August, 2024

THY
Taiwan International
Law Offices

NEWSLETTER

歐盟對於人工智慧發展之因應及我國「AI 基本法草案」之訂定

AI 科技之應用已從單純早期之語音辨識、圖像辨識、GPS 等，日益進步並被多元運用於日常生活以外之高科技產業產品系統、勞力提供、建立預測模型等。惟此新型態人工智慧之出現及高速發展並非現行法規所得規範，故需訂立相關法規，解決人工智慧伴隨而來之爭議。其中內容包括但不限於倫理道德、人工智慧系統定義、如何使用、使用範圍、侵害態樣等。故本文將介紹歐盟近期訂定並通過之人工智慧相關法案及我國在順應此國際潮流下所訂立之「AI 基本法草案」。

一、 歐盟人工智慧法案（AIA）[1]

人工智慧法案（全名為 Artificial Intelligence Act，下稱 AIA）為世界第一部關於人工智慧之規定，其上位目標在於設置一個健全而靈活的 AI 法律框架，採用「基於風險的管理方法」（risk-based approach）對人工智慧產品進行風險分級，並提出符合比例原則的監管措施與設置最低的必要要求做適當管制，以解決人工智慧產品所帶來的可能風險，同時不過度限制或阻礙技術發展。例如生成式 AI 目前為有限風險等級 AI，其基礎模型應符合透明義務，並應揭露於訓練過程中所利用之著作，以確保其不違反歐盟法律（European Union Law）[2]及歐盟各國著作權法等相關法規。此法案經歐盟理事會及歐洲議會擴張適用對象至 AI 製造商、供應商、進口商、經銷商、使用者等等，而以「供應商」及「使用者」為主要課予義務對象，若違反將面臨高額罰款，並預計於 2026 年正式施行。世界各國亦以 AIA 為訂定其 AI 相關規範之基礎及框架。人工智慧簡要之風險分級如下表[3]：

風險等級	應用及特色	使用限制、義務
不可接受風險 AI	違反歐盟價值觀及權利（嚴重威脅人民生命或身心健康等基本權利）	一律禁止適用
高風險 AI	涉及管制商品安全元件（例如：醫療器材、車輛）或特定領域（例如：關鍵基礎設	基本上允許投入市場，惟須遵守某些強制性要求及法定義務（例如：風險評估、充分揭露、

[1] 參考 楊智傑、鄭富源《人工智慧法與生成式 AI 規範》
[2] 例如，「一般資料保護規則（GDPR）」，規則內容請見註腳 6
[3] 參考 楊智傑、鄭富源《人工智慧法與生成式 AI 規範》

	施、公部門或私部門之重要服務）	網路安全等），並應取得合格評定標章。
有限風險 AI	對公民的風險較小且可控（例如：生成式 AI）	透明義務（例如：需告知使用者其與機器正在進行互動，並可決定是否繼續）
最小風險或無風險 AI	對於公民權利與生活幾乎沒有影響，大部分人工智慧應用皆屬此類（例如：垃圾郵件過濾系統）	無特別規範亦無相應義務

二、 我國 AI 基本法草案

為因應 AI 於世界各國快速發展，我國比照歐美採取先指引[4]，後立法之順序。根據台灣「人工智慧科研發展指引（AI Technology R&D Guidelines）」訂定之 AI 基本法草案著重 AI 倫理與法制，包含 (1)發展綱領 (2)政府應提供巨量資料（big data）之共享平台 (3)設立專責機關 (4)個人資料蒐集、處理、利用應符合相當管理機制 (5)在獲取大量數據資料過程中同時保護隱私 (6)將人工智慧做風險分級等。以下表格係就「立法院第 10 屆第 6 會期第 2 次會議議案關係文書」[5] 之草案條文內容為整理：

草案條號	主旨
第 1~7 條	1. 本法之制定目的：基於對 AI 之研發應用，提升國家安全、經濟、競爭力及人民生活品質 2. 名詞定義（本法名詞大量參酌相關法令，例如對於個人資料定義即參考歐盟所訂立之之「一般資料保護規則」[6]） 3. 主管機關、專責機構及其職掌
第 8~10 條	巨量資料（big data）平臺共享機制、人工智慧風險分級[7]及其義務
第 11~15 條	人工智慧發展之基本原則，包含尊重國際公約規範、環境保護

[4] 關於台灣「人工智慧科研發展指引（AI Technology R&D Guidelines）」，另參考本所所撰 Newsletter《台灣 AI 法制簡介》

[5] 於中華民國 111 年 9 月 28 日印發

[6] 原文為 General Data Protection Regulation，簡稱 GDPR），其列舉特殊具敏感性之個人資料範疇，將種族、政治意見及宗教信仰列入個人資料定義範圍。就算 AI 為新型態科技，其對個人資料蒐集、利用、管理等為建構其數據資料庫之行為，亦須符合 GDPR，並無例外。

[7] 參酌 「歐盟 AIA」，將 AI 予以分級並訂定相應應遵守之義務

	及永續發展原則、兼顧人民權益及資訊透明等
第 16~20 條	人工智慧創新實驗場域（Sandbox[8]）之推動及審核、人工智慧產業應公開之服務使用條款(例如以人為本之倫理服務)、人工智慧產品及服務之驗證制度及促進人工智慧產業發展應推動之事項
第 21~24 條	使用者隱私權保障（例如應遵守個資法及確保當事人得隨時保有其個人資料之可攜性[9]）、個人資料彙集原則及倫理審查機制
第 25~27 條	未揭露服務使用條款、未依個人資料當事人要求提供其通用格式之資料、未經倫理審查而執行應經審查核准之計畫，及未依個人資料保護法規定或未經去識別措施而不當利用個人資料導致個人資料當事人嚴重損害之處罰。
第 28 條	行政機關應限期檢討現行法規
第 29 條	施行日期

[8] 透過相關的設計打造實驗場域，提供一套機制讓創新者可以在風險可控的情況下，進行產品、服務或商業模式的測試。

[9] 例如「加州隱私權法（CPRA）」及「歐盟 GDPR」賦予當事人有權接收其提供予控管者（controller）之資料，並請求控管者在技術上可行的範圍內將其個人信息傳輸給其他實體。