Baker McKenzie.

July 2024

人工智慧基本法草案預告我國 AI 監管新紀元法

文/ 黃麗蓉 執行合夥律師 王碩勛 律師

背景

本文作成的 4 天前即 2024 年 7 月 15 日，我國國家科學與技術委員會（下稱「國科會」）在網路上預告臺灣的「人工智慧基本法草案」，標誌著臺灣在人工智慧（AI）法領域監管的新紀元。這是繼 2 個月前即 2024 年 5 月 12 日，歐盟正式通過「歐盟人工智慧法案」（EU Artificial Intelligence Act）成為全球首部全面監管人工智慧之法律後，對於我國 AI 發展有重要影響的法規變化。

AI 開啟種種的法規環境影響評估

自從各種 AI 技術相繼問世後，全球各主要國家、區域體紛紛制定相關法規以應對其帶來的挑戰與機遇，主要包括：

- 2019 年 5 月經濟合作暨發展組織（Organisation for Economic Cooperation and Development， OECD） 通過「人工智慧建議書」（OECD Recommendation on Artificial Intelligence）， 提出基本價值原則，並給予各國政策制訂者相關建議
- 同年歐盟發布「可信賴人工智慧倫理準則」（Ethics Guidelines for Trustworthy AI）， 確保 人工智慧發展所需之共同倫理原則
- 2021 年歐盟提出「人 工智慧法」（Artificial Intelligence Act）草案，2024 年通過審議
- 2022 年美國發布「AI 權利法案藍圖」（Blueprint for an AI Bill of Rights）、2023 年發布「發展與使用安全且可信任的 AI 行政命令」（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence）訂立聯邦各部門人工智慧發展之推動任務
- 2022 年加拿大提出「人工智慧資料法草案」（Artificial Intelligence and Data Act）

AI 將在氣候變遷、環境、醫療、金融、交通、內政、農業、公共服務等對人類產生廣泛影響，這也引領在上述各環節提供服務或製造生產的企業領導者面臨巨大的壓力，

可謂有關 AI 的應用及其對商業生態系統的影響等問題，已成為各企業董事會議程的首要議題，需要考慮的包括：

- 如何建置人工智慧公司治理模型
- 如何應用機器學習來增強員工的能力而不是取代他們
- 如何不陷入圍繞在智慧財產權、資料來源、監管與個資保護的法律雷區
- 如何平衡生成式 AI 的可能性與網路安全和著作權的風險

一言以蔽之，這是一場人工智慧帶來的環境影響評估，而這裡的環境，包含自然與非自然的環境，非自然的部分，就包含技術與法規環境，在跨國律所執行全球業務的筆者，正是要幫助我們的客戶能夠掌握不斷變化的法規，使他們能夠創造新的機會，而不是被動適應。

臺灣「AI 基本法草案」

臺灣的 AI 基本法草案於發布後目前開放為期 60 天之公眾諮詢。草案共計 18 條條文，旨在提升臺灣政府在 AI 研發及應用方面的能力。草案亦揭示了 7 大原則，這些原則與現有的國際 AI 規範和指導方針相似（草案第 3 條）：

1. 永續發展： AI 研發及應用需兼顧社會公平與環境永續。
2. 人類自主：AI 發展應尊重人類自主權及基本人權。
3. 隱私保護及資料治理：需遵守隱私保護及資料治理原則。
4. 資安與安全：在 AI 研發及應用過程中建立資安防護措施。
5. 透明與可解釋：對 AI 產出的資訊內容作適當的資訊揭露或標記，提升可信任度。
6. 公平不歧視：避免演算法產生偏差或歧視風險。
7. 問責：承擔相應的責任，包括內部治理及外部社會責任。

草案還要求數位發展部參考國際標準或規範，推動 AI 風險分類框架，並依此框架制定風險分類規範（草案第 10 條）。政府亦需依 AI 風險分級，通過各種機制來提升可信任的 AI 應用，並制定有關 AI 應用條件、責任、補救、賠償或保險的相關法規（草案第 12 條）。此外，草案亦明文政府須保障勞工權益，以避免勞工因 AI 之發展而受到不利影響（草案第 13 條）。

歐盟「人工智慧法案」

歐盟「人工智法案草案」訂於 2026 年實施。該法案將人工智慧當成一項商品進行管制，並採取風險基礎之監理模式（Risk-Based）。法案所揭示之內容與原則，不僅是我國企業從事全球商業行為時應遵循，料亦將在我國基本法之外的相關後續法規中，成為重要參考。重點如下：

1. 規範對象：只要是將人工智能系統投放在歐盟市場內、對歐盟內之人產生影響，不論是 AI 系統提供商、部署者、進出口商、製造商、亦無論其是否位於歐盟區域內，都受法案之效力所及。換言之，歐盟法案具有域外效力。

2. 明定監管機構：各成員國需設立或指定一個或多個監管機構，負責監督 AI 系統的合規性。而在歐盟層級，則設立歐洲人工智慧委員會，協調成員國的監管活動，確保法規在整個歐盟的一致性和有效性。

3. 依風險高低分層管制：採取風險基礎之監理模式，根據人工智慧系統的風險程度，將其分為四個等級：不可接受風險、高風險、有限風險和最小風險。風險越高之人工智慧系統受到之管制越嚴格：

   (1) 不可接受風險：例如社會信用評分系統、操縱行為的技術、即時遠端生物特徵識別系統，這類 AI 系統被認為對公眾安全和基本權利構成不可接受的威脅，故在歐盟範圍內被禁止使用。

(2) 高風險：需嚴格監管的 AI 系統，主要應用於關鍵領域，如醫療、交通、勞動、法律、金融等，需遵守風險管理、數據治理、記錄保存、透明度、監控和人類監督等合規要求。
(3) 有限風險：需遵守特定透明度義務的 AI 系統，例如與用戶直接互動的聊天機器人，要求告知用戶他們正在與 AI 系統互動。
(4) 最低風險：對低風險的 AI 系統進行最低限度的監管，例如垃圾郵件過濾器和 AI 驅動的遊戲，這些系統的開發者被鼓勵遵守自願行為準則。

4. 規範 AI 提供商之義務：AI 系統提供商需確保其系統符合法案要求。此外，提供商於 AI 系統投放於市場後，亦須持續進行上市後監控。

5. 將「通用型 AI」納管：因應各種生成式 AI 的問世，法案將「通用型 AI」納入管制，並區分為一般型與具系統風險型，並對二種不同類型之提供者課予不同之義務。

6. 主要監管原則：此部分主要是針對高風險 AI 而設，要求如下：

(1) 風險管理：高風險 AI 系統需實施全面的風險管理過程，從設計、開發到部署和使用，確保系統在所有階段都能有效識別和應對風險。
(2) 數據治理：高風險 AI 系統需確保使用的數據集是高質量的、相關的和代表性的，防止數據偏見和歧視。
(3) 技術文件：開發者需準備詳細的技術文件，說明 AI 系統的設計、開發和運行原理，確保系統透明可解釋。
(4) 監控和記錄保存：高風險 AI 系統需具備監控能力，並保存運行記錄，以便事後分析和改進系統。
(5) 透明度和告知義務：用戶需被告知他們正在與 AI 系統互動，尤其是在有限風險和高風險應用中。
(6) 人類監督：高風險 AI 系統需設計和操作方式，使人類能夠有效監督和控制系統，防止自動化決策帶來的負面影響。
(7) 準確性與網路安全：確保高風險 AI 系統具備準確性、可靠性和可重複性，同時訂定完善的備援計劃。

7. **罰則：**法案設有巨額之罰款。如違反「不可接受風險之人工智慧」相關規定，最高可處 3,500 萬歐元或上一財政年度全球年營業額 7%之罰款（較高者為準）。而違反「其他規範義務」，最高可處 1,500 萬歐元或上一財政年度全球年營業額 3%之罰款（較高者為準）。而向主管機關提供不正確、不完整或誤導性訊息，最高可處 750 萬歐元或上一財政年度全球年營業額 1.5%之罰款（較高者為準）。

比較與簡評

歐盟「人工智慧法案」採取全面性的規範，共有 113 條條文，將 AI 系統按照風險等級進行細緻分類，並針對不同風險級別制定相應的合規要求，並課予提供商各種監控義務，亦有嚴格罰則規定。相比之下，臺灣日前預告之「AI 基本法草案」全文 18 條條文，主要為原則性宣示規範，但已提出如數據治理、透明可解釋、資安、公平不歧視等重要管理原則，此與國際監管趨勢一致。且草案立法理由亦說明將推動 AI 風險分級框架，要求數位發展部參考國際標準或規範，推動 AI 風險分類框架，並依此框架制定風險分類規範。

總結來看，草案於法規的全面性、詳細性及監管機制設置上固然不若歐盟「人工智慧法案」成熟，然已表明臺灣在人工智慧法規上已朝著國際標準邁進。尚待考究者，是目前草案似乎無法看出日後臺灣人工智慧發展之專責機構，且多項具體之實施細則和監管機制也有待政府、數位發展部、國科會等日後推出。於此同時，歐盟的經驗可以作為臺灣未來在人工智慧監管方面的重要參考，以確保臺灣 AI 發展的安全與合規。最後如前述，歐盟「人工智慧法案」具有域外效力，實施後勢必將影響臺灣科技企業。政府於後續立法時，亦應密切追蹤瞭解歐盟動向，以評估對臺灣企業之衝擊及影響。

聯繫方式

黃麗蓉 Anna Hwang
執行合夥律師
anna.hwang
@bakermckenzie.com

王碩勛 Terrence Wang
律師
terrence.wang
@bakermckenzie.com