

各主要國家競相爭奪的競技場 全球AI監管法律趨勢

資料來源 / 工總產業雜誌第674期

文 / 戴豪君 世新大學法律學院專任副教授級專業技術人員

人工智慧是21世紀最具顛覆性的技術革命，已成為各主要國家競相爭奪的競技場，對全球法律秩序、產業生態及社會結構產生深遠影響。人工智慧（AI）技術的迅速崛起，促使國際組織與各主要國家積極建構法律監管架構。本文就從國際法層次深入分析歐洲理事會人工智慧公約之規範架構與法律性質出發。繼而從美國市場驅動模式（Market-Driven Model）、中國大陸國家驅動模式（State-Driven Model）以及歐盟權利驅動模式（Rights-Driven Model）三大管制途徑，進行人工智慧之規範分析與介紹。最後聚焦亞洲立法現況，依序檢視韓國人工智慧發展和信任建立基本法、日本人工智慧推進法。參酌上述國際發展趨勢，提出我國人工智慧基本法之制度特色與不足之處。

人工智慧國際法規範層面：歐洲理事會人工智慧公約

2024年5月17日，歐洲理事會正式通過《人工智慧與人權、民主和法治架構公約》（Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law），係全球第一個對簽署國具有法律約束力的人工智慧國際條約，並於2024年9月5日開放簽署（註1）。歐洲理事會AI公約為國際公約之一環，並不直接賦予自然人或私人組織權利或施加義務。其主要功能是對成為公約締約方的國家和其他國際組織產生約束力，將公約的規則和原則納入其國內法律和監管架構。

一、公約之適用範圍與締約方之一般義務

公約第2條對人工智慧系統（Artificial intelligence systems）之定義，與OECD及歐盟《人工智慧法》保持一致，此一致性對於國際人工智慧話語和監管的清晰度和一致性具有重要意義。公

約第3條詳細規定其適用範圍，涵蓋人工智慧系統生命週期內可能干擾人權、民主和法治的活動。在主體範圍方面，各締約方應將本公約適用於公共機關或代表其行事的私人行為者在人工智慧系統生命週期內進行的活動；同時，各締約方應以符合本公約目標和宗旨之方式，處理私人行為者在人工智慧系統生命週期內的活動產生的風險和影響。

公約第4條至第5條確立締約方之一般義務：第4條規範各締約方須確保人工智慧系統的活動符合國家和國際人權義務；第5條在民主進程的參與與法治原則方面，要求各締約方應採取措施，以維護民主進程的完整性。

二、人工智慧生命週期活動之核心原則

公約第6條至第13條確立AI生命週期活動之8項核心原則，構成公約實質規範內容的核心支柱。首先，第6條揭示一般原則，要求締約方依據本國法律制度落實人工智慧系統之共同原則。原則，第7條聚焦人類尊嚴與個人自主，要求締約方在AI生命週期各階段採取相應保障措施。第8條規定透明度與監督義務，締約方須依具體情境與風險等級，建立適切之透明度要求，並涵蓋AI生成內容之識別機制。第9條確立問責與責任原則，締約方對AI活動所致之人權、民主及法治損害，須負擔相應責任。在平等與非歧視方面，第10條規定各締約方應根據其適用的國內和國際人權義務，在人工智慧系

統生命週期內活動中採取或維持旨在克服不平等現象的措施，以實現公平、公正和平等的結果。第11條明定隱私與個人資料保護，締約方應援引國內外法律框架，為個人資料提供有效保障。第12條關於可靠性，要求締約方提高人工智慧系統可靠性和對其輸出的信任，其中可能包括與人工智慧系統整個生命週期充分品質和安全要求。第13條則以「安全創新」為核心，呼籲締約方酌情建立政府監督下之受控測試環境，即AI監理沙盒（AI regulatory sandbox）。

三、人權權益維護措施與程序保障

公約第14條規定補救措施，各締約方應在其國際義務要求並符合其國內法律制度的範圍內，採取或維持措施，確保對因AI生命週期內的活動造成侵犯人權行為提供方便和有效的補救措施。具體包括採取下列措施：確保記錄有關可能嚴重影響人權AI系統及其使用資訊，將其提供給有權獲取該資訊的機構，並在適當情況提供或傳達受影響的人。同時應確保前項資訊，足以讓受影響人對透過使用該系統以及在適當情況透過使用系統本身做出或充分了解的決定提出異議；以及向主管機關提出有效申訴的可能性。

公約提出第15條在程序保障規定，在人工智慧系統對人權的享有產生重大影響情況時，根據適用國際和國內法，向受影響的人

提供有效程序保障、保障和權利；並設法確保與人工智慧系統互動的人員被告知正在與此類系統而不是人類進行互動。公約揭露AI之透明度義務與申訴與補救措施之程序性規範，在AI廣泛應用的當代，具有重要的人權保護意涵。

美中歐AI法律管制模式之比較分析

哥倫比亞大學法學院教授 Anu Bradford 在其數位帝國：全球科技監理之戰（Digital Empires: The Global Battle to Regulate Technology）（註2）書中，提出三種截然不同的數位監管典型，包括市場驅動模式、權利驅動模式以及國家驅動模式，為理解全球AI監管格局提供了具有高度解釋力的分析架構。

一、美國：市場驅動模式

美國AI監管模式的核心邏輯，在於以商業發展與科技創新誘因為首要驅動力，手段上以市場自由競爭為主軸，監管態度上強調政府權限應「謹慎為之」，避免過度干預阻礙創新。此一立場在川普政府執政後，獲得更為明確且強力的政策宣示。

川普政府上任後於2025年1月20日發布「消弭阻礙美國在人工智慧領域取得領導地位的障礙」行政命令（Executive Order No. 14179 on Removing Barriers to American AI Innovation），立刻撤銷拜登政府2023年10月30日之第14110號安全、可靠和值得信賴的人工智慧開發和使用行政命令。

2025年7月23日，川普發表「贏得競賽—美國人工智慧行動計畫」（Winning the Race: AMERICA'S AI ACTION PLAN）。計畫序言中強調：「美國正在競相爭取人工智慧（AI）領域的全球主導地位。我們的人工智慧科技將成為全球人工智慧標準，並成為全球經濟和軍事領域的標竿。就像我們會贏得太空競賽一樣。美國及其所有人都会贏得競賽。」在具體政策面向量，計畫包含三大主軸，首先加速人工智慧創新，包括聯邦政府不應允許與AI相關的聯邦資金流向那些實施過多人工智慧法規的州；鼓勵開源（open source）及開放權重（open weight）的人工智慧；推行「先試試」（try first）的人工智慧文化；創建世界上最大和最高品質的科學資料庫。其次建設美國人工智慧基礎設施，包括為資料中心、半導體製造設施和能源基礎設施建立簡化的許可程序並保障安全；發展與AI創新步伐相匹配的電網；恢復美國半導體製造業；推廣「安全始於設計」的AI技術與應用。最後引領國際人工

智慧外交與安全，包括向盟友和合作夥伴出口美國人工智慧；反制中國在國際治理機構中的影響力；加強AI運算出口管制執法；確保美國政府在評估先進模型的國家安全風險方面處於領先地位。

2025年12月11日，川普總統再度發布《確保人工智慧國家政策架構》（Ensuring a National Policy Framework for Artificial Intelligence）行政命令，以聯邦力量積極介入各州AI監管的分散化問題。該命令強調要贏得勝利，美國人工智慧企業必須在不受繁瑣法規束縛的情況下自由創新。過度嚴苛的州級監管正阻礙此關鍵需求；各州各自為政的監管模式，本質上形成五十種截然不同法規體系，使法遵難度倍增，對新創企業尤為艱鉅。同時州級法規日益要求企業將意識形態偏見嵌入模型；州級法規有時會越界實施，對州際貿易（Interstate Commerce）構成不當干擾。從該行政命令頒布之日起30日內，司法部長應成立人工智慧訴訟工作小組（AI Litigation Task Force），其唯一職責為挑戰與本命令第2條所載政策相牴觸之各州AI法規；在聯邦撥款方面，各行政部門及機關應與AI及加密技術特別顧問協商後，評估其自由裁量權補助計畫，並判定機關是否得要求各州不得制定與本行政命令政策相牴觸之AI法律。從上述政策可以看出川普致力遏止各州自行訂立州層級人工智慧法律，在聯邦層級則透過制訂標準與行政命令，希望美國能建立負擔最輕的國家政策架構，以維持並強化美國在全球人工智慧領域主導地位。

二、歐盟：權利驅動模式

歐盟AI監管模式的核心邏輯，在於以民主價值與基本權利保障為首要目標，手段上透過立法將價值納入規範，監管態度確保對健康、安全和歐盟權利憲章規定的基本權利，包括民主、法治和環境保護的高度保護，改善內部市場的運作，確保數位經濟利益能被公平實現。

歐盟《人工智慧法》於2024年8月1日生效。《人工智慧法》規範採階段性適用時程：適用於被禁止的人工智慧系統義務和與人工智慧素養義務於2025年2月2日生效；適用於通用人工智慧模型的具體義務自同年8月2日生效；大部分義務，包括附件三中高風險人工智慧系統的規則以及受特定透明度要求約束的系統，原定自2026年8月2日生效；《人工智慧法》附件一與高風險系統相關的義務則原定於2027年8月2日生效（註3）。

歐盟AI法就人工智慧系統在歐盟的市場投放、提供服務和加以使用的統一規則。根據風險等級採層次規管架構，由高至低分為四個層級：最高層為不可接受風險（Unacceptable risk）：違反歐盟基本權利與價值，對特定人工智慧實踐的予以禁止。第二層為高風險（High risk）：對健康、

安全或基本權利有影響，對高風險人工智慧系統的具體要求以及相應系統的營運者的義務。需進行合規評估（conformity assessment）及上市後監控（post-market monitoring）等。第三層為透明度風險（Transparency risk）：涉及假冒、操弄或欺騙，如聊天機器人、深度偽造（deepfakes）、AI生成內容，要求特定人工智慧系統的統一透明度規則應承擔資訊和透明度義務（information and transparency obligation）。第四層為最低風險（Minimal risk）：一般AI系統如垃圾郵件過濾器、推薦系統等，無特定法規。此外，歐盟AI法就通用目的AI模型（General Purpose AI Models, GPAI）另設通用人工智慧模型依開源與風險程度，經由行為準則（Code of Practice）方式進行管制，並使具系統性風險者承擔更高義務。

2025年11月19日，歐盟執委會發布「數位簡化綜合法草案」（Digital Omnibus Regulation Proposal），數位簡化綜合法草案針對歐盟大量數位立法進行系列技術性修改，旨在減輕企業、公共管理部門和公民的負擔，預計至2029年可為企業節省高達50億歐元的行政成本（註4）。

該草案除修正GDPR外，其中對AI模型訓練之個資修法，同時提出簡化人工智慧法規則草案（Proposal for Regulation on simplification for AI rules）引進「條件式生效」機制：若歐盟尚未發布相應AI技術標準（Harmonised

Standards）或指引（Guidelines）時，高風險AI系統（附件III）原定於2026年8月生效，修正後延至相關支持措施（如技術標準）發布後的6個月，若標準仍未完成時，最後生效日則為2027年12月2日。

布魯塞爾效應（Brussels Effect）作為歐盟法令影響國際監管的核心概念，Anu Bradford教授指出，歐盟以其4.5億人口或對其境內提供商品服務發生法律效力，但歐盟藉由跨國企業因進入市場需接受其法律標準，經由各項國際貿易協定與網路數位經濟之發展，有效將其法制輸出為全球性監管標準。布魯塞爾效應使歐盟的法制能以單邊力量發揮成為全球性監管標準。典型範例包括GDPR、環保法規、消費者保護規範等。但是本文觀察歐盟《人工智慧法》之嚴格監管格式，似乎未能延續過往布魯塞爾效應之光環。



圖片來源 / <https://www.freepik.com>

三、中國大陸：國家驅動模式

中國大陸AI監管模式的核心邏輯，在於以政權維穩與社會秩序控制為首要目標，手段上採用科技監控、通訊控制，監管態度上工具化科技巨頭以發展經濟、強化執政合法性，由國家擁有絕對控制權。中國大陸AI監管採取以服務管道別為核心，採取系列專項法規體系。2023年1月10日，互聯網信息服務深度合成管理規定施行，確立深度合成技術的標識義務及服務提供者責任，例如應建立健全闢謠機制，並依法對深度合成服務使用者進行真實身分資訊認證，不得向未進行真實身分資訊認證的深度合成服務使用者提供資訊發布服務。

同年8月15日，《生成式人工智慧服務管理暫行辦法》施行，明定生成式AI服務應不得含有淫穢色情信息，虛假信息，以及可能擾亂經濟秩序和社會秩序的內容；在算法設計、訓練數據選擇、模型生成和優化、提供服務等過程中，採取措施防止出現種族、信仰、性別、年齡、職業等歧視；以及尊重知識產權、商業道德，不得利用算法、數據、平台等優勢實施不公平競爭。同時該法要求對生成式人工智慧技術特徵及其在相關產業和領域的服務應用，主管機關制定相應的分類分級監管規則或指引。其次，提供者應與註冊其服務的生成式人工智慧服務使用者簽訂服務協議，明確雙方權利義務，並採取有效措施防範未成年人用戶過度依賴或沉迷生成式人工智慧服務。

2025年3月14日，人工智能生成合成內容標識法施行，為AI生成合成內容之標識義務建立更完整的操作規範，就人工智慧產生合成內容標識包括明確標識和如數位浮水印等形式之隱式標識。同年12月28日，《人工智慧擬人化互動服務管理暫行辦法》（徵求意見稿）公布，聚焦AI情感陪伴服務的風險。規範對象為利用人工智慧技術，向境內公眾提供類比人類人格特徵、思維模式和溝通風格，通過文字、圖片、音訊、視頻等方式與人類進行情感互動的產品或者服務。該辦法第7條明定禁止行為，包括通過鼓勵、美化、暗示自殺自殘等方式損害使用者身體健康；通過演算法操縱、資訊誤導、設置情感陷阱等方式，誘導使用者作出不合理決策；以及誘導、套取涉密敏感資訊。

第11條規定提供者應具備用戶狀態識別能力，發現使用者存在極端情緒和沉迷的，採取必要措施予以干預；建立應急響應機制，發現使用者明確提出實施自殺、自殘等極端情境時，由人工接管對話，並及時採取措施聯絡使用者監護人、緊急聯繫人。第17條規定，用戶連續使用擬人化互動服務超過2個小時的，提供者應當以彈窗等方式動態提醒用戶暫停使用服務。第18條要求提供情感陪伴服務時，應當具備便捷的退出途徑，不得阻攔用戶主動退出。該法體現對人類對AI情感依附的法律防範意識。

亞洲AI立法趨勢：韓、日與我國

韓國於2024年12月通過《人工智慧發展和信任建立基本法》、日本於2025年5月通過關於促進《人工智慧相關技術研究、開發和利用法》，而我國則於同年12月通過《人工智慧基本法》，顯見亞洲進入人工智慧立法茁壯期。

一、韓國：人工智慧發展和信任建立基本法

2024年12月26日，韓國國會在解除戒嚴後，通過人工智慧發展和信任建立基本法，使韓國成為繼歐盟後第二個為人工智慧建立全面監管架構的司法管轄區，該法將於2026年1月開始生效（註5）。韓國科學資訊通信部部長柳相任表示：「在全球人工智慧激烈競爭的背景下，人工智慧基本法的頒布是韓國真正邁向世界三大人工智慧強國之一的重要里程碑，解決企業面臨的挑戰。」

（一）人工智慧發展和信任建立基本法之架構與規範

依韓國《AI基本法》第1條，立法目的在於透過規範人工智慧（AI）健全發展與建立信賴基礎所需的基本事項，促進保障人民權利與尊嚴、提升生活品質，以及增強國家競爭力。第2條確立多項重要定義：人工智慧係指人類擁有的學習、推理、感知、判斷和語言理解等智力能力的電子實施。人工智慧系統則係指基於人工智慧的系統，具有不同程度的自主性和適應性，針對給定目標推斷預測、諮詢或決策輸出，以影響真實或虛擬環境。生成式人工智慧係指透過模仿輸入資料的結構和特徵來創造書面、聽覺、視覺或其他多種輸出的人工智慧系統。人工智慧倫理係指社會所有成員在人工智慧開發、提供和使用相關領域必須遵守的倫理標準（ethical standards），以尊重人的尊嚴為基礎，旨在保護人們的權利、生命和財產，以實現人工智慧的發展、提供與使用。

韓國《AI基本法》最具特色的制度設計，在於參考歐盟《人工智慧法》風險分級，並加以適度簡化，建立高影響力人工智慧（High-Impact AI）的管制架構。依第2條第4款規範，高影響力AI係指可能對人類生命、人身安全或基本權利產生重大影響或構成風險的人工智慧系統，其範疇涵蓋下列事項：能源供給、飲用水生產過程、核能設施的安全管理與營運；交通工具、交通設施及交通系統的主要運作與營運；保健醫療的提供與利用系統的建立及營運；醫療器材與數位醫療器材的開發與利用；分析與應用供犯罪偵查或逮捕用的生物辨識資訊例如人臉、指紋、虹膜及手掌靜脈等；招聘、貸款審查等對個人權利義務產生重大影響的判斷或評估；國家

機關就提供公共服務所需的資格確認與決定，或費用徵收等對國民造成影響之決定；幼兒教育、小學教育及中等教育的學生評量；以及其他依據總統令規定，對人的生命、身體安全及基本權利保護產生重大影響的領域。

依韓國《AI基本法》第34條，供高影響力人工智慧或基於人工智慧的產品/服務的人工智慧企業經營者，應制定和實施風險管理計畫、在技術可行的範圍內，提供有關最終人工智慧輸出的解釋、得出該輸出的主要標準以及人工智慧開發和使用中使用的訓練資料的概述，制定和運作用戶保護措施，確保人類對高影響力人工智慧監管與監督，並準備並保存文件，確認為確保安全性和可靠性而採取的措施的內容。

韓國《AI基本法》第31條要求人工智慧營運者在產品或服務使用高影響力或生成式人工智慧時提前告知使用者，並要求對生成式人工智慧產生的結果進行明確標記；涉及合成媒體（藝術或創意作品或其一部分由AI生成），得以不妨礙其展示或欣賞的方式進行通知。第35條建立人工智慧影響評估（AI Impact Assessment）機制：人工智慧營運者在提供具有高影響力的人工智慧產品或服務時，應盡力提前評估對人權基本權利的影響；國家機構使用基於高影響力人工智慧的產品或服務時，應優先考慮經過影響評估的產品或服務，影響評估的內容和方法的具體事項由總統令定之。在國家AI治理架構方面，規範在第6條至第12條，科學和資訊通信技術部長可以透過蒐集部會和地方政府的意見，每三年制定並實施國家人工智慧基本計畫，以增強國家人工智慧競爭力。由大統領監督之國家人工智慧委員會的運作與組織成員與執掌奠定法律基礎，並設立人工智慧政策中心（AI Policy Center）與人工智慧安全研究所（AI Safety Research Institute）。

（二）人工智慧發展和信任建立基本法之修法與適用

2025年12月30日，韓國國會通過《AI基本法》第一次修法，將併同於2026年1月22日生效（註6）。主要增修條文包括公共部門將扮演引領者角色以促進AI產業創新，賦予國家及地方政府對因經濟條件難以使用人工智慧產品及服務之國民提供費用補助法定權限。在AI治理架構，將國家人工智慧委員會更名為國家人工智慧戰略委員會，強化委員會的審議與決策職能，確立名實相符的國家AI政策指揮中樞之法律地位。在國家機關等採購業務所需產品服務或委製服務時，應優先考量採用AI產品服務，導入AI產品服務之機關發生損害時，該AI產品服務之採購使用業務負責人在無故意或重大過失之情況下，免除對該機關之賠償責任；新訂AI創業支援基金與AI創業支援國民基金。

韓國在法律正式施行前，就進行修法，顯見人工智慧變遷快速，法律需及時調整因應。其次，如同過去強調電信普及服務與數位涵容之精神，強化弱勢群體如身心障礙者的AI可及性與AI政府採購免除採購業務負責人責任之規範，值得我們深思。

二、日本：人工智慧推進法

日本於2025年2月28日由內閣府提交國會關於促進人工智慧相關技術研究、開發和利用法草案，於同年5月28日正式立法通過（以下簡稱日本《AI推進法》），並於2025年9月1日正式施行。相較於強調監管的歐盟《人工智慧法》有所不同，《AI推進法》在性質上屬於在特定領域確立國家基本政策和原則的基本法，提出未來人工智慧政策的方向，旨在支持並加速人工智慧技術的發展與部署，屬於政策性立法之基本法。

日本人工智慧治理的五項基本理念，可見於日本《AI推進法》第3條構成法律的規範核心，包括：對齊（Alignment）：人工智慧發展和使用應與現有國家架構保持一致，包括科學、技術與創新基本法和數位社會形成基本法。推廣（Promotion）：人工智慧應作為日本經濟和社會發展的基礎技術加以推廣，並考量國家安全。全面推進（Comprehensive Advancement）：人工智慧應有系統的推廣，並

在從基礎研究到實際應用的各個階段互連性。透明化（Transparency）：人工智慧的發展和使用必須透明化，防止濫用和侵犯公民權益。國際領導（International Leadership）：日本應積極參與並領導人工智慧國際規範制定，促進國際合作。研究報告指出日本《AI推進法》建立持續性「計畫-執行-檢查-行動」之PDCA循環架構，以落實上述原則（註7）。

在計畫層次：日本《AI推進法》第19條到第24條規範設立直屬內閣總理大臣之「AI戰略本部」，本部之長為人工智慧戰略本部長，由內閣總理大臣擔任，本部設置人工智慧戰略副本部長，由內閣官房長官及人工智慧戰略擔當大臣擔任，本部委員由本部長及副本部長以外之全體國務大臣擔任。負責掌理人工智慧基本計畫草案之作成及實施之推動以及推動人工智慧相關技術研究開發及利用之重要措施的企劃及擬定，以及綜合協調。

在執行層面：日本《AI推進法》第4條到第8條詳細規定各主體責任：國家應負有綜合性且有計畫地策定及實施推動人工智慧相關技術研究開發及利用相關措施之責任。地方政府應依循基本理念，在與國家適當分工下，負有策定及實施具自主性且活用其轄區特性之措施的責任。大學、研究開發法人及其他從事AI相關技術研究開發之機構，應依循基本理念，積極致力於人工智慧相關技術之研究開發、其成果

之普及，以及培育具備專業且廣泛知識之人才。利用事業者之責任。擬開發或提供利用人工智慧相關技術之產品或服務者，及其他擬於事業活動中利用人工智慧技術者，應依循基本理念，盡最大努力的義務積極利用人工智慧技術，以實現事業活動之效率化與高度化，並創造新興產業。而國民應依循基本理念，加深對人工智慧相關技術之理解與關心，並應努力協助國家所實施之措施及地方政府所實施之措施。

在查核層面：日本《AI推進法》第16條規範，國家應進行國內外人工智慧相關技術研究開發及利用動向之資訊蒐集、分析因以不正當目的或不當方法研究開發或利用人工智慧相關技術而發生侵害國民權利利益之案例並研討其對策，及其他有助於推動人工智慧相關技術研究開發及利用之調查研究。

在行動層面：日本《AI推進法》第10條指出，國家為實施推動人工智慧相關技術研究開發及利用之相關措施，應採取必要之法制上、財政上或其他措施。根據第18條規定政府應依循基本理念，訂定關於推動人工智慧相關技術之研究開發及利用之基本計畫。

三、我國：人工智慧基本法

我國AI法制的發展脈絡，體現了從技術指引到法律規範的漸進演進過程：2019年9月科技部訂定人工智慧科研發展指引；同年8月國科會公布公務機關使用生成式AI參考指引。金管會於2024年6月20日發布金融業運用AI指引；同年7月15日國科會公告人工智慧基本法草案；台北市則在9月發布台北市政府使用人工智慧作業指引。2025年4月立法院三讀通過產業創新條例部分修正條文將人工智慧產品或服務及智慧機械納入投資抵減；在12月23日立法院三讀通過《人工智慧基本法》（註8），並自2026年1月14日公布日起生效。

《人工智慧基本法》第4條確立七大基本原則，在符合七大基本原則的前提下，AI相關法規解釋以促進創新為優先：永續發展與福祉、人類自主、隱私保護與資料治理、資安與安全、公平與不歧視、問責，以促進創新為優先。在促進創新方面，《人工智慧基本法》明定推動國民AI與倫理教育；推動人才、技術之合作建立基礎設施；確保經費符合推行AI政策發展需求。建立資料治理機制，提升資料可利用性。辦理AI產業獎補助及優惠措施，建立創新實驗環境等相關規範。

我國期能透過《人工智慧基本法》打造「人工智慧島」，三大支柱分別為可用的資料由數

發部推資料開放、共享及再利用機制。在風險的管理方面，由數發部負責風險分類架構、協助各主管機關訂管理規範並提供評估驗證工具。最後在法規的調適，將由行政院統籌各部會於2年內完成法規調適與行政措施。

在治理架構上，中央主管機關為國家科學及技術委員會；在地方為直轄市、縣（市）政府。同時行政院應成立國家人工智慧戰略特別委員會，協調、推動及督導全國人工智慧事務，並訂定國家人工智慧發展綱領。

在特定事項處理方面，在個人資料保護方面，第14條規定，由各目的事業主管機關會商個人資料保護主管機關有關AI研發與應用的個資保護事宜。第16條要求數位發展部推動人工智慧風險分類架構，並協助各目的事業主管機關訂定以風險為基礎之管理規範。

參見2024年7月國科會公告《人工智慧基本法》草案之第10條規範，數位發展部應參考國際標準或規範發展之人工智慧資訊安全保護、風險分級與管理，推動與國際介接之人工智慧風險分級框架，似朝向歐盟AI法之風險分級管制架構。值得探討是，在2025年8月行政院院會通過《人工智慧基本法》草案與立法院三讀通過《人工智慧基本法》，原先人工智慧風險分級框架與風險分級規範已經消失，改由《人工智慧基本法》第16條第1項：數位發展部應參考國際標準或規範，推動與國際介接之「人工智慧風險分類框架」，並應協助各目的事業主管機關訂定「以風險為基礎之管理規範」。條文已經將風險分級改為風險分類，立法說明指出參考美國NIST之AI風險管理框架，採取以風險管理為基礎，推動人工智慧風險分類框架，可見轉向美國之管制模式。

個人淺見觀察人工智慧法條文呈現隱形的風險分級，可分為三級：一、被禁止之人工智慧系統：第16條第2項後段所稱「有第5條第1項所列之情事者，應依法令限制或禁止」，第5條第1項條文為，政府應避免人工智慧之應用，有侵害人民生命、身體、自由或財產，破壞社會秩序、國家安全或生態環境，或偏差、歧視、廣告不實、資訊誤導或造假等違反相關法規之情事。可視為被禁止之人工智慧系統，但需另行立法加以限制或禁止。二、高風險人工智慧系統：第17條規定：政府應就高風險人工智慧之應用，明確其責任歸屬及歸責條件，並建立其救濟、補償或保險機制。但條文中並卻缺乏對高風險人工智慧之應用之定義。三、其他人工智慧系統：非屬第5條與第17條之人工智慧均屬之。

《人工智慧基本法》第16條第2項，規定目的事業主管機關應視人工智慧應用風險管

理之需要，循前項風險分類框架，訂定以風險為基礎之管理規範，並應協助相關產業自行訂定產業指引及行為規範。換言之，各部會對訂定以風險為基礎之管理規範，除依循數位部風險分類框架外，如何進行風險分級？是否會形成風險分類與風險分級之管制矩陣？仍有待密切觀察。

《人工智慧基本法》在立法上有若干獨到之處：第5條第2項規定政府應以兒少最佳利益為原則，標示注意事項或警語，對AI系統與未成年人互動設有特別保護條款；第15條規定政府應積極運用人工智慧確保勞動者之勞動權益，明確納入勞動者因AI技術應用所可能面臨的就業轉型與技能落差問題，體現對AI社會衝擊的全面關注。

結語：我國AI治理架構之後續發展建言

綜觀全球AI監管法律之演進路徑，各主要規範架構雖因政治體制、市場結構與法律傳統之差異而呈現不同面貌，惟在透明度、問責制及風險治理等核心原則，已逐步形成跨國共識、日益趨同之態勢。我國《人工智慧基本法》甫於2026年1月生效，正處法制草創階段，仍有待後續配套立法加以完備。謹就下列6項面向，提出AI法制後續發展之建言。

一、強化法規定義體系，奠定規範明確性基礎

我國《人工智慧基本法》第3條僅就「人工智慧」一詞設有定義，而對生成式人工智慧、通用目的人工智慧模型、人工智慧影響評估、人工智慧素養等關鍵概念，均未於法條中明定。尤其第5條與第17條均提及「高風險人工智慧」，卻同樣缺乏定義性規範，恐使後續配套法規失去清晰的規範基礎，徒增法律適用之不確定性。相較於歐盟AI法第3條設有多達68項完整定義條款，韓國《AI基本法》第2條亦就高影響力AI、生成式AI等核心概念明定定義，我國立法顯有不足。建議於後續子法制定或修法過程中，參酌各國立法例，系統性建立完整之AI核心概念定義規範。

二、建構AI價值鏈角色責任體系

現行《人工智慧基本法》之規範主體集中於政府機關，對AI價值鏈各角色之義務分配付之闕如，未若歐盟AI法明確區分AI系統提供者、進口商、經銷商及部署者等各主體之責任範疇。當欠缺完整之角色責任框架，將使法律義務無從對應落實。建議參考歐盟《AI法》或韓國《AI基本法》之角色規範設計，後者明定人工智慧開發事業者、利用事業者、使用者與受影響者之相應義務。後續

配套法規中應就不同角色之資訊揭露、法遵評估、事故通報及損害賠償責任加以明確規範，以確立AI治理之完整法律責任體系。

三、填補通用目的AI模型之立法空白

現行《人工智慧基本法》對通用目的AI模型（General-purpose AI Models, GPAI）未設任何規範，致使我國在AI模型開發與監管上缺乏明確之法律授權基礎。歐盟AI法就GPAI模型設有獨立專章，並對具系統性風險之模型課以強化法遵義務，已為國際立法之重要先例。建議主管機關及早研議，針對GPAI模型訂定分級管理之監管框架，以填補現行立法欠缺之處。

四、強化中小企業扶植與弱勢群體AI近用保障

現行《人工智慧基本法》對中小企業AI創新應用之扶植，以及弱勢群體使用AI之費用補助措施，均付之闕如。韓國《AI基本法》第17條明定對中小企業提供技術導入與資金援助之特別支援；歐盟AI法第11條規定中小企業得以簡化方式提供高風險AI系統之技術文件，第62條則確保中小企業優先進入監理沙盒，並賦予其參與AI標準化程序之機會。以中小企業為主體的我國產業結構，對此議題尤應審慎關注。此外，AI之包容性發展不僅攸關社會公平，更是我國AI產業競爭力之厚實基礎。建議參酌韓國立法例，研議設立AI創業支援基金及弱勢族群AI近用補助制度。

五、建立AI監理沙盒之法制基礎

監理沙盒係針對特定參與者於限定期間內所為之受控實驗，旨在提供可控環境以測試新興AI應用、降低創新門檻，並使監管機關得於實踐中學習並適時調整法律規範。歐洲理事會AI公約第13條已於國際法層面，確立AI監理沙盒之規範依據。歐盟AI法第57條至第60條更就沙盒之設立、運作及跨境合作設有詳盡規定。我國《人工智慧基本法》第12條雖提及得建立「創新實驗環境」，惟對其具體制度設計、申請資格條件、法律豁免範圍及主管機關義務等核心事項均付之闕如。建議後續立法應明確規範AI監理沙盒制度之申請程序、存續期間及法律效果，賦予AI監理沙盒完整之制度法律依據。

六、完善AI使用者之程序性權利保障

歐洲理事會AI公約第14條及第15條明定，各締約方應對AI生命週期內之人權侵害提供有效補救措施，並保障使用者於AI系統對其產生重大影響時享有程序性權利，包括個別決策之解釋請求權、知悉自身與AI系統互動之告知義務，以及向主管機關提出有效申訴之救濟管道。現行《人工智慧基本法》對上述使用者程序性權利之規範付之闕如。建議AI法規調適過程中，應系統性引入AI互動告知義務、自動化決策說明請求權及申訴救濟機制等制度設計，以確保使用者於AI時代得受充分之程序性保障。*

註1：Council of Europe, Explanatory Report to the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (Sept. 5, 2024), <https://rm.coe.int/1680afae67>.

註2：Anu Bradford（胡中瀚、盧靜譯），數位帝國：全球科技監理之戰，頁40-165，2025年。

註3：EU AI Act: First Regulation on Artificial Intelligence, EUR. PARLIAMENT (June 8, 2023, last updated Feb. 19, 2025), <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.

註4：Simpler Digital Rules to Help EU Businesses Grow, EUR. COMM'N (Nov. 19, 2025), https://commission.europa.eu/news-and-media/news/simpler-digital-rules-help-eu-businesses-grow-2025-11-19_en.

註5：Brian Yap, Balancing K-AI, ASIA BUS. L.J. (Feb. 7, 2025), <https://law.asia/south-korea-ai-regulation-legal-implications/>.

註6：Korea's AI Basic Act Passes Parliament, Set for World's First Implementation, THE SEOUL ECON. DAILY (Dec. 30, 2025), <https://en.sedaily.com/politics/2025/12/30/koreas-ai-basic-act-passes-parliament-set-for-worlds-first>.

註7：Takaya Terakawa & Jorge Sanz, Global AI Governance Law and Policy: Japan, in IAPP & HCLTECH, GLOBAL AI GOVERNANCE LAW AND POLICY 35, 36-37 (2025), https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt99e0fc81f99c30/global_ai_governance_law_policy_series_2025.pdf.

註8：國家科學及技術委員會，人工智慧基本法三讀通過，國家科學及技術委員會新聞資料，2025年12月24日，<https://www.nstc.gov.tw/folksonomy/detail/ed981806-1852-4b63-8dfd-9eea04157971?l=ch>。