擴大高品質資料之取得、促進人工智慧於戰略部門之採用、強化人才與技能，以及監理之簡化與遵循。

就算力而言，該計畫規劃設置至少十三座人工智慧工廠（AI Factories）與至多五座人工智慧超級工廠（AI Gigafactories），並透過 InvestAI 倡議動員約 200 億歐元之投資[78]。就法制而言，最值得注意者為《雲端與人工智慧發展法》（Cloud and AI Development Act）之立法預告，其目標為於五至七年內使歐盟境內資料中心容量增至三倍[79]。此外，人工智慧法服務櫃臺（AI Act Service Desk）已於 2025 年 7 月於歐洲人工智慧辦公室內設立，其功能為降低業者之遵循成本[80]。

在語言模型層面，歐洲數位基礎設施聯合體下之語言科技聯盟（ALT-EDIC）以建立歐洲各官方及區域語言之模型基礎設施為目標[81]，並參與 OpenEuroLLM 計畫[82]；波蘭之 PLLuM 專案則於 2025 年 2 月發布，為以本國語料訓練之大型語言模型[83]。此經驗對我國具有直接可比性：波蘭語與繁體中文同屬全球語料庫中

---

[77] Communication from the Commission, The AI Continent Action Plan, COM (2025) 165 final (Apr. 9, 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0165 (last visited Sept. 11, 2026).

[78] European Commission, The AI Continent Action Plan,at 8.

[79] European Commission, Cloud and AI Development Act, Shaping Europe's Digital Future (last updated June 3, 2026), https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act (last visited Sept. 11, 2026).

[80] European Commission, *Supra* note78, at 21-23.

[81] European Commission, *Supra* note78, at 12.

[82] OpenEuroLLM Consortium, *OpenEuroLLM: A Series of Foundation Models for Transparent AI in Europe*, https://openeurollm.eu/ (last visited Sept. 11, 2026).

[83] ALT-EDIC, *Poland Launches a Polish Large Language Model (PLLuM)*, https://www.alt-edic.eu/news/poland-launches-a-polish-large-language-model-pllum/(last visited Sept. 11, 2026).

之相對少數，其以國家計畫結合學研機構建立本國語言模型之路徑，與我國TAIDE計畫之取向相近。

該計畫之意義，不在於其投資金額，而在於其所揭示之治理形態。歐盟並未以管制手段要求業者使用歐洲基礎設施，而係以公共投資改變市場結構，使歐洲基礎設施成為業者之可行選項，該觀察對我國之意義有二。其一，《AI新十大建設推動方案》之算力建設與該取向相同，惟我國欠缺對應之法律基礎，其存續繫於年度預算。其二，公共投資雖屬給付行政，惟其分配決定仍涉及對事業之差別待遇，於補助、委託與投資之個案中，仍應受平等原則與正當程序之拘束，其密度是否足夠，容有討論餘地。

四、資料聯盟策略

2025年11月19日，歐盟執委會發布歐洲資料聯盟策略（Data Union Strategy）[84]，提出三項優先行動[85]。

第一為擴大人工智慧之資料取得（Scaling up access to data for AI）：其核心工具為資料實驗室（Data Labs），該策略將其界定為提供安全環境、工具與專家支援之專門設施，用於資料之匯集、整理、假名化與匿名化；其運作原則為資料不直接移轉，而以同態加密與安全多方計算等隱私強化技術達成分析目的。歐盟並規劃自2026年起投入約1億歐元推動優先部門之資料空間，至2026年底將歐洲共同資料空間擴及健康、移動、能源、公共行政、環境、法律司法與國防等領域；另依開放資料指令，將逾三千萬件歐洲文化機構之數位化成果提供人工智慧開發使用[86]。

第二為資料規則之簡化（Streamlining data rules）：其手段為將契約標準化，包括資料取得與利用之非拘束性契約條款，以及雲端運算之定型化契約；後者涵蓋轉換與退出、終止條款，以及切換期間之安全與業務持續性三個面向。數位綜合法案（Digital Omnibus Regulation Proposal）[87]並將既有之若干規則整合至相關

；ALT-EDIC, *ALT-EDIC Will Contribute to Open-Source LLM Development Under the OpenEuroLLM Project*, https://www.alt-edic.eu/news/alt-edic-will-contribute-to-the-development-of-open-source-large-language-models-under-the-openeurollm-project/(last visited Sept. 11, 2026).

[84] Communication from the Commission, Data Union Strategy – Unlocking Data for AI, COM(2025) 835 final (Nov. 19, 2025), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2025:835:FIN (last visited Sept. 11, 2026).

[85] European Commission, European Data Union Strategy, Shaping Europe's Digital Future (last updated May 18, 2026), https://digital-strategy.ec.europa.eu/en/policies/data-union (last visited Sept. 11, 2026).

[86] *Id.*

[87] Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU)

法規中。

第三為歐盟資料主權之維護（Safeguarding the EU's data sovereignty）：該策略明示，資料主權意指歐盟必須保留對資料如何被取用、利用與保護之控制權；其政策取向為開放與力量之結合，亦即對可信賴夥伴保持跨境資料流通之開放，惟須以公平、安全並符合歐盟價值與利益為條件，並將發布評估歐盟資料於境外是否受公平對待之準則[88]。

就本文而言，第二項行動最具制度參考價值。前述資料實驗室與資料空間所處理者為「資料從何而來」，而標準契約條款所處理者為「依賴如何退出」。須一併指出者，歐盟就資料主權所採之表述值得我國參照，該策略並未主張資料不得跨境，而係主張歐盟應保留對取用、利用與保護方式之控制權，並以夥伴是否可信賴、條件是否公平作為開放之前提。此一立場與本文第貳章所述可控的相互依賴之框架一致：管轄之維持不以封閉為手段。

五、數位綜合法案對一般資料保護規則（GDPR）之修正

2025 年 11 月 19 日歐盟執委會所發布之數位綜合法案，明定人工智慧系統及其底層模型之開發與運作，於訓練、測試與驗證各階段處理個人資料時，得依一般資料保護規則第 6 條第 1 項第 f 款所定之正當利益為之[89]；控管者於權衡時，應考量其所追求之利益對資料主體與社會整體是否有益，並採取適當保障措施。草案並就特殊類別個人資料設有豁免。其理由構成為：大規模資料蒐集過程中，特殊類別個人資料縱非處理目的所必要，仍可能殘留於訓練、測試或驗證資料集，甚或保留於模型之中；考量控管者識別及移除該等資料之能力有其極限，為免過度阻礙人工智慧之開發與運作，應允許此類處理[90]。

該法同時規定，個人資料之處理係基於控管者開發及運作人工智慧系統或模型之必要利益者，得依正當利益為之，但其他歐盟或會員國法律明確要求同意者，以及資料主體之利益或基本權利與自由凌駕於該等利益者，不在此限；該處理並須採取適當之組織性、技術性措施與保障措施，包括資料來源篩選階段之最小化、訓練與測試過程之規範落實、防止殘留資料遭揭露、對資料主體之透明度強化，

2022/868 and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final (Nov. 19, 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837 (last visited Sept. 11, 2026).

[88] European Commission, *Supra* note85.

[89] Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 and Directive (EU) 2019/1024 (Digital Omnibus), recital 32.

[90] *Id.* recital 33.

以及賦予資料主體無條件反對處理之權利。

六、歐盟主權 AI 之其他論述

雖然歐盟之做法已相對成熟，然有認為不應將歐盟模式逕予理想化。Mügge 對歐盟執委會自 2018 年以來七份核心人工智慧戰略文件進行文本分析，並延伸考察歐盟人工智慧法立法三方協商過程，提出三方面之疑問：主權 AI 究竟是法域間之對抗（管轄主權），還是公民相對於強大科技產業之賦權（公民主權）？主權 AI 旨在提升歐洲在全球競賽中之地位，抑或作為擺脫競爭束縛之手段？主權 AI 係以「歐洲優先」為框架，抑或同樣顧及歐盟境外人民之利益[91]？

其分析結果顯示，歐盟人工智慧主權論述呈現強烈之管轄主權導向、親競爭導向與歐洲中心導向：執委會文件持續強調「激烈的全球競爭」與推動「歐洲製造的人工智慧」[92]，而布魯塞爾理論中常見之對大型科技公司之疑慮，在人工智慧戰略文件中幾近闕如[93]；文件反覆強調「歐洲產業不能錯過這班列車」，監理設計上應「僅在嚴格必要時介入，並以將經濟營運者負擔降至最低之方式」進行，未見任何關於延緩人工智慧擴散速度或補償勞動市場輸家之政策考量[94]。

未來社會智庫之報告則自另一角度提出批評。該報告以「小心技客（Geeks）的禮物」為題[95]，指出歐盟主權面臨之最重大風險，未必透過強制施加，而可能以「禮物」之姿降臨，透過基礎設施投資、模型存取協議或技術夥伴關係，以短期利益換取結構性削弱主權之長期依賴。該報告對四份主要執委會通訊文件中所公布之 92 項倡議進行系統性分析，發現該政策組合雖展現真實之戰略意圖，惟各倡議往往彼此脫節，欠缺針對主權前沿人工智慧堆疊之整全願景，且聚焦短期經濟利益之傾向過於狹隘[96]；並識別出歐盟主權辯論中反覆出現之五項目標，即經濟競爭力、韌性與備災、安全與國防、歐洲價值與認同，以及對外關係與國際觀感。該報告並指出，歐盟自結構性依賴之位置進入此轉型，前沿人工智慧模型幾乎完全來自美國或中國，美國之人工智慧超級電腦運算容量約為歐盟之 16 倍，全球超大規模資料中心容量僅 15%位於歐盟境內[97]。

---

[91] Daniel Mügge, *Supra* note29,at 2201.

[92] Daniel Mügge, *Supra* note29,at 2202.

[93] Daniel Mügge, *Supra* note29,at 2212.

[94] Daniel Mügge, *Supra* note29,at 2213.

[95] 標題原文為：Beware of Geeks Bearing Gifts:Building True EU Frontier AI Sovereignty，其源自希臘神話「特洛伊木馬」，原指提防暗藏陰謀的禮物。本處將「希臘人」諧音為「極客(Geeks)」，藉此警告：要小心科技人員提供的免費產品、程式或技術協助，其背後可能潛藏漏洞或別有用心的企圖。

[96] Nick Moës et al., *Supra* note 30at 2.

[97] Nick Moës et al., *Supra* note 30.

將此二項批評與前述 EuroStack 報告所載逾八成基礎設施仰賴進口之數據併觀，可得一項對我國具警示意義之結論：歐盟之政策密度為全球之最，其技術依賴程度卻仍屬嚴重。政策文件之數量與制度實效之間，並無必然關聯；真正決定主權程度者，是這些文件是否轉化為具拘束力之義務與可執行之條款。

七、歐盟路徑之歸納

歐盟模式之結構特徵，在於其對模型課予嚴格之透明義務，同時放寬資料處理之合法性基礎，二者形成交換關係。如此「以透明換取合法性」之立法結構，對我國最具參考價值，理由在於其同時處理了「資料從何而來」與「權利人如何知悉」兩個問題，而我國現行法對二者均無回答。

除該結構外，本章另指出三項可資參考之制度設計。其一為 EuroStack 七項原則所提供之分析架構，其中主權與安全、去專有化與互通性二項，與本文所提有效法律支配及可替代性判斷標準契合。其二為人工智慧大陸行動計畫所展示之治理形態，亦即以公共投資改變市場結構，而非以管制強制業者選擇；此一形態與我國 AI 新十大建設推動方案相近，惟我國欠缺對應之法律基礎。歐盟經驗同時提供兩項警示。首先，主權論述若僅以產業競爭力為內涵，將無法承擔憲法上之正當化功能，Mügge 所指出之「公民主權」面向必須被明確納入。再者，以基礎設施投資與模型存取協議之形式出現之依賴，其風險不因其外觀為「合作」而降低。

伍、我國主權 AI 法制建構之初步構想

本章承繼上一章節，將以歐盟為參照對象。如前所述，歐盟於本文中具有制度來源與失敗樣本之雙重身分。本章所提之建議，因而均須通過同一項檢驗：該設計是否已轉化為具拘束力之義務或可執行之手段？若否，則其與我國現行之政策文件並無二致。歐盟制度之內容不於本章重述，悉依第肆章各該節；我國現況亦同，悉依第參章。本章之篇幅集中於移植條件之檢驗與修法方向之提出。

一、三項移植原則

第一，規範端與產業端須同步推進。歐盟雙軌並行之結構及其互為條件之關係，已詳第肆章。我國現況恰為二者脫節：產業端已有 AI 新十大建設推動方案之算力與語料規劃，規範端則僅有綱領性之人工智慧基本法，二者之間欠缺制度性連結。其表現至為具體：推動方案就語料平臺、授權條款與釋出動能設有四項規劃，而人工智慧基本法第 13 條僅課予政府「建立資料開放、共享及再利用

機制」之綱領性義務，方案所規劃之各項作為，於法律上均無對應之授權基礎或義務主體。

第二，資料側之放寬須以模型側之透明為對價。歐盟人工智慧法第 53 條第 1 項第 d 款課予訓練內容摘要義務[98]，同時於數位綜合法案放寬個人資料處理之合法性基礎，二者形成交換結構。該結構之規範功能在於：透明義務使權利人得以判斷其權利是否受影響，從而使放寬後之利益失衡得以透過個別行使權利加以矯正。我國若僅移植資料側之放寬而未同時建立透明義務，其結果將為保護水準之下降。

第三，可替代性應以契約標準化實現，而非以在地化強制實現。歐盟資料聯盟策略所發布之雲端運算標準契約條款，其所標準化之事項已詳第肆章。此手段之干預強度顯著低於資料或算力之在地化要求，於比例原則之審查上較易通過，而其對依賴關係之調整效果未必較小。我國現行政府採購法就雲端與人工智慧服務並無對應之定型化要求，各機關議約能力參差，風險因而由個別機關各自承擔。

三項原則所對應之規範形式各異：第一項須以法律創設義務與授權，第二項須以法律增訂例外並配置對價義務，第三項則得以法規命令或採購契約範本為之。規範形式之選擇並非技術問題，而係法律保留密度之判斷，其判準已於第貳章提出。以下四節即依此序列說明。

二、資料供給面：促進資料創新利用發展條例之立法定位

歐盟就資料供給所採之手段：資料實驗室、共同歐洲資料空間之擴大，以及依開放資料指令釋出既有文化資產，已詳第肆章。三者之共同特徵，在於國家並非單純「開放」其所持有之資料，而係主動整備並提供使資料得以被使用之條件。我國欲建立同等之供給能力，前提即在於將該義務明文化。我國現況與之相較，差距不在規模而在法律形式，其表現有四：語料庫之依據僅為行政計畫而非法律，存續繫於年度預算；各機關並無盤點與釋出之義務，是否釋出實質上屬裁量事項；承辦人員欠缺責任限制，釋出之公共利益歸於社會而風險歸於個人，理性之機關因而選擇不釋出或僅釋出低價值資料；機敏資料欠缺受控利用之途徑，致高訓練價值之醫療、司法與教育資料一律排除於外。促進資料創新利用發展條例草案業於 2025 年 6 月預告，目前已排入院會交付審查中[99]；本文以下四項方向，即係就

---

[98] Regulation (EU) 2024/1689, Article 53(1)(d)

[99] 立法委員賴惠員等 18 人擬具，「促進資料創新利用發展條例草案」，立法院議案關係文書，院總第 2110 號，委員提案第 20307 號，民國 115 年 4 月 10 日印發，https://ppg.ly.gov.tw/ppg/bills/202110203070000/details（最後瀏覽日：2026/09/14）。

該條例應承擔之立法任務所為之主張。

第一，明定政府所持有資料之著作權歸屬與標準授權。宜設一般性規定，明定政府機關於執行職務所作成之資料，除法律另有規定外，得依標準授權條款供再利用，並將臺灣主權 AI 訓練語料授權條款納為法定授權態樣之一。該條款之授權撤回不溯及既往原則與簡化標示義務已具進步性，惟效力現僅及於契約當事人，提升為法定態樣後方生對世效力。**第二，建立資料品質之最低標準與課責機制。**宜明定資料上架之最低品質要求，包括機器可讀格式、詮釋資料完整性與更新頻率，並納入機關考核。就本文之判斷標準而言，品質與互通性標準即可替代性之技術前提：格式不一致者，其更換成本趨於無限。**第三，設置受控利用之安全運算環境。**宜授權主管機關就涉及個人資料或營業秘密之高價值資料，建置得供研究者於不取得資料本體之前提下進行分析之環境，並明定存取審核程序與稽核義務，使敏感資料自「一律排除」轉為「條件利用」。**第四，就承辦人員設置責任限制。**宜明定機關依本條例所定程序釋出資料者，就釋出行為所生之著作權或個人資料爭議，於已踐行法定程序之範圍內減輕或免除其責任。此設計對扭轉機關之防禦心態具直接效果，相關成本亦低。

三、資料利用面：著作權法之相關問題

歐盟於該領域之設計，其重點在於例外與義務之配對：數位單一市場著作權指令第 4 條建立文字與資料探勘之例外並容許權利人保留，人工智慧法第 53 條第 1 項第 d 款則課予通用模型提供者公開訓練內容充分詳細摘要之義務。二者合併觀之，利用之自由使模型開發成為可能，透明之義務使權利之行使成為可能，保留之機制使權利人得以退出；三者缺一即失衡，僅有例外而無透明，權利人無從舉證；僅有透明而無例外，開發者仍須逐一授權；僅有例外與透明而無保留，權利人失去選擇。惟保留機制本身尚不足以解決權利人之利益問題：保留之行使以權利人知悉、具備技術能力並願意承擔退出成本為前提，未行使者其著作即得被無償利用。準此，例外與保留之二元結構應輔以報酬機制，使未退出者亦得分享利益。

我國現行著作權法未就文字與資料探勘設有例外，人工智慧訓練是否構成合理使用須依同法第 65 條逐案判斷。此一不確定性之代價已由 2025 年之兩起事件具體呈現，其後果為語料建置中斷、機關防禦心態強化與政策路徑被動化；問題之核心非授權金之高低，而係交易成本與法律不確定性。本文主張於著作權法增訂例外，並以負責任 AI 三大支柱為其適用要件，即透明性揭露義務、合理報酬與機器可讀之退出選擇，以及輸出端之過濾責任與責任分擔。其修法方向有以下。

（一）例外之客體與行為應予明定：客體宜限於已公開發表之著作，行為涵蓋重製、改作及其他利用態樣，並以「於必要範圍內」為限。所謂資訊分析，宜界定為自多數著作或大量資訊中抽出其所構成之語言、聲音、影像或其他要素之相關資訊，並為比較、分類、統計或其他解析；其功能在於區隔「分析」與「再現」，使例外不及於以重現原著作表達為目的之利用。

（二）取得之合法性應與分析之自由分離：例外之適用，宜以利用人係以合法方式取得該著作或取得其接觸權源者為限。該要件為整組設計之界線所在，其意義詳見本節末段。

（三）應設機器可讀之保留機制：另宜設一般性衡平條款，就依著作之種類、用途及利用態樣有害及著作財產權人利益之虞者，排除例外之適用。保留之方式與技術標準宜授權主管機關公告，以免因標準不一而使保留形同虛設。

（四）營利性之公眾模型應負三項義務，並以之為主張例外之要件：以營利為目的、以例外所允許之利用結果訓練並供公眾使用之模型，其提供者宜負：公開足以使著作財產權人判斷其著作是否經利用之訓練內容摘要、就未經保留之著作透過集體管理團體或其他適當方式支付合理報酬，以及就模型輸出採行合理措施以避免重現受保護著作之表達；未履行者不得主張例外。此一「義務作為要件」之立法技術，使三項支柱毋須另設罰則即具強制力。

（五）義務密度宜依規模、用途與影響分級：摘要之項目與詳細程度宜授權主管機關分級定之，非以營利為目的或供學術研究之用者應得簡化或免除。合理報酬之計算基準與分配方式，則宜由主管機關會商集體管理團體及產業團體定之，以保留隨技術與市場變動調整之空間。

（六）輸出端之責任應與控制力相對應：模型提供者未採行過濾措施致輸出侵害他人著作財產權者，宜與該輸出之利用人負連帶責任；惟利用人明知或可得而知該輸出構成侵害而仍予利用者，模型提供者應得向其求償。

上開六項之分工，係以第一至第三項處理「利用之自由」，以第四至第六項處理「自由之代價」。其理由有三。第一，使非營利研究與商業開發受差別待遇：前述語料集釋出爭議中，行為人為在學研究生而自陳非營利性質，依上開方向，該類行為僅須符合例外本身之要件即得主張，無須負揭露與報酬義務。第二，使著作財產權人取得三重選擇，保留而完全退出、不保留而透過集體管理取得報酬、於著作遭重現時依一般規定請求救濟。相較於現行「全有或全無」之對抗結構，協商因而成為可能。第三，使責任與控制力相對應：過濾機制之設置能力集中於模型提供者，故以其為第一線責任主體，利用人之惡意利用則以但書之求償設計處理。須強調者，上開方向並未使前述新北地院判決所處理之行為合法化。第二

項取得合法性之要件，其功能正在於將「分析之自由」與「取得之合法性」分離；未經授權而以自動化程式大量擷取他人資料庫者，其違法性不因資訊分析例外之增訂而受影響。此界線應於立法理由中明確揭示，以避免制度誤讀。

四、基礎設施：AI 新十大建設推動方案之法制化

歐盟人工智慧大陸行動計畫所展示之治理形態，係以公共投資改變市場結構而非以管制強制業者選擇，其具體說明已詳第肆章。就政府自身之使用，Apply AI 策略另提三項行動：建立專供公共行政（包括司法機關）使用之開源可用之工具箱、加速生成式人工智慧解決方案於公共行政之採用，以及修訂歐洲互通性框架以納入「人工智慧優先」政策之指引。須特別指出者，歐盟所提供者為互通性之標準與工具，而非統一之運行環境，各會員國仍分別採購並自行部署；其成因為二十七個會員國之協調成本過高，統一平臺於政治上不可行。我國之處境則不同：法域單一、行政一體，中央機關間之協調成本遠低於歐盟會員國之間，共通平臺於中央層級之可行性因而較高；惟人工智慧基本法第 2 條既設有地方主管機關，共通平臺之設計仍須處理地方機關之納入方式，不得逕以中央一體視之。準此，本節所提之建議並非移植，而係在歐盟所確立之方向上，利用我國組織結構之優勢，採行歐盟力有未逮之集中化設計。

我國現況之不足有四。**其一，算力建設欠缺法律基礎：**推動方案第七項設有累計能耗與算力建置之具體目標，惟其法律形式為行政計畫，2025 年預算遭刪減即影響擴充進度。**其二，公私協力欠缺法律形式：**方案就「推動公私協力算力資源聯盟」設有規劃，惟其組織形態、政府出資上限與表決權配置、民間出資者之退場與買回均未見設計；我國雖有促進民間參與公共建設法、行政法人法等形式，惟該等制度以公共建設之興建營運或特定行政任務之執行為原型，就算力設施此種技術迭代迅速、資產汰換週期短且須持續採購境外硬體之標的，其適用之扞格尚未見討論。**其三，政府使用人工智慧欠缺共通平臺與依賴治理義務：**各機關之依據僅為行政院所發布之參考指引，其性質為行政規則，分別採購之結果為管轄分散、治理不一與供應商鎖定。**其四，算力在地化並非充分條件：**如第貳章所述，措施之技術層次須與其所欲控制之對象相對應，算力中心設於境內而營運、管理與系統維運仍由境外主體掌控者，管轄權連結仍屬形式。據此，本文提出三項方向：

（一）算力與語料設施應取得法定地位：其效果有二，預算編列以法律上之作為義務為基礎，行政機關於預算遭刪減時得據以請求，立法機關之刪減亦須面對該法定義務未能履行之責任；設施之治理結構、使用規則與資安標準並得以法規命

令定之，而非僅以內部作業規範處理。

（二）公私協力應先行處理法律設計：宜於法律中明定特殊目的公司之設立依據、政府持股上限、買回條款之限制與退場機制，並就營運能力設定資格要件。此等細節看似技術性，實則決定民間是否參與：欠缺退場機制之投資，其風險無從計價，理性之投資人將選擇不參與，計畫因而停留於紙面。

（三）建立政府共通人工智慧平臺：其要點包括：由數位發展部建置並維運，運行於政府自有雲端環境；模型層採複數模型並行以確保選擇權；各機關就涉及機敏資料或輔助作成行政決定之應用，原則上應使用該平臺；平臺應保留完整之使用紀錄與資料來源標記，以供事後審查。就地方機關，宜明定其得選擇使用該平臺或自行建置而符合同等之治理標準。

五、管轄與問責：人工智慧基本法之修正

本文就人工智慧基本法所提之修正方向有五項，以下分述：

（一）國家訓練資料與提供機制之明文化（宜增訂於第 13 條之後）：其要點有五。其一，由中央主管機關會商數位發展部及各中央目的事業主管機關建置並管理該機制；國家所提供者非僅資料本身，而係使資料得以被使用之安全環境、工具與專家支援。其二，課予中央二級機關定期盤點並上架之義務，盤點標的宜以「具自然語言特性、語意連貫、結構完整，或具我國語言與文化特色」為準，其標準與期限授權主管機關定之。其三，明定政府為充實機制內容，得自行或委託民間製作、蒐集訓練資料，並得編列預算。其四，授權訂定標準授權條款，並就已踐行該條款所定程序之機關，就其上架行為所生之著作權爭議減輕或免除責任。其五，得對利用者收取費用，學術研究或非營利用途應予減免。

（二）境外提供者之國內代理人義務（宜增訂於第 16 條之後）：其要點有四。其一，於我國領域外提供人工智慧產品或服務者，符合一定門檻時，應指定於我國領域內有住所或營業所之代理人並向主管機關報備。其二，門檻宜採「影響、資料、規模」三重設計，即產出對我國人民權益有重大影響、模型訓練利用我國領域內資料達一定規模，或於我國之使用者人數或營業額達一定基準，三者有一即足。其三，代理人之職務為代理提供者履行通知、報告、說明及配合調查義務，並為送達之受領人。其四，違反者宜設限期命其改正之程序，屆期未改正者始得限制或禁止其產品或服務之提供。另宜參考歐盟人工智慧法第 54 條第 6 項之立法例，就權重公開且授權允許取用、修改與散布之開源模型設例外，但具系統性風險者不在此限。

（三）政府使用人工智慧之依賴治理義務（宜增訂於第 19 條之後）：其要點有

四。其一，政府機關使用人工智慧執行業務或提供服務者，應作成依賴關係說明書並定期更新；記載所用模型與雲端服務之提供者名稱、所屬法域及契約期間；機關得取得之模型資訊範圍；供應中斷、條款變更或效能劣化之因應安排；更換提供者所需之期間、成本與技術障礙。其二，說明書原則上應公開，涉及國家安全、營業秘密或資安者得就該部分不予公開並敘明理由。其三，人工智慧相關採購應於招標文件載明轉換與退出條款、資料及模型產出之返還格式、切換期間之最低服務水準。其四，涉及機敏資料或輔助作成行政決定之應用，應優先評估採用得取得模型權重之模型，採用其他模型者應敘明理由。

（四）促進優先原則之限縮（第 11 條第 1 項）：宜增設但書，將涉及人民自由權利之限制或剝奪，以及涉及國家安全、公共安全維護之事項，排除於促進優先原則之適用範圍外。現行條文以第 4 條七項原則為唯一制約，而該七項原則本身即為綱領性條款，其密度不足以在個案中形成有效限制；以明文排除特定事項，較諸期待綱領性原則發揮作用為可靠。

（五）檢視義務之實質化（第 18 條）：宜增設三項程序要求，各中央目的事業主管機關應於一定期限內完成主管法規與行政措施之檢討並作成清單，載明法規名稱、條次、不符情形與擬採處理方式，送中央主管機關彙整後公開；中央主管機關應定期彙整辦理進度並向立法院提出報告；逾期未完成者，該管機關於適用該法規時應就其結果是否符合第 4 條所定原則附具理由。三者之共同功能，在於使檢視義務自「應為之事」轉為「可被檢驗之事」。該條所定二年期限將於 2028 年 1 月 14 日屆至，本方向之時程因而最為緊迫。

六、小結

本章所提之制度設計，得依其規範功能歸為三層。**第一層為實體法層**，即著作權法之資訊分析例外。其功能在於解決私人參與語料建置之法律風險。**第二層為組織與程序層**，即人工智慧基本法所應增訂之訓練資料綜合提供系統、國內代理人義務與依賴治理義務。其功能在於使國家取得資料供給能力、對境外提供者建立管轄連結，並使行政機關之技術依賴受制度控制。**第三層為配套層**，即促進資料創新利用發展條例之立法與 AI 新十大建設推動方案之法制化。其功能在於處理政府所持有資料之流通與算力設施之法律地位。

三層之間並非單純之先後，而係相互為條件。第一層若未先行，則第二層之整備與提供機制仍將受限於「避開爭議」之策略，其內容侷限於低價值語料；第二層若未建立，則第一層所釋放之利用自由將無對應之供給來源；第三層之配套若付之闕如，前二層所課予機關之義務即無組織與財政上之承接基礎。準此，三

者宜同步推動，所謂先後，係指論理上之條件關係，而非立法時程上之次序。就優先順序而言，本文認為著作權法之修正最為迫切。理由有二：其為唯一已產生刑事風險之領域，寒蟬效應正在發生，而其餘缺口之後果多為機會成本；且其修法所需之立法資源最小，只須增訂例外規定並於立法理由中劃定其與取得合法性之界線，即得解除當前之主要不確定性，無須建置新機關或編列新預算。

最後須指出者，本章之建議均以可控的相互依賴為框架，其目標並非切斷對外依賴，而係使依賴關係透明、可替代並受本國法有效支配。其所憑藉之手段有三：規範形式之審慎選擇，使各項措施所受之法律保留密度與其干預強度相稱；管轄權連結之建立，使境外提供者進入本國法之規範射程；以及契約之標準化，使可替代性自個別機關之議約能力轉為制度性之要求。三者之共同特徵，在於均不以巨額投資為前提。就我國之財政規模與立法資源而言，此類低成本而高槓桿之制度設計，其可行性遠高於算力之全面自建。

陸、 結論

本文之問題意識，起於 2025 年 DeepSeek 事件與 2023 年中央研究院模型事件：前者呈現管轄之外部化，後者呈現價值流失之風險，二者共同之結構成因，則為我國語料在全球訓練資料庫中之弱勢地位。模型偏差之成因既在於語料結構而非傳播行為，因應之道即應自對輸出之事後管制，前移至對訓練資料之事前供給。本文之論證即循此一視角展開。就概念層次，本文將主權 AI 界定為國家就技術堆疊各層依賴關係所建立之制度安排，並提出透明性、可替代性與有效法律支配三項階層性判準。就策略選擇，全技術堆疊主權於我國並不可行，可行者為可控的相互依賴，亦即以法律機制設定依賴之條件，而非切斷對外連結；ASML 之不可或缺性雖較全技術堆疊更具可移植性（對比於我國之台積電），惟仍以我國具備可供他國依循之法制內容為條件。

以上開判準檢視現況，所見者為政策密度與法制密度之落差。算力匱乏使模型向境外遷移，實質管轄因而減損；開放資料之授權狀態不明，使國家自身持有之語料難以進入訓練；2025 年兩起著作權事件所引發之寒蟬效應，可能使民間與學術社群退出語料建置；人工智慧基本法之資料條款則僅具綱領性質。上開缺口彼此增強，形成算力、語料與價值對齊相互拖累之循環。比較法上，歐盟最具參考價值者為「以透明換取合法性」之立法結構，亦即於放寬資料側利用之同時，就模型側課予訓練內容之揭露義務。惟歐盟政策密度為全球之最，技術依賴程度仍屬嚴重；決定主權程度者，非政策文件之數量，而係其是否轉化為具拘束力之義務。

據此，本文所提之制度建構分為三層：以著作權法之資訊分析例外消除私人參與語料建置之法律風險，以人工智慧基本法之修正建立資料供給能力、對境外

提供者之管轄連結及行政機關之依賴治理義務，並以促進資料創新利用發展條例與算力設施之法制化為配套。三層互為條件，宜同步推動，而以著作權法之修正最為急迫。末須強調者有二。其一，主權論述具有雙面性，同一套語彙既得回復民主價值，亦得為監控與審查提供正當化基礎，制度設計因而必須考量控制機制。其二，本文所處理者限於供給側，適用側之課題及鄰國日本、韓國之做法，均有待後續研究補充。

參考文獻

壹、中文文獻

一、專書及專書論文

1. 李建良，數位社會的智慧治理法制：思維框架的建構，收於：數位社會的智慧治理，頁 1-92，2026 年。

二、期刊論文

1. 李建良，人工智慧基本法的基本課題，台灣法律人，48 期，頁 63-91，2026 年。
2. 林佳瑩，從國際 AI 發展趨勢探析我國主權 AI 推展策略，經濟研究，26 期，頁 1-26，2026 年。
3. 陳譽文，從 DeepSeek 事件觀察主權 AI 治理趨勢與我國法制回應，當代法律，41 期，頁 68-78，2025 年。
4. 廖明輝、洪尉淳，各國發展主權 AI 策略對我國的啟示，經濟前瞻，215 期，頁 84-89，2024 年。

三、官方文件及政策報告

1. 中央研究院，中研院資訊所對 CKIP-Llama-2-7b 之回應，中央研究院網站，2023 年 10 月 9 日，https://www.sinica.edu.tw/news_content/70/1850
2. 司法院，臺灣新北地方法院 111 年度智訴字第 8 號違反著作權法等案件新聞稿，司法院網站，https://www.judicial.gov.tw/tw/cp-1888-1350821-0ca41-1.html
3. 立法委員賴惠員等 18 人擬具，促進資料創新利用發展條例草案，立法院議案關係文書，院總第 2110 號、委員提案第 20307 號，2026 年 4 月 10 日印發，https://ppg.ly.gov.tw/ppg/bills/202110203070000/details
4. 行政院，AI 新十大建設推動方案（114 年至 117 年）（核定本），2026 年 1 月 28 日核定，國家發展委員會網站，https://www.ndc.gov.tw/Content_List.aspx?n=EF80A54FA6A63200
5. 行政院（國家科學及技術委員會提供資料），完善臺灣 AI 基礎建設——打造可信任 AI 對話引擎 TAIDE，行政院全球資訊網「重要政策」，2024 年 6 月 11 日，https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/582206fe-26fc-4184-b911-aa6e4569ff3e
6. 國家科學及技術委員會，TAIDE——推動臺灣可信任生成式 AI 發展：計畫重點研發與活動歷程，TAIDE 官方網站，https://taide.stpi.niar.org.tw/
7. 楊蕙如，主權 AI 發展相關問題研析——以數據資料與大型語言模型之建立為例，立法院法制局議題研析，編號 R02904，2025 年 10 月，https://www.ly.gov.tw/Pages/List.aspx?nodeid=46869
8. 數位發展部，「臺灣主權 AI 訓練語料庫」上線！數位發展部攜手 200 個機關打造本土語料資源，數位發展部網站，2025 年 12 月 24 日，

https://moda.gov.tw/press/press-releases/18314
9. 數位發展部、經濟部智慧財產局，臺灣主權 AI 訓練語料授權條款——第 1 版（Taiwan Sovereign AI Training Data License, Version 1.0），2025 年 12 月。
10. 數位發展部數位產業署，AI 產品與系統評測中心（AIEC）公布最新語言模型評測結果，強化 AI 在地能力與可信任發展，數位產業署網站，2026 年 5 月 4 日，https://moda.gov.tw/ADI/news/latest-news/19588
11. AI 產品與系統評測中心（AIEC），開源／指標模型測試結果，AIEC 官方網站，2026 年 9 月 2 日更新，https://www.aiec.org.tw/web/guest/result

四、新聞報導及網路資料

1. 林志成，國慶日是 10 月 1 日？中研院語言模型出錯急下架，工商時報，2023 年 10 月 9 日，https://www.ctee.com.tw/news/20231009700630-431401。
2. 陳佳鑫、張梓嘉，數發部長指算力中心建在台灣才能有效掌握 AI 主權，公視新聞網 PNN，2026 年 6 月 30 日，https://news.pts.org.tw/article/815472
3. 謝馥伊，和解案後，未解的台灣主權 AI 語料困局：開發者和內容方能否終結授權衝突？，報導者 The Reporter，2026 年 3 月 22 日，https://www.twreporter.org/a/taiwan-sovereign-ai-zhtw-llm-copyright-conflict
4. 蘇文彬，數發部今年擬增購 100 片 GPU 擴大產業免費可用 AI 算力資源，與金管會討論開放保險業投資 AI 算力，iThome，2026 年 3 月 4 日，https://www.ithome.com.tw/news/174181
5. iThome，數發部揭主權 AI 策略：算力中心必須在臺灣、模型需具備 3 大理解力，另看好主權 AI 服務出海，iThome，2026 年 7 月 1 日，https://www.ithome.com.tw/news/177017
6. TechNews，，AI 評測中心公布模型評測，Gemini 2.5 Flash 最具「台灣價值觀」，2025 年 10 月 3 日，https://infosecu.technews.tw/2025/10/03/aiec-unveils-its-first-model-benchmark-results/

貳、外文文獻

一、專書及研究報告

1. Lucía Bosoer & Daniel Innerarity, Unpacking AI Sovereignty, STG POL'Y PAPERS, Issue 2025/18 (Eur. Univ. Inst. Sch. of Transnat'l Governance, Nov. 2025).
2. Francesca Bria, Paul Timmers & Fausto Gernone, EUROSTACK – A EUROPEAN ALTERNATIVE FOR DIGITAL SOVEREIGNTY (Bertelsmann Stiftung 2025), https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/EuroStack__2025_final__1_.pdf.
3. Conor Chapman, Jon Bateman, Andrew Grotto, Colin Kahl, Arthur Nelson & Lakshmee Sharma, AI SOVEREIGNTY, DIFFUSION, AND RISK: STRATEGY

IN A CONTESTED LANDSCAPE (Stanford Program on Geopolitics, Tech. & Governance & Carnegie Endowment for Int'l Peace, Policy Brief, Aug. 12, 2026), https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2026-08/gtg-ceip_ai_sovereignty_2026-08.pdf.

4. IBM INST. FOR BUS. VALUE, THE CALCULUS OF AI SOVEREIGNTY: BALANCING CONTROL, FLEXIBILITY, AND RISK (June 16, 2026), https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-sovereignty.
5. Shreya Joshi, Early Lessons in the Pursuit of Sovereign AI (Carnegie Endowment for Int'l Peace, June 17, 2026), https://carnegieendowment.org/research/2026/06/early-lessons-in-the-pursuit-of-sovereign-ai.
6. Nick Moës et al., Beware of Geeks Bearing Gifts: Building True EU Frontier AI Sovereignty (The Future Soc'y, Apr. 17, 2026), https://thefuturesociety.org/wp-content/uploads/2026/04/Beware_of_Geeks_17April26.pdf.
7. OECD, A Blueprint for Building National Compute Capacity for Artificial Intelligence, OECD DIGITAL ECONOMY PAPERS (Feb. 27, 2023), https://doi.org/10.1787/876367e3-en.
8. Brooke Tanner, Cameron F. Kerry, Andrew Wyckoff, Nicoleta Kyosovska, Andrea Renda & Elham Tabassi, IS AI SOVEREIGNTY POSSIBLE? BALANCING AUTONOMY AND INTERDEPENDENCE (Brookings Inst. & Ctr. for Eur. Pol'y Studies, Report, Feb. 2026), https://www.brookings.edu/wp-content/uploads/2026/02/20260217_AI_sovereignty_final.pdf.
9. WORLD ECONOMIC FORUM & BAIN & COMPANY, RETHINKING AI SOVEREIGNTY: PATHWAYS TO COMPETITIVENESS THROUGH STRATEGIC INVESTMENTS (2026).

二、期刊論文

1. John Perry Barlow, A Declaration of the Independence of Cyberspace, 18 DUKE L. & TECH. REV. 5 (2019).
2. Anupam Chander & Haochen Sun, Sovereignty 2.0, 55 VAND. J. TRANSNAT'L L. 283 (2022).
3. Artur Ishkhanyan, The Sovereignty–Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control, 5 DISCOVER A.I., art. 123 (2025).
4. Daniel Mügge, EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?, 31 J. EUR. PUB. POL'Y 2200 (2024).
5. Huw Roberts, Digital Sovereignty and Artificial Intelligence: A Normative Approach, 26 ETHICS & INFO. TECH., art. 70 (2024).

6. Hazrat Usman, Bushra Nawaz & Saiqa Naseer, The Future of State Sovereignty in the Age of Artificial Intelligence, 5 J.L. & SOC. STUD. 142 (2023).

三、網路資料

1. Muath Alduhishy, Sovereign AI: What it is, and 6 strategic pillars for achieving it, WORLD ECON. F. (Apr. 25, 2024), https://www.weforum.org/stories/emerging-technologies/sovereign-ai-what-is-ways-states-building/.
2. ALT-EDIC, ALT-EDIC Will Contribute to Open-Source LLM Development Under the OpenEuroLLM Project, ALT-EDIC, https://www.alt-edic.eu/news/alt-edic-will-contribute-to-the-development-of-open-source-large-language-models-under-the-openeurollm-project/
3. ALT-EDIC, Poland Launches a Polish Large Language Model (PLLuM), ALT-EDIC, https://www.alt-edic.eu/news/poland-launches-a-polish-large-language-model-pllum/
4. Andrea Benito, Sovereignty Beyond Residency: Why Gulf Governments Must Rethink AI Control, COMPUTER WEEKLY (Aug. 12, 2026), https://www.computerweekly.com/news/366648672/Sovereignty-beyond-residency-Why-Gulf-governments-must-rethink-AI-control.
5. Brian Caulfield, NVIDIA CEO: Every Country Needs AI, NVIDIA BLOG (Feb. 12, 2024), https://blogs.nvidia.com/blog/world-governments-summit/.
6. EnterpriseDB, Data and AI Sovereignty, EDB, https://www.enterprisedb.com/what-is-sovereign-ai-data-sovereignty
7. European Commission, Cloud and AI Development Act, SHAPING EUROPE'S DIGITAL FUTURE (last updated June 3, 2026), https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act
8. European Commission, European Data Union Strategy, SHAPING EUROPE'S DIGITAL FUTURE (last updated May 18, 2026), https://digital-strategy.ec.europa.eu/en/policies/data-union
9. Ren Ito, AI Sovereignty Is About Options, Not Ownership, TAIPEI TIMES, 2026/06/25, https://www.taipeitimes.com/News/editorials/archives/2026/06/25/2003859687.
10. Jeremy Jurgens, The Myth of AI Sovereignty, FOREIGN POL'Y (Mar. 9, 2026), https://foreignpolicy.com/2026/03/09/artificial-intelligence-ai-sovereignty-taiwan-semiconductor-manufacturing-tsmc-chip-supply-chain-united-states-china/.
11. Shana Lynch, The AI Sovereignty Paradox: Should Countries Buy, Build, or Lease to Maintain Strategic Control of Their AI?, STANFORD HAI (July 14, 2026), https://hai.stanford.edu/news/the-ai-sovereignty-paradox-should-countries-buy-build-or-lease-to-maintain-strategic-control-of-their-ai.

12. NVIDIA, What Is Sovereign AI?, NVIDIA RESOURCES, https://resources.nvidia.com/en-us-telco-ai-factories-mc/en-us-telco-ai-factories/what-is-sovereign-ai.
13. OpenEuroLLM Consortium, OpenEuroLLM: A Series of Foundation Models for Transparent AI in Europe, OPENEUROLLM, https://openeurollm.eu/
14. Juan N. Pava, Caroline Meinhardt, Elena Cryst & James Landay, AI Sovereignty's Definitional Dilemma, STANFORD HAI (Feb. 17, 2026), https://hai.stanford.edu/news/ai-sovereigntys-definitional-dilemma.
15. Gregory Smith, Open Models, Digital Sovereignty, and the Future of AI: Why This Debate Matters for Trinidad and Tobago, UNDP (Aug. 13, 2026), https://www.undp.org/trinidad-and-tobago/blog/open-models-digital-sovereignty-and-future-ai-why-debate-matters-trinidad-and-tobago.
16. Cole Stryker, What is an AI Stack?, IBM THINK (Nov. 29, 2024), https://www.ibm.com/think/topics/ai-stack.
17. Stephanie Susnjara & Ian Smalley, What is AI Sovereignty?, IBM THINK (Feb. 4, 2026), https://www.ibm.com/think/topics/ai-sovereignty.