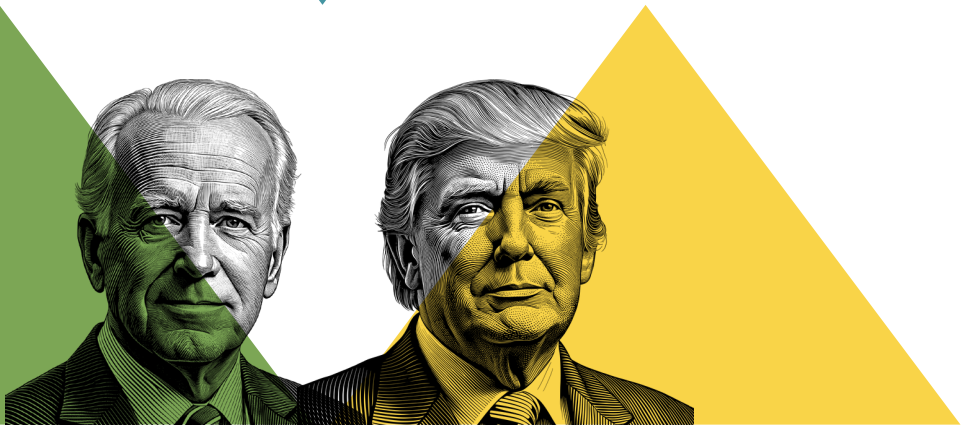
美國聯邦政府AI治理

- 從拜登的風險控管與倫理監管到川普2.0的市場導向開放創新MAGA -



2025.05.06
許慧瑩
東吳大學法律學系
hyhsu007@scu.edu.tw

拜登政府的AI治理與風險管理

美國聯邦政府的應用概述

- AI應用的目標
  - 提高效率、改進決策、改善公共服務
  - 建立AI治理框架與安全標準

- AI應用挑戰
  - 平衡風險與機會
  - 確保隱私與安全
  - 跨機關合作與標準化

拜登政府的AI治理與風險管理

主要監管機構

- 制定：管理與預算辦公室 (OMB)
- 標準：國家標準與技術研究院 (NIST)
- 執行：美國政府問責辦公室 (GAO)

核心治理原則

- 透明度、公正性、問責性
- 風險識別與應變計劃
- 建立首席AI官 (CAIO)

拜登政府AI治理呼應歐盟採取嚴格監管模式

2024年3月OMB第M-24-10號《強化聯邦政府機關使用AI之相關治理與風險管理》備忘錄

目標

- 制度建置、現況盤點及最低程度的遵循，確保機關AI應用的一致性

規範來源

- 以拜登政府第14110號行政命令《AI的安全、可靠與可信的開發和使用》為框架，並與《2020年政府AI法》（AI in Government Act of 2020）及《促進美國AI法》（Advancing American AI Act）之規定相符

拜登政府AI治理呼應歐盟採取嚴格監管模式

2024年3月OMB第M-24-10號備忘錄

核心要求

- **加強AI治理：設立CAIO 首席AI官**
- **推進負責任的AI創新，例：採取促進AI模型、程式碼及資料共享和再利用的相關措施**
- **管理AI風險，例： 最低風險管理標準**
  - 影響安全和權利的AI時須遵守的最低實踐準則
  - 列舉被認定屬影響權利與安全的特定AI類別
  - 聯邦機關採購AI的風險管理，提出系列建議
- **促進AI應用例：技術基礎設施與勞動力影響評估**

拜登政府AI治理呼應歐盟採取嚴格監管模式

2024年3月OMB第M-24-10號備忘錄

- 透明公開與公眾溝通AI的使用，與其可能帶來的影響
- 確保AI系統符合倫理原則，注重公平性、透明度和問責
- 首席AI官負責推動聯邦機關有關AI採購和使用的任務
- 建議參考NIST Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile，以促進機關AI應用相關之技術，符合倫理和安全制度建置與最低標準，確保聯邦機關AI應用的一致性

拜登政府AI治理呼應歐盟採取嚴格監管模式

2024年9月OMB第M-24-18號《強化聯邦政府機關可課責的AI採購》

目標

- AI治理應前置至政府採購階段
- 強調跨機構合作及風險管理，促進AI技術的創新與競爭
- 從早期階段管理隱私風險，確保遵守相關規則並保障公共安全與權利
- 部門合作聚焦於識別和排序AI投資項目，通過委員會制定最佳實作

核心策略

- 跨機關協作，例：共享AI採購資訊
- AI風險與功效管理，例：隱私、安全、互操作性
- 促進競爭性AI市場，例：防止供應商壟斷

拜登政府AI治理呼應歐盟採取嚴格監管模式

2024年9月OMB第M-24-18號

重點

- **確保跨職能及跨機構協作，共享資訊**
- **管理AI風險與功效**
  - 基於OMB第M-24-10號備忘錄所確立之與採購相關的實踐
  - 對影響權利及影響安全類別的AI，採取各自所需的風險管理措施
  - 採取額外措施，確保負責任地採購生成式AI和生物特徵辨識AI系統
- **透過創新採購促進競爭性AI市場 (不會lock-in)**
  - 應優先考量互操作性，並防止讓供應商獨佔採購優勢的問題
  - 鼓勵創新實踐，在AI採購中獲得最佳結果支持多元具競爭力與彈性之AI聯邦政府採購市場

拜登政府AI治理呼應歐盟採取嚴格監管模式

拜登政府 OMB 備忘錄發展方向

- 持續發展方向
  - 強化AI治理框架
  - 提升機關對AI技術的適應力
  - 擴大與私部門合作

- 關鍵挑戰
  - 平衡創新與監管
  - 確保公平與道德標準
  - 技術發展與法律更新同步

川普2.0後美國AI法律與監管方向改變

2025年1月20日首次撤銷有害的行政命令和行動

- **撤銷第 14110 號行政命令《安全、可靠且值得信賴的AI開發與使用》**
  - 第 14110 號行政命令中有關要求開發人工智慧的公司在其產品向公眾發布之前與聯邦政府分享有關其技術的資訊，頗受批評
  - 除有關使用公共土地作為資料中心第14141號行政命令 (2025年1月)外，所有其他與人工智慧有關的拜登政府行政命令也被撤銷

川普2.0後美國AI法律與監管方向改變

2025年1月23日發布第14179號《消除美國AI創新障礙》行政命令

- **消除阻礙AI創新的政策，促進美國經濟競爭力和國家安全**

主要面向

- **消除AI創新的政策障礙**
  - 撤銷拜登政府對AI研發和部署的嚴格限制，鼓勵私部門創新
  - 要求各聯邦政府機關修改或撤銷不利於AI發展的政策與法規
- **增強美國AI的領導地位**
  - 強調AI開發須避免意識形態偏見
  - 指示制定AI行動計劃，由白宮科技團隊和國家安全顧問協同領導，確保美國在AI領域的持續競爭力
  - 取消拜對AI政策的限制，增強美國在全球AI的領導地位

川普2.0後美國AI法律與監管方向改變

2025年1月23日發布第14179號行政命令

- 總統科技助理(APST), the Special Advisor for AI and Crypto, and the APNSA與機關首長應檢視依據第14110 號行政命令所採取的行動
  - 若有與本命令之促進美國的經濟競爭力和國家安全政策不一致或可能不一致或構成障礙的行為，機關首長應引可適用的法律，暫停、修改或撤銷行為
  - 如行為無法即刻暫停、修改或撤銷， APST與機關首長應立採取行動，，根據可提供豁免之命令、規則、條例、指引或政策，確保適當且符合法律規定，直到此類行動最終確定
  - 與OMB 主任協調，以本命令促進美國的經濟競爭力和國家安全的政策，修訂 OMB 第M-24-10 和 M-24-18備忘錄

川普2.0的AI治理方向在巴黎高峰會可得探知

2025年2月巴黎AI促進公共利益憲章

- 61國簽署AI行動峰會宣言，峰會目的：尋找安全地鬆綁管制，促進發展
  - 公開促進科學進展，催生創新並促進競爭。AI 的公開性（ openness）主要由少數參與者決定部分開放其基礎模型所推動。彈性的生態系統有助於支援開放模型的開發，涵蓋標準制定、工具和最佳實作
  - 在 AI 設計、開發和部署各階段，問責制（Accountability ）是實現公共利益 AI 的基石。問責依賴現有國家和國際框架的執行，為研究、監督和賦權機構和民間社會創造有利條件
  - 參與和透明度是公共利益 AI 民主治理的先決條件

AI ACTION SUMMIT

川普2.0的AI治理方向在巴黎高峰會可得探知

巴黎AI促進公共利益憲章

- 歐盟AI ACT側重保護公民隱私，被評阻礙創新
- 南方國家強調AI對低收入國家經濟發展方面的影響
- 美英拒簽
  - 美國「過度監管AI可能扼殺這個變革性產業」
  - 批評歐盟《數位服務法》及GDPR法遵成本沈重
  - 英國基於國家安全與全球治理問題
- 歐盟承諾
  - 將減少繁文縟節，但也為其監管政策辯護
  - 多使用開源

AI ACTION SUMMIT

川普2.0將AI治理轉為開放創新與MAGA

2025年4月7日預算與管理辦公室(OMB)發布兩份備忘錄

- **OMB 第M-25-21號《透過創新、治理與公眾信任加速聯邦機關AI的使用》 》(AI使用) 備忘錄，OMB 第M-25-22號《推動聯邦政府機關有效率地取得AI》(AI採購)備忘錄，**
- **調動方向**
  - 採取前瞻性、支持創新與競爭的思維，非延續拜登政府的風險規避策略
  - 避免在行政部門內施加不必要的行政官僚限制
  - 各機構應更靈活有彈性、具成本效益並提高效率
  - 在提升美國在AI創新領域的全球領導地位的同時，改善美國民眾的生活

川普2.0將AI治理轉為開放創新與MAGA

OMB 第M-25-21號備忘錄

目標

- 加速聯邦政府AI應用：推動創新、強化治理、建立公眾信任
- 提升政府服務品質：透過AI技術，提升政府效率與服務品質
- 確保公民權益保障：在推動AI應用的同時，維護公民的隱私權、權利與自由

核心策略

- 移除創新障礙：減少不必要的官僚限制，促進AI的負責任採用
- 制定AI策略：各機構需制定AI策略，提升AI應用的成熟度
- 最大化現有投資價值：共享資源、重複使用資料與模型，避免重複投資
- 強化AI人才：培養並保留具備技術經驗的AI人才，推動應用

川普2.0將AI治理轉為開放創新與MAGA

OMB 第M-25-21號備忘錄

重點

- **指定首席AI官（CAIO），領導AI相關事務（促進與推動）**
- **建立AI治理委員會，協調AI的開發與應用**
- **制定AI風險管理政策**
  - 針對高影響力的AI系統（對個人權利、公共安全或關鍵政府運作可能造成重大影響），實施最低風險管理實踐
- **持續監測AI系統，定期評估性能，確保其安全性與可靠性**
- **提供人為監督與介入機制**
  - 確保AI系統在關鍵決策具人為監督與介入的能力
- **建立申訴與補救機制**
  - 為受AI系統影響的個人提供申訴與補救的途徑

川普2.0將AI治理轉為開放創新與MAGA

OMB 第M-25-22號《推動聯邦政府機關有效率地取得AI》備忘錄

目標

- 促進競爭性美國AI市場，確保政府和公眾從競爭性的美國AI市場中受益。
- 保障納稅人的稅金，透過追蹤AI性能和風險管理，確保AI系統符合目的並提供一致的結果
- 在AI採購過程推動跨部門合作，解決潛在問題

核心策略

- 明確需求規範：政府必須傳達清晰且具體的需求，使供應商能夠提供最先進的AI能力，以支持高效且有效的公共服務
- 避免供應商鎖定：在加速採用AI服務時，機構必須注意供應商來源、數據可攜性和長期互操作性，以避免對單一供應商的重大且昂貴的依賴
- 強化性能追蹤與風險管理：確保所採購的AI系統適合其目的，並提供一致的結果，以維護公眾信任

川普2.0將AI治理轉為開放創新與MAGA

OMB 第M-25-22號備忘錄

重點

- **制定AI採購指引**
  - 提供快速、具競爭力且負責任地取得AI技術
- **支援競爭性的美國AI市場**
  - 最大化使用美國AI系統，強化國家競爭力與安全
- **避免供應商依賴與加強互操作性**
  - 注意供應商來源、資料可攜性和長期互操作性，防止對單一供應商的依賴
- **建立共享資源庫：**
  - 推動AI採購工具與資源的共享，促進跨機構的協作與知識累積
- **簡化報告與合規要求：**
  - 簡化機構報告流程，提升效率，同時保障隱私與合法使用政府資料

拜登v. 川普

OMB 第M-25-21號備忘錄 (AI使用)

- 取代OMB第M-24-10號備忘錄
- 川普2.0三個優先事項創新、治理和公眾信任，與川普1.0於2019年頒布之第 13859 號行政命令主張一致
- 沿用Biden政府AI管理相關機制，例如CAIO、委員會，例如拜登時期稱AI使用的風險（right-impacting or safety-impacting），川普2.0稱高影響力 “high-impact”

OMB 第M-25-22號備忘錄 (AI採購)

- 取代 OMB第M-24-18號備忘錄
- 延續拜登政府對競爭性AI市場、追蹤AI效能和管理風險以及跨職能協作的好處
- 川普2.0增加最大化利用美國製造的AI

拜登v. 川普

同

- AI使用的風險與高影響力AI雖然名詞不同，在最低限度的風險管理實踐，例如測試和影響評估
- 均有終止不符合風險管理要求的用途，但新MEMO要求各機構在一年時間內提供文件，證明最低限度的做法得到遵守，並停止不合規的使用案例
- 均有申請豁免風險管理要求的能力，新MEMO有高影響力用途清單（例示），部分與拜登政府MEMO類別相同

- 異

- 川普延續1.0行政命力要求各機構有責任維護年度和公開清單，記錄該技術在該機構的使用情況
  - 鼓勵持續更新清單的公開版本，反映AI使用情況

對M-25-21的評論

目的務實，但對權利保障不足，或規範過於抽象

正評

- 因其在創新與風險管理之間取得平衡而受到讚揚，允許各機構移除官僚障礙，同時維持基本風險控管。
- 首席AI官（CAIO）有助於各機構內部AI政策的責任明確

批評

- 該政策被批評對「不必要」治理定義過於模糊，賦予機構過多裁量權，可能導致執行上的不一致
- 對高影響力AI系統僅要求「最低限度風險管理」，被認為不足以保障公民權利

對M-25-22的評論

市場導向應將增進效率，但MEMO過簡可能產生風險

正評

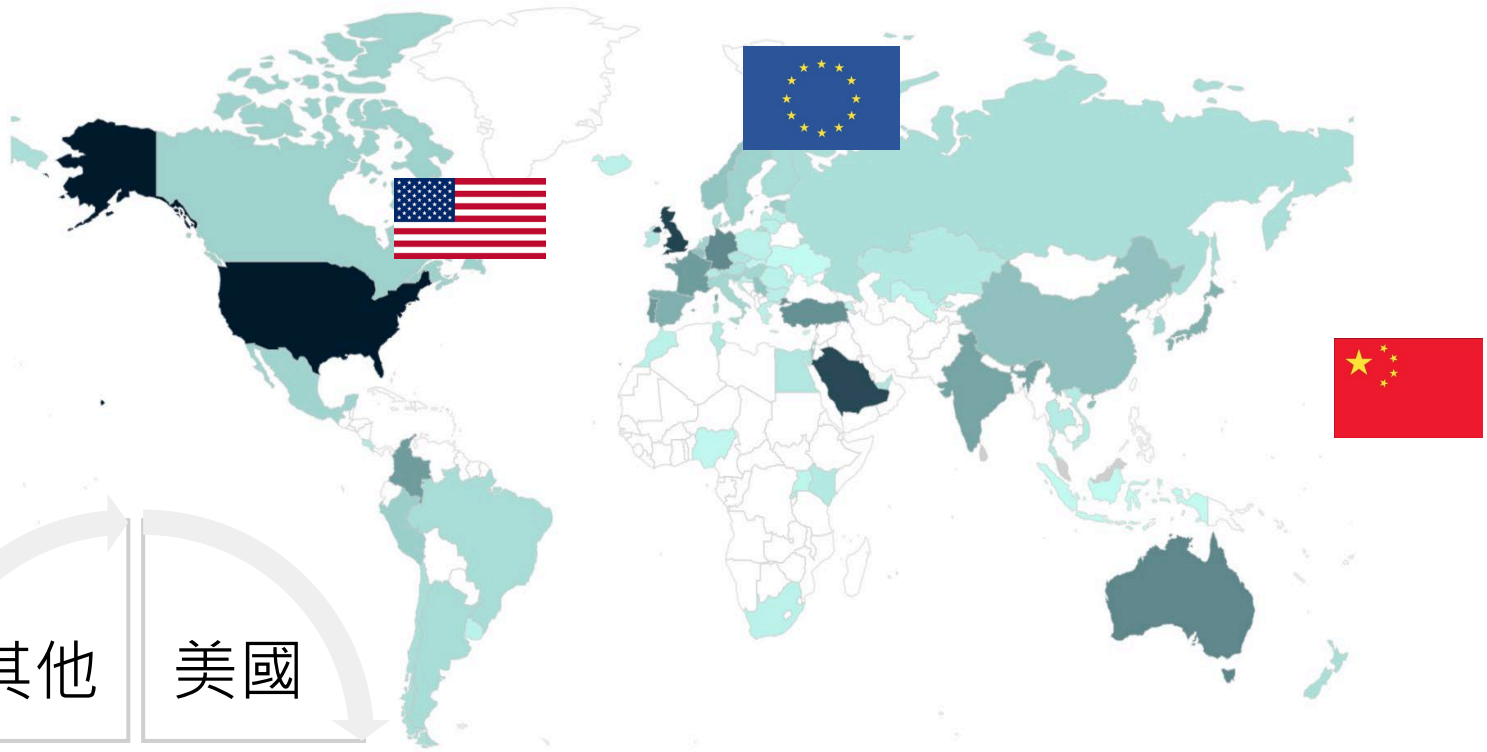
- 鼓勵具競爭性的AI採購、支持美國本土市場及避免供應商依賴
- 機構須謹慎處理供應商來源、資料可攜性與長期互操作性，避免對單一供應商產生重大且昂貴的依賴

批評

- 過度著重於效率與速度，可能忽視對AI系統偏誤、公平性及倫理問題
- 缺乏明確的公眾透明義務，導致問責性不足的疑慮
- 簡化採購流程 可能使無法應對快速大規模競標的小型企業被排除

AI 治理的政治角力

資料來源：OECD.AI (2021), powered by EC/OECD (2021), database of national AI policies, accessed on 26/04/2025, https://oecd.ai.



其他 美國

中國 歐盟