

現階段歐盟與美國對人工智慧規範之 比較分析 *

陳奕璇

銘傳大學犯罪防治學系助理教授

摘要

歐盟《人工智慧法》2024 年 8 月 1 日正式生效，期間歷經公開審議、接納各方建議、彙整後由歐盟執委會做出修改，這是公、私部門相互協商的討論內容。美國總統川普以創新發展為優先，但美國聯邦政府與州政府之間對人工智慧 (Artificial Intelligence, 簡稱 AI) 監管立場卻有不同。就管制 AI 系統來說，歐盟以權利導向 (right-driven) 為基礎，美國則以市場導向 (market-driven) 為主。目前美國是全球 AI 發展最為快速的國家，歐盟 AI 使用率較不普及。然而歐盟為何儘早制定《人工智慧法》，目的希望數位轉型過程預先「管制風險」，防堵 AI 所造成的技術漏洞。歐、美在 AI 規範設置雖看似立場不同，但實際上仍有部分趨同的現象。有鑑於此，本文將試圖提出監管性權力 (regulatory power) 與風險管理及 AI 韌性的概念，用以檢視歐盟、美國的 AI 規範，並對臺灣 AI 發展提供建議。

關鍵字：歐盟、美國優先、人工智慧、監管性權力、AI 韌性

* 本文為國科會研究計畫之部分研究成果，計畫編號：NSTC 113-2410-H-130-051-。

Comparative Analysis of Current Artificial Intelligence Regulations in the European Union and the United States

Yi-Hsuan Chen

Assistant Professor, Department of Criminal Justice,
Ming Chuan University

Abstract

The European Union (EU) Artificial Intelligence Act will officially take effect on August 1, 2024. This legislation has undergone a period of public consultation, during which inputs from multiple stakeholders were incorporated by the European Commission to revise relevant provisions. The legislative process reflects ongoing negotiations between the public and private sectors regarding artificial intelligence (AI) applications. By contrast, the United States has prioritized AI innovation and development under the policy of the Trump administration, where the federal and state governments have different stances on AI regulations. In terms of regulatory approaches, the EU adopts a rights-driven model, whereas the United States follows a market-driven one. Currently, the United States leads the world in the rapid development of AI, and the EU exhibits lower rates of AI adoption. Nevertheless, the EU's decision to introduce the Artificial Intelligence Act at the early stage of AI development aims to manage potential risks during digital transformation and to preemptively address vulnerabilities arising from AI technologies. Despite apparent divergences in regulatory philosophy between the EU and the United States, their approaches also converge

in several aspects. In light of these dynamics, this study adopts the concepts of regulatory power, risk management, and AI resilience to examine the respective AI governance models of the EU and the United States, in addition to providing policy recommendations for AI development in Taiwan.

Keywords: European Union, America First, Artificial Intelligence, Regulatory Power, AI Resilience

壹、前言

自從 2021 年 4 月 21 日歐盟《人工智慧法》草案 (European Union Artificial Intelligence Act, 以下簡稱 EU AI Act) 提出後, 歐盟希望以「優良與可信性之方向去確保人工智慧 (Artificial Intelligence, 以下簡稱 AI) 發展的安全性」, 保護基礎人權不受到侵害為原則。然而縱觀世界強權對發展 AI 想法不一, 歐盟從嚴謹面向制定法律。而美國希望以鬆綁 AI 法規、創新發展為目標, 因此, 2025 年 1 月川普總統 (Donald Trump) 上任後撤銷拜登總統 (Joe Biden) 所公布的行政命令第 14110 號《安全、可靠且值得信賴的人工智慧使用與開發》 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence), 希望將 AI 限制鬆綁。美國是市場導向 (market-driven) 特別在數位科技領域中是依據市場需求調整內部法規與政策,¹ 獲取最大利益為優先。川普上任後率先發布行政命令第 14148、14177、14179 號以及兩項重要的備忘錄《以創新、治理與公共信任推動聯邦政府加速採用人工智慧》 (Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, 以下簡稱 M-25-21)、《推動政府部門更有效率地採購人工智慧》 (Driving Efficient Acquisition of Artificial Intelligence in Government, 以下簡稱 M-25-22), 到 2025 年 7 月 23 日川普政府公布《美國 AI 行動計畫》 (America's AI Action Plan), 可看出川普對 AI 規範與未來政策方向。

¹ Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (New York: Oxford University Press, 2023), pp. 33-68.

事實上，當 EU AI Act 生效後，成為全球第一部 AI 立法，當下即有對 AI 法規監管緊縮與寬鬆之探討。而為何會有 AI 規範緊縮與寬鬆的差異？國家若採取緊縮法規，是擔心 AI 快速發展會導致大規模侵害人權、犯罪等情事發生，同時，AI 等同運用大規模資料建構，資料來源可能會涉及侵害隱私，此外，自動化決策過程的不透明性，恐會傷害人權。而歐盟為減緩未來使用 AI 所造成危機，設立 EU AI Act 形塑安全化路徑。反觀美國採取鬆綁法規的立場，則是因為法規會限制 AI 發展與創新，傷害國家經濟利益。雖然歐盟與美國在 AI 發展觀點上存有極大差異，但歐盟、美國主要目標都是要加速 AI 發展，只是歐盟建立「法規」是希望透過監管方式降低 AI 風險創建永續環境，²而美國聯邦政府鬆綁「法規」以創新為目標，但各州政府仍有相關 AI 法規，顯見美國依舊存有監管的事實。

有鑑於此，本文選取歐盟與美國作為案例分析，主因歐、美為 AI 發展的重要引領國會對世界產生外部、內部效應。藉此本文試圖以監管性權力 (regulatory power) 及風險管理與 AI 韌性 (resilience) 之概念，試分析歐盟與美國對 AI 發展態度，作為臺灣未來 AI 發展之方向。

貳、AI 規範引發的效應

美國學者 Stephen Krasner 認為國際建制 (International

² European Commission, *The AI Continent Action Plan*, April 9, 2025, <<https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan>> (2025 年 7 月 17 日查詢)。

Regimes) 通常被解釋為原則、規範、規則及決策制定的過程。³ 其中規範可作為一種標準，形式亦可用法律方式來表現，因為規範多半是內生 (endogenous) 其中，會影響建制中的特別議題，作為依據藉此延伸解釋，假若行為者所採取的行動不符合規範，有時候也會使建制消散。⁴ 就此設定內部標準建構法律並因應各種問題產生應變措施，而監管性權力的概念就是在以法制工具為中心，透過監管來形塑 AI 發展的安全環境，其中先期風險管理就是要降低危險的產生。因此，何謂監管性權力、風險管理與 AI 韌性？以下試圖解釋與說明。

一、監管性權力

監管性權力的概念主要是透過法律約束設定規範並影響多方行為者，⁵ 此權力可使內部環境去風險化外，並希望擴散影響力，建構安全的發展環境。但要成為監管性權力的重要條件就是必須考量到監管方市場影響力，⁶ 即代表監管能力 (regulatory capacity) 是否足夠。所謂的監管能力代表規範制定方能否讓參與方遵守規則，其中市場大小會影響利益產出，當規範制定方市場規模大、

³ Stephen D. Krasner, *International Regimes* (Ithaca, NY: Cornell University Press, 1983), p. 1.

⁴ Stephen D. Krasner, *International Regimes*, pp. 16-17.

⁵ Andreas Goldthau & Nick Sitter, *A Liberal Actor in a Realist World: The European Union Regulatory State and the Global Political Economy of Energy* (New York: Oxford University Press), pp. 107-124.

⁶ Anu Bradford, "The EU as a Regulatory Power," In Mark Leonard eds., *Connectivity Wars: Why Migration, Finance and Trade are the Geo-Economic Battlegrounds of the Future* (London: European Council of Foreign Relations, 2016), pp. 133-139.

經濟動能強對企業會有引力，規範制定方也可擁有較大的話語權與掌控力；此外，監管目標必須在參與方有共識等狀態才會增強對外影響力，⁷ 因為制定規範可能會改變成本與利益分配。

若以歐盟為例，市場大小與制度特色會吸引規範方內部企業及個人、⁸ 外部行為者包含國家或非國家行為者等遵循，而市場自由度或內部利益團體所產生集體壓力，可能同樣會降低外部行為者遵守之意願。事實上，就市場大小來看，歐盟目前為全球經濟產值第二，⁹ 然而建立法規與制度的目的是希望維持單一市場並有共同標準，用以規範會員國，遵守法律維護市場秩序讓歐盟會員國可採取共同行動；反觀美國，目前為全球最大的經濟體，使用者與科技公司可因應多元解決方案並快速回應風險，其規範制定方也會依循市場趨勢來設定法規界線，就制度層面是較為彈性且可因應市場變化進行調整。¹⁰ 由此可見，歐、美雙方市場本

⁷ Penelope Canan and Nancy Reichman, “Ozone Partnerships, the Construction of Regulatory Communities, and the Future of Global Regulatory Power,” *Law & Policy*, Vol. 15, No. 1 (January 1993), pp. 61-74; Alasdair R. Young, “The European Union as a Global Regulator? Context and Comparison,” *Journal of European Public Policy*, Vol. 22, No. 9 (June 2015), pp. 1233-1252; Paul M. Schwartz, “Global Data Privacy: The EU Way,” *New York University Law Review*, Vol. 94, No. 771 (October 2019), pp. 771-818; Sandra Lavenex, Omar Serrano and Tim Buthe, “Power Transitions and the Rise of the Regulatory State: Global Market Governance in Flux,” *Regulation and Governance*, Vol. 15, No. 3 (May 2021), pp. 443-471.

⁸ 市場大小則是以國內生產毛額 (GDP) 為基礎，制度特色則是強調市場內部建立的規則與價值，如以市場自由為基礎或其內部有無明確法規可得遵循。

⁹ 根據國際貨幣基金組織 (IMF) 報告認為歐洲先進經濟體則僅限歐元區國家。

¹⁰ Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (New York: Oxford University Press, 2023), pp. 39-57.

身經濟動能與社會力量介入為影響市場平衡的重要因素。¹¹ 但由於監管性權力是運用規範來限制行動，雖然歐、美雙方市場大小僅在第一與第二大之差異，歐盟著重建立規範來傳遞本身價值，自然較美國而言內部控制力較強；美國目前雖採取最低限度的監管模式，但假若遭到大規模 AI 風險事件仍需要政府制定應對模式。¹²

基本上，監管性權力存在目的是為達成安全。法制工具的使用好比領土擴張 (territorial extension)，所以當法制向外延伸等同是將管轄範圍擴大。¹³ 監管的運用是將數位科技安全化，而這可以透過主動與被動兩種方式來實現。主動實踐安全是將「監管」當作數位轉型過程「去風險化」之工具；被動方式是因數位科技存有脆弱性 (vulnerability)，必須透過「監管」方式使其被動安全化 (securitization) 用於解決人類對科技發展未知性所產生的不安

¹¹ Chad Damro, “Market Power Europe: Exploring a Dynamic Conceptual Framework,” *Journal of European Public Policy*, Vol. 22, No. 9 (June 2015), pp. 1336-1354.

¹² 2020 年期間美國遭遇駭客攻擊事件，駭客透過植入木馬程式進入 SolarWinds 的 Orion 監管更新軟體當中，當客戶更新軟體時，則會受到損害。當時聯邦政府是 SolarWinds 的客戶，後來在 2020 年 12 月 13 日由美國國土安全部網路安全與基礎設施安全局 (Cybersecurity and Infrastructure Security Agency, CISA) 發布緊急命令。最後，12 月 16 日則由白宮國家安全委員會啟動了網路統一協調小組 (Cyber Unified Coordination Group, UCG)，該小組則負責國家情報總監辦公室、聯邦調查局以及 CISA 官員聯合合作降低損害。資料來源：<https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic?utm_source=chatgpt.com>。

¹³ Joanne Scott, “Extraterritoriality and Territorial Extension in EU Law,” *The American Journal of Comparative Law*, Vol. 62, No. 1 (April 2014), pp. 87-126.

全感。¹⁴ 監管性權力的出現其目的都是為達成「安全」途徑，用以降低發展過程中所產生不可預知的「風險」。

二、風險管理及 AI 韌性

（一）風險管理

世界各國開始針對 AI 進行相關規範與發展方案，包含 AI 快速發展對整體社會帶來隱憂，擔心無法辨識犯罪來源是真、是假外，侵害隱私權、道德等爭議甚囂塵上。歐洲刑警組織 (Europol) 認為 AI 自動生成影片、圖片，會造成更多孩童性暴力素材 (child sexual abuse material)，更難辨識「誰是受害者」與「誰又是犯罪者」。¹⁵ 因此，如何透過監管方式加強辨識數位轉型過程所遭遇的風險則為重要目標。

AI 系統存有風險若管控不當則可能有負面影響 (impacts)；就 AI 系統 (AI system) 定義是經由機器為運作基礎藉由資料輸入產生建議、預測或其他結果且可影響週邊環境。¹⁶ 根據國際標準化組織 (International Organization for Standardization，簡稱 ISO) 公布 ISO/IEC 42001 主要提供 AI 管理系統 (AI Management

¹⁴ Daniel Mugge, "The Securitization of the EU's Digital Tech Regulation," *Journal of European Public Policy*, Vol. 30, No. 7 (January 2023), pp. 1431-1446.

¹⁵ Europol, "Internet Organised Crime Threat Assessment," July 26, 2024, <<https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>> (2025 年 7 月 12 日查詢)。

¹⁶ OECD, "OECD Framework for the Classification of AI System," February 22, 2022, <https://www.oecd.org/en/publications/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en.html> (2025 年 7 月 19 日查詢)。

Systems，簡稱 AIMS）。¹⁷ 內容當中提到 AI 風險評估、AI 影響評估以及資料保護與 AI 安全等層面。¹⁸ 過程中，必須著重 AI 系統相關利害關係者 (stakeholder) 協調與溝通，¹⁹ 告知 AI 系統性風險來調節因應措施。

而美國國家標準與技術研究院 (National Institute of Standard and Technology，簡稱 NIST) 認為風險管理必須經由治理 (govern)、映射 (map)、測量 (measure) 與管理 (manage) 等步驟來進行。治理則是強調組織中對 AI 系統需要有風險管理認知及應對方案，而這是最重要的步驟。²⁰ 同時定義具可信任度的 AI 系統必須包含有效且可靠 (valid and reliable)、安全 (safe)、資安與韌性 (safety and resilience)、可歸責性與資訊透明度 (accountable and transparent)、可解釋性與詮釋性 (explainable and interpretable)、隱私保護 (privacy-enhanced)、公平性與有害偏見管理 (fair-with harmful bias managed) 等條件。²¹ 風險管理重要工作則是預先檢查與使用過程中用以偵測 AI 系統存在之風險。

¹⁷ ISO, “ISO/IEC 42001,” December 2023, <<https://www.iso.org/standard/42001#lifecycle>> (2025 年 9 月 17 日查詢)。

¹⁸ KPMG, “ISO/IEC 42001 Certification: The Global standard for AI Management Systems,” May 2025, <<https://kpmg.com/ch/en/insights/artificial-intelligence/iso-iec-42001.html>> (2025 年 9 月 17 日查詢)。

¹⁹ 利害關係者代表消費者、客戶和主管機關等 AI 系統使用者。

²⁰ NIST, “Artificial Intelligence Risk Management Framework, AI RMF 1.0,” January 26, 2023, <<https://www.nist.gov/itl/ai-risk-management-framework>> (2025 年 7 月 19 日查詢)。

²¹ *Ibid*, pp. 13-18.

（二）AI 韌性

當 AI 系統出現故障或錯誤資料輸入時，具有韌性則為風險管理的重要關鍵。韌性一詞最早是出現在 2007 年愛沙尼亞受到網路攻擊，引發歐盟與北大西洋公約組織（North Atlantic Treaty Organization，簡稱 NATO）的關注。²² 近年世界因新冠肺炎 (COVID-19) 疫情，各國在封鎖、解禁與疫後經濟復甦過程中，重新檢視工業 4.0 的影響。因 COVID-19 的關係導致各國大量推動產業智能化與數位化發展，雖有效降低時間及人力成本，但卻也因加速推動而面臨風險，如科技性失業、各國數位準備不足與技術落差、薪資所得差距拉大等，²³ 如何化解並產生因應措施則相當重要。

簡言之，所謂的韌性是有效應對變化，並從挑戰或困難中迅速恢復，以及承受壓力和災難的能力，²⁴ 這是在數位轉型階段必須存在的特質。因為韌性所產生的彈性不僅是回復原狀 (bounce back)，而是邁向新的狀態 (bounce forward)。²⁵ 目前全球都面臨數位轉型階段，AI 韌性更強調「當自動化系統依據人類所定義目標而生成內容、預測、建議或決策，但若遭遇硬體故障影響正常執

²² NATO Strategic Communications Centre of Excellence, “Hybrid Threats: 2007 cyber attacks on Estonia,” June 6, 2019, <<https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>> (2025 年 12 月 7 日查詢)。

²³ 張鴻，〈工業 5.0 與亞太區域產業及社會永續發展的契機〉，《臺灣經濟研究月刊》，第 46 卷第 2 期（2023 年 2 月），頁 21-28。

²⁴ Dawn J. Wright, “Toward a Digital Resilience,” *Elementa Science of the Anthropocene*, (February 2016), pp. 1-9.

²⁵ Yi-Hui Lee, Chih-Yuan Chou and Hsin-Lu Chang, “Building digital resilience against crises: The case of Taiwan’s COVID-19 pandemic management,” *Information System Journal*, Vol. 34, No. 1 (January 2024), pp. 39-79.

行時，其利害關係者是可以接受降低服務層級並需要有迅速反應與回復的能力。」²⁶ 藉此風險管理的流程是可以透過風險評估、風險辨識與回應等措施來降低 AI 系統不當影響並進而增強應對措施之彈性。

參、EU AI Act 的發展與效應

AI 因牽涉到公民隱私權、社會公平價值與演算法透明性等問題，而歐盟以維護人類基本價值為核心，首重道德規範作為 EU AI Act 的核心價值。²⁷ 因此，2018 年 5 月 25 日歐盟執委會提出「AI 戰略」，並在 12 月公布「可信賴 AI 倫理準則草案」(Ethics Guidelines for Trustworthy AI)，於 2019 年 4 月 8 日正式公開該準則。²⁸ 而可信任的 AI 須具備三項要素：法律性 (lawful)、道德性 (ethical)、堅韌性 (robust)，須在完善法律與規範狀態下，秉持尊重道德與價值全面考量到整體社會環境等情況，引領 AI 發展走向正面軌道。

2020 年歐盟執委會提出《人工智慧白皮書》(White Paper on AI)，建構全面 AI 法規，並採取風險分類途徑 (risk-approached)，以降低未來高風險 AI 系統帶來對個人或其他法律實體之影響。²⁹

²⁶ ISO, “ISO 22989,” July 2, 2022, <<https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:ed-1:v1:en>> (2025 年 7 月 19 日查詢)。

²⁷ 洪德欽，〈歐盟有關人工智慧的倫理指引與法律規範〉，王震宇主編，《數位貿易政策與資訊科技法律》(台北：五南圖書，2022 年)，頁 1-34。

²⁸ European Commission, “Ethics Guidelines for Trustworthy AI,” April 8, 2019, <<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>> (2025 年 7 月 12 日查詢)。

²⁹ European Commission, “White Paper on Artificial Intelligence: a European

2021 年 4 月 21 日當 EU AI Act 草案正式出爐，如先前白皮書中的風險途徑與漸進去風險化 AI 系統為發展方向，並於 2024 年 8 月 1 日正式生效；此法律的提出代表歐盟希望運用監管方式來降低風險。

就風險管理從 EU AI Act 內容當中，是將風險途徑先區分 AI 系統為絕對禁止或不可接受風險 (unacceptable risk)、高風險 (high-risk)、有限風險 (limited-risk)、最小風險 (minimal risk)，最主要形成歐盟內 AI 系統具有危險性則是絕對禁止、不可接受風險與高風險系統。因絕對禁止風險會侵害到部分特定族群，如發聲玩具可能會鼓勵孩童進行危險動作或系統依據行為、社經地位及個人性格等條件進行社會評分並建立分級制度，³⁰ 可能會造成侵害人權之行徑，而不透明決策過程與資料可信度則演變為 AI 系統中備受質疑之處。2025 年 2 月 2 日開始適用 EU AI Act 當中絕對禁止風險 AI 系統期，而《通用 AI 實踐守則》(General-Purpose AI Code of Practice)（以下簡稱《實踐守則》）已於 2025 年 7 月 10 日正式公布，作為 EU AI Act 先行指引。³¹

approach to excellence and trust,” February 19, 2020, <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>（2025 年 7 月 12 查詢）。

³⁰ European Parliament, “EU AI Act: first regulation on artificial intelligence,” February 19, 2025, <<https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4>>（2025 年 7 月 12 查詢）。

³¹ 主要是規範通用一般 AI 模型；所謂的通用一般 AI 模型，是指運用大量資料進行訓練的 AI 模型，而該模型可以廣泛執行不同任務並整合到各種接收系統或應用程式中。

現階段外部效應來看，EU AI Act 對進入歐洲市場的跨國企業採取自願簽署加入，但可分為兩個時間點來觀察：第一時間點為 2024 年 8 月 1 日正式生效後，歐盟執委會推動《AI 協議》(AI Pact)，主要依據高風險系統在 EU AI Act 調適期階段並協助利益關係者進入準備期，所以處於諮詢意見期間。《AI 協議》當中囊括兩項支柱：網路公開徵詢意見、企業自願加入。第一項支柱由 AI 辦公室在網路組織一般企業、非營利組織、學術界及公部門等參與者提供運作 EU AI Act 之建議；第二項支柱則是鼓勵企業自願參與，為 EU AI Act 當中減緩高風險系統之要求儘早做好實施準備。根據歐盟執委會公布名單中，自願加入的企業約莫有 230 家，包含 Google、OpenAI、Airbus、Cisco、IBM 等企業。³² 此階段採自願加入，是徵求 EU AI Act 運行前向各公、私團體進行意見諮詢與同意。

然而，第二個時間點為 2025 年 7 月 10 日由歐盟執委會公布的《實踐守則》，內容原則聚焦在資安行為、著作權與透明度三項準則。由 AI 辦公室訂立這三項原則，其中資安行為是在 EU AI Act 第 55 條當中，納入風險評估與風險減緩措施（如圖 1）；著作權行為必須遵守歐盟著作權等相關指令 (Directive 2019/790) 之內容，³³ 對網路使用內容必須尊重歐盟著作權法；透明度章節

³² European Commission, “AI Pact,” October 3, 2025, <<https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-Signatories-of-the-AI-Pact>> (2026 年 1 月 7 日查詢)。

³³ 歐盟於 2019 年 6 月 7 日通過數位單一市場著作權指令，主要內容為因應數位及跨境環境之權利限制與例外，其中內容包含資料探勘、教學活動、文化遺產保存等項目，另外，關於優化授權實務及著作利用等相關規定，亦在其中。

當中提供「模型文件說明表單」協助開發者提供完整資料與模型用途設計等資訊提供。然而，就 Meta 表明拒絕簽署此項《實踐守則》，³⁴ 而 OpenAI、Google、IBM、Microsoft 等 28 家公司簽署並願意承擔相關責任；通常企業不願意簽署，是因認為 EU AI Act 已為正式生效的法律，《實踐守則》多重疊加恐會造成模型開發者額外責任與義務，進而增加法律的不確定性，此外企業認為過度監管會阻礙 AI 模型的創新發展，讓 AI 技術研發及競爭力降低，並會暴露商業機密和技術細節等影響。而企業願意簽署則為增強在歐洲市場的影響力，可以順利佈局歐洲擴展企業版圖。³⁵ 但假若供應 / 開發商 (provider) 未簽署事前自願協議的話，歐盟執委會則依據 EU AI Act 第 91 條要求供應 / 開發商提供檔案與資料並依據第 92 條評估風險性，系統若為高風險性則會遭受行政罰鍰約全球營收 7% 或是 3,500 萬歐元，³⁶ 因此受到 AI 辦公室等監

³⁴ Meta 全球事務執行長 Joel Kaplan 在 LinkedIn 言明歐盟 AI 政策正走向錯誤的方向，資料來源：<<https://www.linkedin.com/news/story/meta-refuses-to-sign-eus-ai-code-6459708/>>。

³⁵ Google 宣布 2026 年至 2029 年期間將在德國投資 55 億歐元建立新的資料中心在 Dietzenbach，擴建黑森州漢諾 (Hanau) 資料中心，並擴充柏林、法蘭克福與慕尼黑辦公室，Google 在德國的雲端將會提供進一步高科技 AI 服務，其中包括整合 Gemini 模型的 Vertex AI 平台，資料來源：<<https://www.googlecloudpresscorner.com/2025-11-11-Google-Announces-EUR5-5-Billion-Investment-in-Germany,-including-AI-Infrastructure,-through-2029>>。Open AI 則是在 2025 年 5 月啟動國家合作計畫，並持續推進歐洲 AI 基礎建設—其中包含資料中心、教育學習、提供公共服務等內容，資料來源：<https://openai.com/global-affairs/eu-code-of-practice/?utm_source=chatgpt.com>。

³⁶ European Commission, "Communication-Approval of the content of the draft Communication from the Commission – Guidelines on the scope of the obligations for general-purpose AI models," July 18, 2025, <<https://digital->

管力道會更大。

目前為止，因 EU AI Act 仍持續推行中，外部效應主要是針對跨國科技公司，這部分是採取自願性質，未來是否會引發更多企業遵守，尚待時間觀察。

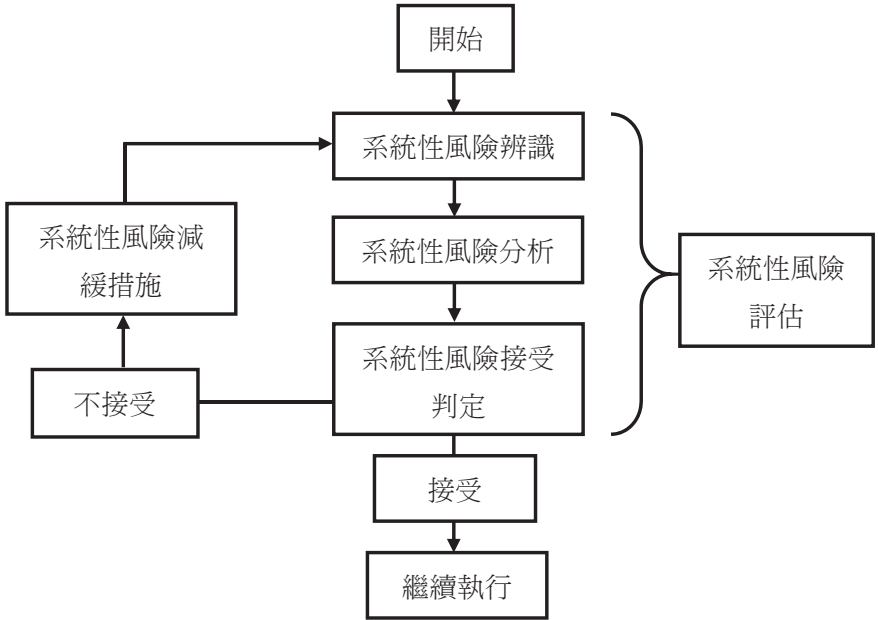


圖 1：系統風險評估與減緩過程

資料來源：European Commission, “Code of Practice for General-Purpose AI Models-Safety and Security Chapter,” July 10, 2025, <<https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>>（2025 年 7 月 20 日查詢）。

就內部效應來看，目前是 EU AI Act 初步實踐階段，必須藉由相關監管機構來督促各會員國。EU AI Act 的監管機構主要由歐

[strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act](https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act)>（2025 年 7 月 20 日查詢）。

洲資料保護監督機構（The European Data Protection Supervisor，以下簡稱 EDPS）、AI 辦公室與 AI 委員會；EDPS 可對違反 EU AI Act 的歐盟組織等機關處以行政罰鍰，並對市場違反資料保護、隱私權、競爭法或智慧財產權等內部組織進行監督；AI 辦公室則是協助 EU AI Act 可以在各會員國內部落實，並結合廣泛專家社群因應相關條文內容推動實施細則以有效實踐 AI 去風險化途徑（如圖 2）；AI 委員會則是擔任 AI 治理角色，協調各會員國內監管機構與合作資訊，擔任各會員國監管機構間的政府間論壇；歐盟會員國內部必須成立相關監管機構，監督各國內部市場的運作。然而，整體來說主要負責監管單位為 AI 辦公室。該辦公室將會協助 27 個會員國在執法方面合作，包括提供通用人工智慧模型發展與風險評估報告、調查違規行為、為供應商制定實踐守則、提供建議給會員國建立 AI 監管沙盒等相關工作，因此該部門將會負責整體歐盟 AI 政策與監督走向。

此外，為避免過度監管導致中、小企業創新與發展受限，歐盟執委會決定給予財政支持 40 億歐元到 2027 年，³⁷ 而中小企業提供的 AI 系統可獲得監管沙盒優先使用權，減輕中小企業測試的負擔，³⁸ 希望在控管風險與安全之間兼顧歐盟創新發展，並增強社會韌性以因應未來數位科技之發展。

³⁷ European Commission, “Commission Launches AI Innovation Package to Support Artificial Intelligence Startups and SMEs,” January 24, 2024, <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383> (2025 年 7 月 13 日查詢)。

³⁸ 黃國寶、張凱鑫，〈影響全球 AI！歐盟 AI 法案的「沙盒」如何運作？〉，《遠見雜誌》，2024 年 12 月 19 日，<<https://www.gvm.com.tw/article/117909>> (2025 年 7 月 13 查詢)。

當歐盟內會員國若遭遇因 AI 而形成風險事件並涉及歐盟法律之效力及解釋問題，各會員國地方法院向歐盟法院 (Court of Justice of the European Union) 要求先決裁示 (preliminary rulings)。就 2024 年至今已有三個案例申請，其中來自於保加利亞電信業者費率自動化系統、³⁹ 波蘭隨機案件分配系統、⁴⁰ 匈牙利新聞入口網站出版商及營運管理者之著作權法保護爭議。⁴¹ 這三起案件，

³⁹ 案件編號：C-806/24，提出時間為 2024 年 11 月 25 日並於 2025 年 7 月 2 日正式申請。主要爭議為原告電信業者 (Yettel Bulgaria EAD) 控訴消費者未支付月租費與契約終止，而消費者主張帳單是由 AI 驅動的自動化系統生成，缺乏透明度，導致無法核實收費是否正確。此問題涉及到 EU AI Act 第 86 條是否可適用於此類消費契約、消費者是否有權要求取得自動化系統的演算法或參數說明、法院是否可要求開發者交出 AI 模型技術資訊等內容。

⁴⁰ 案件編號：C-159/25，提出時間為 2025 年 2 月 26 日並於 2025 年 6 月 6 日正式申請。主要爭議點為案件背景涉及兩起商業交易中延遲付款的訴訟，而這兩起案件都是透過波蘭司法部開發隨機分配案件系統 (Random Case Allocation System，以下簡稱 SLPS) 而引起爭議；因原審法官審理案件 100 件，被行政單位調離法庭，透過 SLPS 隨機指派新法官接續審理。然而，案件分配嚴重不均，新法官接手 56 件，其餘法官案件量極少，導致當事人無法在期限內即時提出司法救濟。涉及爭議點在 SLPS 屬於一種自動化決策工具，未能公開演算法細節，是否會對形成司法獨立性與公正性潛在威脅。同時，若從 EU AI Act 當中若用於司法體系當中屬於高風險系統，是否應該受到更嚴格的規範等爭議。

⁴¹ 案件編號：C-250/25，申請日 2025 年 4 月 3 日，主要爭議原告 Like Company 為匈牙利新聞入口網站 (news portals) 的出版商與營運管理者控告 Google Ireland Ltd.，爭議內容為原告經營新聞網站靠廣告收入維生，其文章受著作權保護，而 Google 提供的大型語言模型 (Large Language Model) 聊天機器人 Gemini (前稱 Bard) 在回應中呈現部分與原告新聞網站內容裡相同的文字摘要，認為侵犯到歐盟與匈牙利法律下的重製權與公開傳輸權，從此案件雖未直接涉及 EU AI Act 相關條文，但卻涉及生成式 AI 對新聞著作內容的使用與重製權，其中涉及近期發布的《通用 AI 實踐守則》三項原則有所關聯。

其中兩起案件都是針對 AI 系統中的自動決策系統「不透明性」產生爭議，顯見 AI 系統在結果產出過程中，確實造成使用者等疑慮。此外，反應出 EU AI Act 已引起會員國內部的重視。

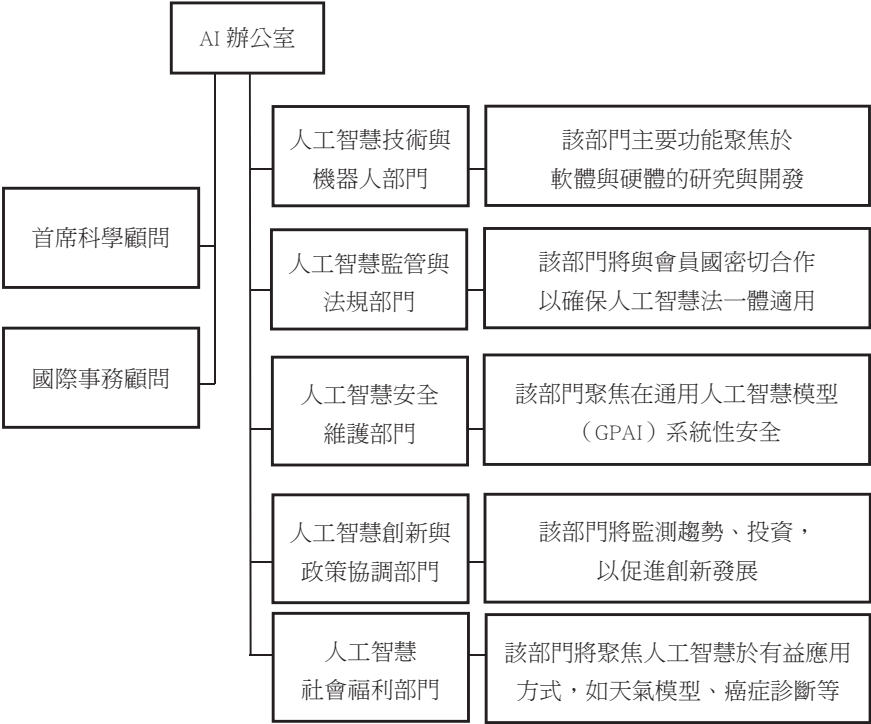


圖 2：歐盟 AI 辦公室的結構圖

資料來源：European Commission, “European AI Office,” June 12, 2025, <<https://digital-strategy.ec.europa.eu/en/policies/ai-office>> (2025 年 7 月 21 日查詢)。美國對人工智慧規範發展與效應

肆、美國對人工智慧規範發展與效應

2023 年 10 月 30 日美國前總統拜登簽署行政命令第 14110 號《安全、可靠且值得信賴的人工智慧使用與開發》(Safe, Secure,

and Trustworthy Development and Use of Artificial Intelligence)，主要目的就是希望在國會立法前先以行政命令建構安全且具信任度的 AI。前拜登政府時期的立場，認為 AI 的快速發展雖對整體社會經濟、公民有利，但可能在無意識的狀態下侵害到人權，建立風險管理 (risk-management) 機制則會確保 AI 發展的可靠性。⁴² 川普總統上任後廢除前政府的行政命令，並推出新的行政命令第 14148 號、第 14177 號、第 14179 號，此外，美國白宮預算管理局 (Office of Management and Budget，簡稱 OMB) 推出兩項備忘錄 M-25-21 及 M-25-22，主張以 AI 創新為理念，加速美國 AI 發展。

然而，其中行政命令第 14148 號則是撤銷前政府行政命令 14110 號，其後在 1 月 23 日發布行政命令第 14177 號旨在重建「總統科學與技術顧問委員會」(President's Council of Advisors on Science and Technology)，成員共 24 位專業包含 AI 及加密貨幣顧問，提供科技與教育政策等相關建議。⁴³ 而行政命令第 14179 號則主要目的是移除一切 AI 發展的障礙，並在 180 天之內發展《美國 AI 行動計畫》，而 2025 年 7 月 23 日川普總統也正式公布該行動計畫。

就外部效應來看，川普極力消除一切對 AI 發展的障礙。美國現階段監管法規以州政府為例，內容以保障民眾基本權利防範

⁴² Bureau of Cyberspace and Digital Policy, "Risk Management Profile for Artificial Intelligence and Human Rights," U.S. Department of State, July 26, 2024, <<https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/>> (2025 年 7 月 12 日查詢)。

⁴³ Federal Register, "Executive Order 14177," January 23, 2025, <<https://www.federalregister.gov/documents/2025/01/31/2025-02121/presidents-council-of-advisors-on-science-and-technology>> (2025 年 7 月 21 日查詢)。

未來犯罪情事的發生。立法主要內容包含針對高風險系統監管與辨識、⁴⁴ 建立 AI 立法工作小組、深偽 (deepfake) 技術影音合成品、兒童性犯罪素材、政治廣告、維護民眾基本權利等相關 AI 立法（如表 1）。就美國部分州 AI 監管法案當中包含刑事與民事責任，用以懲罰不當使用者。同時，也針對特別族群與個別行業來界定使用規範，如維吉尼亞州 (Virginia) 規範 AI 輔助系統在刑事司法決策過程其法官擁有最終主導權、猶他州 (Utah) 以生成式 AI 為基礎聊天機器人跟使用者知情權等內容。

然而川普所公布《美國 AI 行動計畫》，以三大支柱作為核心：支柱一、加速 AI 創新；支柱二、建構美國 AI 基礎建設；支柱三、國際 AI 外交與安全。內容中強調要求各聯邦機構檢視現有法規撤銷阻礙創新的條款，同時，在資金補助時必須考量到各州 AI 監管強度，減少資金流向過度管制的州。⁴⁵ 2025 年 12 月 11 日川普簽署行政命令將建立全國層級 AI 政策框架，若部分州法案衝突到聯邦 AI 政策框架應以聯邦先行。

總體來說，目前聯邦政府希望美國各州減少不必要監管，但州級 AI 法律部分範圍仍可先行，包含兒童安全保護、AI 演算與資料中心基礎設施、州政府對 AI 採購與使用及其他經另行認定等事項。部分州 AI 監管法設置目的為保障因演算法歧視、隱私權侵害、工作權剝奪等基本權利，同時，適度揭露 AI 系統使

⁴⁴ 所謂的高風險系統定義則是佈置後作出關鍵決策或在關鍵決策中起到任何作用的 AI 系統。

⁴⁵ The White House, “White House Unveils America’s AI Action Plan,” July 23, 2025, <<https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/>>（2025 年 9 月 17 日查詢）。

用，可降低民眾使用過程中因不知情而遭受損害情況。監管 AI 系統乃是為降低不法情事的發生，並強化社會使用 AI 之韌性。如美國財政部下的金融犯罪執法局 (Financial Crimes Enforcement Network) 曾發出警示強調使用 deepfake 新型犯罪是透過生成式 AI 製造假資料、照片與影像等技術使金融詐騙案例增生。⁴⁶ 若透過制定法律降低 AI 不當運用，應可減少犯罪，這也是美國具有有限度之監管模式。

表 1：美國部分州通過或生效之 AI 監管法案 (2024-2025)

類別	州 (法案編號)
高風險系統定義	Colorado (SB205)、 ⁴⁷ Kentucky (SB4)
建立 AI 工作小組或相關部門	Alaska (HCR3)、Kentucky (SB4)、Maryland (HB956)、Texas (SB2818)、West Virginia (HB3187)
AI 模型開發者內部吹哨者機制	California (SB53)
嚴禁使用部分國家的 AI 系統	Kansas (HB2313) ⁴⁸

⁴⁶ Financial Crimes Enforcement Network, *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions*, November 13, 2024, <https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial?utm_source=chatgpt.com> (2025 年 12 月 2 日查詢)。

⁴⁷ Colorado 的 Consumer Protection for Artificial Intelligence 是於 2024 年 5 月 17 日簽署，並於 2026 年 2 月 1 日生效。

⁴⁸ 遭到禁止的國家包括中華人民共和國、古巴、伊朗、北韓、俄羅斯、委內瑞拉。

防止 AI 生成式深偽 (deepfake) 影像性犯罪事	Arizona (SB1462)、Colorado (SB25)、 ⁴⁹ Montana (HB514)、 ⁵⁰ Oklahoma (HB1364)、
件、惡意散佈、不當使用等目的	Texas (SB441)、West Virginia (SB198)、New Hampshire (HB1432) ⁵¹
兒童性犯罪素材	Arkansas (HB1877)、Kansas (SB186)、Montana (HB82)、 ⁵² Nevada (SB263)、Texas (HB581、SB1621、SB20)、West Virginia (SB198)
使用在政治廣告或選舉等活動，誤導選民	Florida (HB919)、 ⁵³ Kentucky (SB4)、 ⁵⁴ Montana (SB25)、South Dakota (SB164)
保障民眾基本權益	Arkansas (HB1876)、Maryland (HB820)、Texas (SB1964)、Utah (SB271)
保護個別族群	Tennessee (ELVIS Act) ⁵⁵

⁴⁹ 生成式 AI 描繪被描述者的私密身體部位或被描述者性行為等內容，被描述者因為經同意被公開或遭致威脅而受到傷害。無論被披露之個人是否同意、此一行為而導致嚴重情緒困擾與可識別此人身份等狀態，原告可以收回被告所賺取金錢收益，或 15 萬美金獲得損害賠償。

⁵⁰ 修訂《通訊隱私犯罪條款》，擴大對數位性影像勒索與深偽 (deepfake) 淫穢內容的刑事處罰。

⁵¹ 使用深偽 (deepfake) 並用於故意製造、散佈或呈現相關內容，其目的是為使當事人名譽或金錢受損，受害人可提起民事訴訟。

⁵² 主要是誘導兒童性交易或性侵害，包含使用 AI 製成圖片等相關內容且無法清晰明辨是否為孩童等狀態。

⁵³ 關於 AI 生成的政治廣告必須強制揭露，同時，生成的影像、圖片等若有誤導選民或傷害某位候選人，都可以向佛羅里達選舉委員會提出申訴或調查。

⁵⁴ 與高風險系統定義同一法案 (SB4)，內含防止 AI 生成不實音訊或影像影響選舉結果與公眾觀感。

⁵⁵ 全名為 Ensuring Likeness, Voice, and Image Security Act，保護個人姓名、肖像、聲音與形象等具識別性特徵不遭他人未經授權用於商業用途，特別透過 AI 技術仿效所形成之濫用風險。

AI 互動之揭露義務	California (SB243)、 ⁵⁶ Maine (HB1727)、 ⁵⁷ Utah (SB226、HB452、SB149 ⁵⁸)
AI 輔助系統在刑事司法決策過程中，人類主導最終主導權	Virginia (HB1642)
自動化決策工具	New York (SB S7543B、SB S822)
未成年被逮捕者禁止使用 AI 或以其他方式製作的虛假證據	Virginia (HB2692)

資料來源：本資料表為作者蒐集，主要資料來源為 <<https://legiscan.com>>，這是全美各州立法追蹤網站，並提供原始出處。目前此表格內容則是以公開資料中可獲取最完整為主。

就內部效應來看，雖然川普總統所頒布行政命令第 14179 號是消除一切對於 AI 發展的障礙，⁵⁹ 不代表則會放棄風險管理。事實上，川普時期由 OMB 所發布的兩項備忘錄是基於過去拜登時期再推進 M-24-10、M-24-18 之內容，⁶⁰ 主要規範對象是行政機

⁵⁶ 針對伴侶機器人設限，包含 AI 平台不得提供治療或心理建議、與使用者展開未經協定自殺 / 自傷 / 心理健康建議對話、偵測情緒或心理狀態。

⁵⁷ 這項法案禁止個人使用能模擬人類對話與互動的軟體應用程式，並在以下情況該互動可能會誤導或欺騙消費者以為自己是在與人類互動。

⁵⁸ 2024 年 5 月 1 日生效，該法案明確規定若公司使用 AI 工具與客戶進行互動時，必須具有揭露責任。本法案原先僅為試驗法條，應於 2025 年 5 月 1 日失效。而 2025 年 3 月 25 日，通過法案再延長為兩年有效至 2027 年 7 月 1 日。

⁵⁹ 行政命令內容談到，執行過程會受到既有法律框架與預算授權所限制；總統所簽訂的行政命令雖具有強制執行力，但還是必須看是否有抵觸現有法律與憲法為基礎。

⁶⁰ M-24-10 內容主要是依據先前拜登政府所公布行政命令第 14110 號當中

關。當中 M-25-21 採取最低風險管理，若涉及對個人或社群的權益、機會及安全具有高影響性 (high-impact) AI 系統，則優先考慮使用較為安全 AI 產品。同時，川普總統行政命令當中強調持續推進 AI 創新，在聯邦各機關首長必須任命或指派「首席 AI 官員」（Chief of AI Officer，以下簡稱 CAIO），此官員將與機關內相關權責官員進行合作，⁶¹ 從內部規定當中，強調以最低管制風險方式來使用 AI，使用前或過程中都必須持續進行風險評估。

各聯邦政府機構內所設的 CAIO，為高影響性 AI 是否使用的關鍵決策者。在落實風險管理與終止不合規的 AI，基本上在備忘錄發布後 365 天內各機關就必須完成最低風險管控措施，並在 OMB 年度定期審查，報告年度 AI 使用清單等內容，假若不符合相關安全性使用或無法減低風險時，則各機關首長可決定停止使用。⁶² 而機關內 CAIO 則是判斷 AI 系統經過風險評估後其適用性

針對 AI 系統風險管理模式，制定風險管理政策與實施準則、設立 AI 審查機制、建立減緩 AI 風險等相關措施，最遲在 2024 年 12 月 1 日前各機構必須採取 AI 系統清單與風險報告。此外，在 M-24-10 附件一當中則根據備忘錄第五部分建立使用此 AI 會對權利及安全產生影響之推定狀態。M-24-18 則是針對政府 AI 採購政策，其中必須注意 AI 系統採購要可以跨部門使用與協調，同時，無論行政單位是自建、或者是從外部採購都必須符合 M-24-10 底下的風險管理等原則，注意隱私、安全、資料擁有等相互使用性，與其外部簽訂條約針對 AI 系統也必須依照 M-24-10 等風險管理規範來設定，可以讓政府單位或第三方單位來評估系統是否存有演算法歧視等風險。

⁶¹ The White House, “White House Releases New Policies on Federal Agency AI Use and Procurement,” April 7, 2025, <<https://www.whitehouse.gov/articles/2025/04/white-house-releases-new-policies-on-federal-agency-ai-use-and-procurement/>>（2025 年 12 月 5 日查詢）。

⁶² *Ibid.*

的主要關鍵者。

而何謂高影響性的 AI？從 M-25-21 內容當中提到，若 AI 產生或提供基礎原則及行動涉及法律、約束人身自由或其他明顯反應下列情形：1. 涉及個人或實體公民權利、自由或隱私；2. 涉及個人或實體獲得教育、保險、信貸、雇用或其他項目的機會；3. 涉及個人或實體獲得關鍵政策支援或服務；4. 人類健康與安全；5. 涉及重要基礎建設或公共安全；6. 戰略資產或資源，包括高價值財產及被聯邦政府標記為敏感或機密資訊等內容。⁶³

目前最低風險管控僅限於高影響性 AI 產品，如果要使用則是必須要先進行事前風險評估外並完成 AI 影響力評估，包含對 AI 預期目的與收益、模型能力品質與適當性、運用資料是否會涉及侵害公眾權利，過程中依舊需要定期進行相關評估與測試、成本分析等步驟，才得以使用高影響性 AI，並持續監控以防後續產生不良影響或負面結果，步驟可參考圖 3。



圖 3：最低風險管控措施與過程

資料來源：作者自製

而這份備忘錄中，提供高影響性 AI 類別，以及所產生之結果會造成不良影響與負面結果等行為標準（如表 2）。事實上，

⁶³ The White House, “Accelerating Federal Use of AI through Innovation, Governance, and Public Trust,” April 7, 2025, p. 19, <<https://www.whitehouse.gov/articles/2025/04/white-house-releases-new-policies-on-federal-agency-ai-use-and-procurement/>>（2025 年 7 月 22 日查詢）。

這份清單並非是全部高影響性 AI 而只是部分，內容僅為預測若不當使用會對公眾產生的嚴重影響。這兩份備忘錄都是依循前拜登政府所發布對 AI 行政命令，因此，依舊有風險評估等管理措施在其中，並會因應不同事件來進行相對回應則可增強政府應對危機之韌性。

表 2：預估使用高影響性 AI 影響之層面

使用類別	產生影響
關鍵基礎設施或政府設施	緊急服務、火災或生命安全系統、食物安全機制、交通控制系統或其他實際控制運輸之系統
機器人、機器運作等產品	無論此產品在陸、海、空中或地底下，或工業裝置會對人類形成明顯的傷害
武器運用	攻擊或防禦等相關行為會對人類造成嚴重傷害
化學物品或生物製劑	運用在此種物品的運輸、安全、開發、設計或使用
系統測試或公共基礎設施	假如出現問題時，對公共安全會造成極大傷害
醫療	運用在患者診斷、風險評估、治療或公共保險、健保成本的控制
政府設施	進出入口的控制與安全設施
貨物進、出口	投資、航運制裁或相關貿易限制
言論	阻止、移除等保護言論之限制
執法	辨識犯罪嫌疑人；預測犯罪；公共場所跟蹤車輛；應用生物辨識；面部重建；社交媒體監控；數位取證技術；網路入侵；個人定位監控或跟蹤；檢測武器或暴力活動；累犯、判刑、假釋、監督釋放、緩刑、保釋、審前釋放或審前拘留有關之司法決定等
移民、庇護、拘留等出入境美國資訊	準備、裁決與尋求臨時或永久進入美國及其領土的外國國民有關之風險評估

生物辨識系統	在公共場所使用生物辨識系統
社會福利	申請社會福利，包括貸款或獲得公共住房等權利
僱傭關係	就業前篩選、薪資或晉升、工作績效管理、招聘或解僱、工作紀律處分；將員工重新分派任務或至新團隊
語言翻譯	當回覆具有法律約束力或可直接提供資訊並影響行政機構決定及行動

資料來源：作者自製

然而 M-25-22 當中與過去不同的地方則是禁止供應商在未經機構明確同意下，對非公開政府資料進行商業模型培訓，因這會涉及到智慧財產權。同時，現今政府採購則是希望敦促各機關最大限度使用「美國製造 AI」。⁶⁴

伍、結論與建議

一、結論

本文以監管性權力、風險管理與 AI 韌性來理解歐盟、美國現階段 AI 規範；歐盟本就秉持較為嚴苛的管制方式來監督 AI，用以降低不法情事發生，而美國則是施以鬆綁法規來面對 AI 發展。但事實上，歐盟透過監管的方式形塑安全環境，以建立未來 AI 永續發展，而美國則先以發展為目標，讓美國強大並成為 AI 龍頭後，最終依舊會運用法律來限制。目前川普總統雖然透過行動計畫明示各州不得過度監管，並透過新的行政命令嚴格執行，然而若 AI 系統不當使用，包含生成式圖片或影片侵害到兒童等

⁶⁴ Brooker Tanner, “New OMB Memo Signal Continuity in Federal AI Policy,” May 8, 2025, <<https://www.brookings.edu/articles/new-omb-memos-signal-continuity-in-federal-ai-policy/>> (2025 年 7 月 22 日查詢)。

權益時，政府適度運用法律監管仍為必要措施，這是一種保護方式。監管性權力看似是將國家權力往內限縮，實質上運用法律來框限管制範圍，這為有限度的管轄模式。至此，管轄過程才會考量中小企業的 AI 創新，並適度保持自由空間以讓中小企業可以充分發展。

而有限程度的管轄可降低發生不法情事；就歐盟針對 AI 系統制定法律內容雖鉅細靡遺，但這卻也明確管轄範圍。此種作法或產生減緩企業 AI 發展之隱憂；然目前以丹麥 (27.58%)、瑞典 (25.09%)、比利時 (24.71%) 企業在 AI 應用程度較為普及（如圖 4），⁶⁵ 雖離 2030 年設定目標 75% 仍有距離，但各國使用 AI 成長趨勢依舊也有緩步成長，不過因 EU AI Act 施行時間尚短仍須長期觀察。反觀美國強調降低監管力道，但假若 AI 引起的犯罪行為或侵害人權等問題依舊會立即因應，並因應法規來施以後續防制措施。⁶⁶ 歐盟以嚴格法律革除 AI 引起的風險並力圖建構永續發展環境，EU AI Act 只是歐盟數位政策的一部分。而美國在市場驅使下力圖 AI 發展，在面對國安層級 AI 運用依舊需要高規格安全防護，降低外來威脅。美國會因需求不同而有相異應對模式，這也顯示出是一種有限度的監管模式。

事實上，監管 AI 系統最主要影響仍為跨國公司與企業團體；但跨國公司與企業團體僅須因應法律或政策立即調整，其實際影

⁶⁵ European Commission, “DESI indicators,” June 16, 2025, <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2025&indicator=desi_ai&breakdown=ent_all_xfin&unit=pc_ent&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE>（2025 年 10 月 13 日查詢）。

⁶⁶ 但由於美國行政命令為概括性，致使因應與保護措施需要更明確建立。

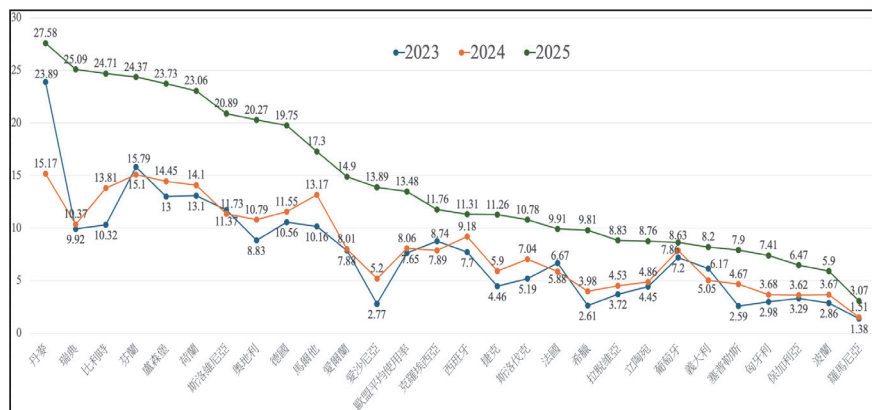


圖 4：歐盟會員國企業使用 AI 比例

資料來源：European Commission, “DESI indicators,” June 16, 2025, <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2025&indicator=desi_ai&breakdown=ent_all_xfin&unit=pc_ent&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE>（2025 年 12 月 7 日查詢）。

響範圍不大外，調整與變化方式快速，同時，跨國公司與企業團體彼此間則會相互仿效跟進，自然會強化國家監管性權力的擴散，並增強歐盟、美國在 AI 發展上的影響力，也會增強社會內部對應變危機所需的韌性。

此外，中、美兩國現爭奪 AI 國際規範的主導權，而中國 AI 規範亦是值得觀察面向。由於中國使用生成式 AI 用戶約佔 5.15 億人，使用者眾多其潛在風險隨之增加，包括換臉換聲虛構影像、版權侵權問題增生、學術濫用等影響。⁶⁷ 中國在 2023 年 7 月 10 日公布《生成式人工智能服務管理暫行辦法》，當中第 20 條提

⁶⁷ 中國互聯網絡信息中心，〈生成式人工智能應用發展報告（2025）〉，2025 年 10 月 23 日，<<https://www.cnnic.cn/n4/2025/1021/c88-11391.html>>（2026 年 1 月 6 日查詢）。

到若境外向境內用戶提供生成式 AI 服務者，都將列入中國國家互聯網信息辦公室（簡稱網信辦）的監管範圍。⁶⁸ 同時，2025 年 9 月推出《人工智能安全治理框架》2.0 版，其中包含過去技術內生、技術應用安全風險外，現將技術衍生安全風險如因 AI 導致社會和環境安全風險、倫理安全風險等內容新增其中，而風險級別也區分為低安全風險、一般安全風險、較大安全風險、重大安全風險與特別重大安全風險，⁶⁹ 其中重大安全風險與特別重大安全風險則必須加以防範與化解。有鑑於此，集結歐盟、美國甚至中國對 AI 規範的發展，預防不當使用 AI 致使風險發生已成未來之趨勢。

二、建議

近期我國《人工智慧基本法》（以下簡稱 AI 基本法）立法院三讀通過。⁷⁰ 就過去各版本《AI 基本法》草案當中條文說明，⁷¹

⁶⁸ 中國國家互聯網信息辦公室，〈生成式人工智能服務管理暫行辦法〉，2023 年 7 月 10 日，<https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm>（2026 年 1 月 7 日查詢）。

⁶⁹ 重大安全風險為具有重大威脅性和區域影響特徵，對國安安全、社會穩定和公民權益可能帶來嚴重影響，產生重大社會面危害；特別重大安全風險則為具有災難性和系統性威脅特徵，對國家安全、社會秩序和公民權益造成顛覆性或不可逆轉的特別嚴重影響。資料來源：<https://www.cac.gov.cn/2025-09/15/c_1759653448369123.htm>。

⁷⁰ 2025 年 12 月 23 日立法院三讀通過，於 2026 年 1 月 14 日公布。中央主管機關為國家科學及技術委員會，未來將負責國家 AI 戰略特別委員會之幕僚作業，數位發展部負責訂定風險分類框架、提供評估驗證工具以協助事業主管機關認定高風險應用及推動資料治理機制等內容。資料來源：<<https://www.nstc.gov.tw/folksonomy/detail/ed981806-1852-4b63-8dfd-9cea04157971?l=ch>>。

⁷¹ 過去各個版本《AI 基本法》草案除行政院推出版本外，亦包含原先國科會版本、外加上立法院當中各政黨及立委之提案做參考。

參考國家包含美國、歐盟、新加坡及 G7 廣島 AI 國際行動規範等條文。此目的與用意就是希望我國在《AI 基本法》通過後有著國際經驗作為背書，增添我國立法的實務性與多元性。通過《AI 基本法》條文內容當中基本原則，則與國際上現有 AI 規範原則相符。⁷²有鑑於此，綜合歐盟、美國兩方在面對 AI 的態度與經驗來看，提供下列觀點作為參考：

首先，風險分級制度必要性與明確性，幫助國內 AI 產業發展有所依歸。EU AI Act 風險分級包含絕對禁止及不可接受風險、高風險、有限風險或最小風險，細部化的設計有利於公、私部門可即早參照，我國可儘早設定符合國情的風險分級機制，有利於內部規範明確化，若有不符合法律定義者亦可即早改善。

就我國經驗來說，將交由數位發展部推動 AI 風險分類框架，各機關則會依此與需要訂定以風險為基礎之層級管理規範。我國應仔細思考國際標準其適用性外，風險分類框架內容則必須明確定義，或建立先行指導原則，讓一般企業得以明確了解不同風險層級所需要應對的措施。

其次，AI 治理須秉持以人為本之精神來推動，並強化國安層面 AI 應用之安全性；歐盟是權利導向的 AI 立法，而臺灣可參考歐盟的價值規範，著重於維護人類永續發展、降低對人權之侵害，可保障臺灣民眾內部工作權與發展權。此外，美國對 AI 發展雖採較為寬鬆的態度，但政府與國防部的 AI 應用仍須保障演算法

⁷² 包含 G7 廣島 AI 進程中《開發先進 AI 系統國際行為準則》(Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI System) 中的永續性原則、歐盟 2019 年可信賴 AI 倫理準則等相關內容。資料來源：<<https://futurecity.cw.com.tw/article/3909>>。

的安全、以及設計 AI 事件回應機制，這都是管控 AI 風險的方式，我國應可效法並強化國安層面 AI 應用的安全機制。

最後，風險評估機制的建立，可事前評估、定期更新並適時檢討；從《實踐守則》當中內容當中有系統性風險評估與減緩過程，亦如同美國公部門採用最低風險管控措施與過程作為參考，未來我國施以《AI 基本法》應儘早設立評估過程與標準，增強公部門在 AI 應用上的明確認知，亦可成為一般企業之參考。

AI 本為一種因人便利所產生的工具，然創新與監管本就是 AI 發展的雙面刃，我國必須思考應以何者為先。若以創新發展為目標，後續若有相關規範其監管嚴格程度必須調整，才能讓中、小企業得以自由發揮。若以監管為目標，其法律的明確性就必須更加清晰，並做好中、小型企業發展 AI 產業之配套措施，以提早進行去風險化的安全途徑。（投稿：2025 年 10 月 20 日；修訂：2025 年 11 月 28 日；接受：2025 年 12 月 9 日）

參考文獻

一、中文部分

(一) 專書論文

洪德欽，2022。〈歐盟有關人工智慧的倫理指引與法律規範〉，王震宇主編，《數位貿易政策與資訊科技法律》。臺北：五南圖書。頁 1-34。

(二) 期刊論文

張鴻，2023/2。〈工業 5.0 與亞太區域產業及社會永續發展的契機〉，《臺灣經濟研究月刊》，第 46 卷第 2 期，頁 21-28。

(三) 網際網路

中國國家互聯網信息辦公室，2023/7/10。〈生成式人工智能服務管理暫行辦法〉，<https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm>（2026 年 1 月 7 日查詢）。

中國互聯網絡信息中心，2025/10/23。〈生成式人工智能應用發展報告（2025）〉，<<https://www.cnnic.cn/n4/2025/1021/c88-11391.html>>（2026 年 1 月 6 日查詢）。

黃國寶、張凱鑫，2024/12。〈影響全球 AI！歐盟 AI 法案的「沙盒」如何運作？〉，《遠見雜誌》，<<https://www.gvm.com.tw/article/117909>>（2025 年 10 月 12 日查詢）。

二、英文部分

(一) 專書

Bradford, Anu, 2023. *Digital Empires: The Global Battle to Regulate Technology*. New York: Oxford University Press.

Goldthau, Andreas and Nick Sitter, 2015. *A Liberal Actor in a Realist World: The European Union Regulatory State and the Global Political Economy of Energy*. New York: Oxford University Press.

Krasner, Stephen D., 1983. *International Regimes*. Ithaca, NY: Cornell University Press.

(二) 專書論文

Bradford, Anu, 2016. “The EU as a Regulatory Power,” In Mark Leonard eds., *Connectivity Wars: Why Migration, Finance and Trade are the Geo-Economic Battlegrounds of the Future*. London: European Council of Foreign Relations. pp. 133-139.

(三) 期刊論文

Canan, Penelope and Nancy Reichman, 1993/1. “Ozone Partnerships, the Construction of Regulatory Communities, and the Future of Global Regulatory Power,” *Law & Policy*, Vol. 15, No. 1, pp. 61-74.

Damro, Chad, 2015/6. “Market Power Europe: Exploring a Dynamic Conceptual Framework,” *Journal of European Public Policy*, Vol. 22, No. 9, pp. 1336-1354.

- Lavenex, Sandra, Omar Serrano and Tim Buthe, 2021/5. “Power Transitions and the Rise of the Regulatory State: Global Market Governance in Flux,” *Regulation and Governance*, Vol. 15, No. 3, pp. 443-471.
- Lee, Yi-Hui, Chih-Yuan Chou and Hsin-Lu Chang, 2024/1. “Building Digital Resilience against Crises: The Case of Taiwan’s COVID-19 Pandemic Management,” *Information System Journal*, Vol. 34, No. 1, pp. 39-79.
- Mugge, Daniel, 2023/1. “The Securitization of the EU’s Digital Tech Regulation,” *Journal of European Public Policy*, Vol. 30, No. 7, pp. 1431-1446.
- Schwartz, Paul M., 2019/10. “Global Data Privacy: The EU Way,” *New York University Law Review*, Vol. 94, No. 771, pp. 771-818.
- Scott, Joanne, 2014/4. “Extraterritoriality and Territorial Extension in EU Law,” *The American Journal of Comparative Law*, Vol. 62, No. 1, pp. 87-126.
- Wright, Dawn J., 2016/2. “Toward a Digital Resilience,” *ELEMENTA*, pp. 1-9.
- Young, Alasdair R., 2015/6. “The European Union as a Global Regulator? Context and Comparison,” *Journal of European Public Policy*, Vol. 22, No. 9, pp. 1233-1252.

(四) 網際網路

- Bureau of Cyberspace and Digital Policy, 2024/7/26. “Risk Management Profile for Artificial Intelligence and Human Rights,” *U.S. Department of State*, <<https://2021-2025.state.gov/risk->

management-profile-for-ai-and-human-rights/>.

European Commission, 2019/4/8. “Ethics Guidelines for Trustworthy AI,” <<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>>.

European Commission, 2020/2/19. “White Paper on Artificial Intelligence: A European approach to excellence and trust,” <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>.

European Commission, 2024/1/24. “Commission Launches AI Innovation Package to Support Artificial Intelligence Startups and SMEs,” <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383>.

European Commission, 2024/7/2. “Report on the state of the Digital Decade 2024,” <<https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024>>.

European Commission, 2024/9/25. “AI Pact,” <<https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-Signatories-of-the-AI-Pact>>.

European Commission, 2025/4/9. “The AI Continent Action Plan,” <<https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan>>.

European Commission, 2025/6/12. “European AI Office,” <<https://digital-strategy.ec.europa.eu/en/policies/ai-office>>.

European Commission, 2025/6/18. “DESI indicators,” <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2025&indica-

tor=desi_ai&breakdown=ent_all_xfin&unit=pc_ent&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE>.

European Commission, 2025/7/18. “Communication-Approval of the content of the draft Communication from the Commission – Guidelines on the scope of the obligations for general-purpose AI models,” <<https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act>>.

European Parliament, 2025/2/19. “EU AI Act: first regulation on artificial intelligence,” <<https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4>>.

Europol, 2024/7/26. “Internet Organised Crime Threat Assessment,” <<https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-ioc-ta-2024>>.

Federal Register, 2025/1/23. “Executive Order 14177,” <<https://www.federalregister.gov/documents/2025/1/31/2025-2121/presidents-council-of-advisors-on-science-and-technology>>.

ISO, 2022/7/2. “ISO 22989,” <<https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:ed-1:v1:en>>.

ISO, 2023/12. “ISO/IEC 42001,” <<https://www.iso.org/standard/42001#lifecycle>>.

KPMG, 2025/5. “ISO/IEC 42001 Certification: The Global standard for AI Management Systems,” <<https://kpmg.com/ch/en/>>

insights/artificial-intelligence/iso-iec-42001.html>.

NATO Strategic Communications Centre of Excellence, 2019/6/6.

“Hybrid Threats: 2007 cyber attacks on Estonia,” <<https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>>.

NIST, 2023/1/26. “Artificial Intelligence Risk Management Framework, AI RMF 1.0,” <<https://www.nist.gov/itl/ai-risk-management-framework>>.

OECD, 2022/2/22. “OECD Framework for the Classification of AI System,” <https://www.oecd.org/en/publications/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en.html>.

Tanner, Brooker, 2025/5/8. “New OMB Memo Signal Continuity in Federal AI Policy,” <<https://www.brookings.edu/articles/new-omb-memos-signal-continuity-in-federal-ai-policy/>>.

The White House, 2025/4/7. “White House Releases New Policies on Federal Agency AI Use and Procurement,” <<https://www.whitehouse.gov/articles/2025/4/white-house-releases-new-policies-on-federal-agency-ai-use-and-procurement/>>.

The White House, 2025/7/23. “White House Unveils America’s AI Action Plan,” <<https://www.whitehouse.gov/articles/2025/7/white-house-unveils-americas-ai-action-plan/>>.

