歐盟人工智慧法案簡介

駐歐盟經濟組/2024 年 8 月 19 日

一、前言

近年人工智慧(下稱 AI)技術逐漸成熟，並可簡易地落實在當今社會經濟的各個部門，其影響可跨越歐盟會員國間之國境，目前部分會員國已開始研商可確保 AI 信賴安全之國家法規，部分會員國則尚未採取行動，歐盟各會員國間對於 AI 監管之不一致性恐破壞單一市場，並對使用、進口、開發 AI 系統等行為增加法規不確定性，爰歐盟執委會於 2021 年 4 月提出歐盟 AI 法案，該法案係全球首部針對 AI 之全面性法規，旨在確保歐盟開發及使用之 AI 係值得信賴，提供保護人們基本權利之保障措施，於歐盟建立一致的 AI 市場，並為相關技術之投資與創新創造支持性環境，該法案已於 2024 年 8 月 1 日生效，適用歐盟全體會員國。

二、法規要點

(一)以風險為基礎：歐盟 AI 法案(下稱法案)採用基於風險的方法來監管 AI 系統，將 AI 引發之潛在風險區分不同級別，相關定義如下：

1. 最小風險(Minimal risk)：依據歐盟新聞稿指出[1]，大多數 AI 系統皆屬最小風險，例如支援 AI 之推薦系統和垃圾郵件過濾器等，由於該等系統對人們之權利與安全風險極小，無須承擔法案規定之義務。

2. 有限的 AI 風險：在使用 AI 系統過程中，使用者面臨的主要風險來自 AI 系統缺乏透明度，爰法案第 50 條制訂透明化相

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123

關規定，如必須能夠讓用戶瞭解其正與 AI 系統互動；AI 產生之內容必須被標記為人工生成；須讓用戶知悉其正處於生物識別分類或情緒辨識系統之使用環境等。

3. 高風險 AI 系統：依據法案第 6 條規定，倘 AI 系統作為產品之安全零組件，或該 AI 系統本身即為獨立產品且適用於法案附錄 1 所列舉之法規清單，即可視為高風險 AI 系統。此外，法案附錄 3 所敘明有關生物辨識、關鍵基礎設施、教育或職業培訓、評估使用公共或私人服務資格等 AI 系統與應用，倘對自然人之健康、安全及基本權利構成重大損害，亦將被視為高風險 AI，例如用於招募、評估貸款資格等 AI 系統，依據法案第 8 至 15 條相關規定，高風險 AI 系統需要遵守相關要求，包括具備風險管理系統、高品質之資料集(data set)、活動記錄、明確的使用者資訊、人工監督和高水準的準確性及網路安全性等條件。

4. 不可接受之風險：依據法案第 5 條規定，對人們基本權利構成明顯威脅之 AI 系統將被禁止，如忽視用戶自由意志並操縱用戶行為之 AI 系統或應用程序，包括使用語音輔助鼓勵未成年人危險行為之玩具、政府或公司可進行「社會評分」之系統，此外，生物識別系統之即時用途將被禁止，例如在工作場所使用情緒識別系統、對自然人進行分類之 AI 系統、及在公共場合將遠程生物識別系統用於執法等應用，惟倘生物識別系統用於尋找失蹤者、預防對自然人之生命威脅、識別犯罪嫌疑人等情況，可准予使用。

(二)適用對象：依據法案第 2 條及第 3 條規定，自 AI 供應鏈各階段之提供者、進口商、經銷商、佈署者等，及歐盟境內受影響之自然人，皆為本法案適用對象，另依 AI 用途目的設有免適用情況，相關說明如下：

1. **提供者(provider)**：係指開發 AI 系統或通用 AI(GPAI)模型，或以自己名稱或商標將開發之 AI 系統或 GPAI 模型投入市場之自然人、法人、公部門機構或其他團體等。法案適用將 AI 系統或 GPAI 模型投入到歐盟市場之提供者，無論該等提供者位於歐盟境內或其他第 3 國，並包括前述位於第三國之提供者在歐盟之授權代表(authorized representative)。

2. **佈署者(deployer)**：係指使用 AI 系統之自然人或法人、公部門機關或其他團體等。法案適用在歐盟境內之 AI 系統佈署者，或是在第三國但其 AI 系統輸出結果應用於歐盟境內之 AI 系統佈署者。

3. **製造商**：法案適用將其產品結合 AI 系統並投入到歐盟市場之產品製造商，且該產品標示該產品製造商之公司名稱或商標。

4. **進口商和經銷商**：法案適用 AI 系統的進口商(importer)和經銷商(distributor)，其中，AI 系統進口商係指位於歐盟之自然人或法人，前述自然人或法人將自第三國自然人或法人名稱或商標下之 AI 系統引進市場；經銷商係指供應鏈中除供應商或進口商以外之自然人或法人，其製造用於歐盟市場之 AI 系統。

5. **自然人**：適用歐盟境內受影響之自然人。

6. **排除適用之情況**：包括為科學研究而開發之 AI 系統或模型、投入市場前之測試開發、非專業用途之 AI 個人使用等情況，均不適用法案相關規定。

(三)適用對象之義務：對於高風險 AI 系統及具系統風險之通用 AI 模型，法案針對相關人士規定不同之義務如下：

1. **高風險 AI 系統**：

(1). 提供者之義務：依據法案第 16 條規定，高風險 AI 系統提供者除須確保其 AI 系統符合法案第 8 至 15 條有關風險管理

系統、數據治理(data governance)、技術文件、透明化、確保網路安全等規定外，其他相關義務包括依法案第 17 條規定建立品質管理系統，以書面形式記載法規遵守，符合性評鑑、設計驗證等相關資訊；依法案第 18 條規定保存技術文件、品質管理系統等文件；依法案第 19 條規定保存 AI 系統之日誌檔(logs)；確保 AI 系統符合法案第 43 條有關符合性評鑑之規定等。

(2). 歐盟境外第三國之提供者：法案第 22 條則規定歐盟境外第三國之提供者在其高風險 AI 系統投入歐盟市場前，應書面任命一名位於歐盟境內之授權代表，執行授權書所委託之事宜，可委託事宜包括驗證法案第 11 條規定之技術文件、驗證第 47 條規定載明之符合性聲明、向主管機關提供必要文件與資訊、配合針對其高風險 AI 系統所採取之任何行動等。

(3). 進口商之義務：依據法案第 23 條規定，高風險 AI 系統進口者須確認提供者已落實相關義務，例如 AI 系統之符合性評鑑、起草技術文件等；另須確保 AI 系統應貼有 CE 標籤並附有法案第 47 條規定載明之符合性聲明等；在 AI 系統之包裝或隨附文件上註記名稱、註冊商標、聯絡地址等資訊；向主管機關提供必要文件與資訊，配合針對其高風險 AI 系統所採取之任何行動等。

(4). 經銷商之義務：法案第 24 條載明相關義務，如在高風險 AI 系統投入市場前，經銷商應驗證該 AI 系統是否帶有所需的 CE 標誌，並附有第 47 條中提到的歐盟符合性聲明副本和使用說明；倘經銷商認為其高風險 AI 系統恐不符法案第 8 至 15 條相關規定，不得將其 AI 系統投入市場等。

(5). 部署者之義務：依據法案第 26 條規定，相關義務包括部署

者應採取適當之技術和措施，依照高風險 AI 系統之使用說明據以使用該 AI 系統；監控該系統之運作，並適時提供運作相關資訊予供應者；保存 AI 系統之日誌檔(logs)至少 6 個月等。另依據法案第 27 條規定，倘部署者係受公法管轄之機構或提供公共服務之私人實體，且其使用之高風險 AI 系統係用於評估自然人之信用分數或生命風險，則該部署者須於使用前評估對基本權利之影響。

(6). AI 價值鏈之責任：依據法案第 25 條規定，任何經銷商、進口商、部署者或其他第三方倘符合以下條件，均將被視為高風險 AI 系統之提供者，應遵守法案第 16 條相關規定：

- 將其名稱或商標放在已投入市場或使用之高風險 AI 系統；
- 對已投入市場或使用之高風險 AI 系統進行實質修改，且修改後依據法案第 6 條規定仍屬高風險 AI 系統；
- 修改 AI 系統之用途，且修改後依據法案第 6 條規定屬高風險 AI 系統。

2. 具系統風險之通用 AI 模型：依據法案第 3 條規定，通用 AI(GPAI)模型係指一種 AI 模型，包括使用大規模數據進行自我監督 (self-supervision)訓練之 AI 模型，該模型顯示出顯著的通用性(generality)，且無論以何種態樣進入市場，皆能夠執行各種不同的任務，並可整合到下游各種系統或應用程式中，但排除在進入市場前用於研究、開發、試驗活動(prototyping activities)之 AI 模型，另依據法案第 51 條規定，倘 GPAI 模型經執委會認定、適度評估或其模型訓練所使用之累積計算量大於 10^{25} 浮點運算量級，該模型將被視為具高度影響力，歸類為具系統風險之 GPAI 模型，相關提供者之義務如下：

(1). GPAI 模型提供者：法案第 53 條規定 GPAI 模型提供者應履行之義務，涵蓋撰擬技術文件、揭露訓練模型之簡要資訊

國家主管機關進行必要合作等，相關義務列舉如下：應撰擬並更新模型之技術文件，該技術文件應包含模型預計執行之任務、架構、參數、技術手段等法案附件 11 所載明之資訊；為下游 AI 系統供應商制定文件，確保供應商瞭解該 GPAI 模型之能力及侷限性，俾遵守相關法規義務；根據歐盟 AI 辦公室提供之格式，撰擬並公開有關於訓練 GPAI 模型之簡要資訊等義務。

(2). 歐盟境外第三國之提供者：法案第 54 條則規定歐盟境外第三國之提供者在其 GPAI 模型投入歐盟市場前，應書面任命一名位於歐盟境內之授權代表，執行授權書所委託之事宜，並履行法案第 53 條及 55 條所載之相關義務。

(3). 具系統風險 GPAI 模型之提供者：法案第 55 條另規定具系統風險 GPAI 模型之提供者應履行之義務，除應履行前述第 53 條及 54 條所載之相關義務外，應依據技術演進評估模型，以減輕潛在風險，並對模型及其基礎設施提供網路安全保護措施，倘意外事件之發生，需向歐盟 AI 辦公室及國家主管機關報告發生情形。

(四)歐盟相關執行單位

1. 歐盟 AI 辦公室：法案第 56 條規定，歐盟 AI 辦公室應推動歐盟層級之行為準則(code of practice)，以促進本法案之實施，並同時考量國際作法，此外，其業務範疇應確保前述第 53 條及 55 條所載之相關義務有效落實，該辦公室並可邀請 GPAI 模型提供者及相關國家主管機關參與產業規範之制定過程；法案第 64 條明定，執委會應透過 AI 辦公室建立歐盟在 AI 領域之專家能力。

2. 歐洲人工智慧委員會：依據法案第 65 條規定，將設立歐洲人工智慧委員會(European Artificial Intelligence Board)，由各會

員國指派一位代表組成該委員會，依據第 66 條規定行使職權，如該委員會將負責各會員國主管機關在落實本法案及相關行政管理之協調、就法案實施提供建議、協助 AI 辦公室支援相關主管機關建立和發展 AI 監管沙盒機制、促進與第三國或國際組織間之合作、向執委會就 AI 國際事務提供建言等。

3. **諮詢論壇：**依據法案第 67 條規定，將設立諮詢論壇(Advisory Forum)，以向執委會與歐洲人工智慧委員會提供技術知識及建言，該論壇成員將來自產業、學術、中小企業、新創等，另歐盟基本權利署(The Fundamental Rights Agency)、歐盟網路安全局(ENISA)、歐洲標準委員會(CEN)、歐洲電工標準化委員會(CENELEC)和歐洲電信標準協會(ETSI)應為諮詢論壇的永久成員。

4. **獨立專家科學小組：**依據法案第 68 條規定，執委會應透過施行細則，制定成立獨立專家科學小組之相關規定，該小組由具備 AI 領域專業知識者組成，負責向 AI 辦公室提供有關落實本法案之相關建言。

5. **國家主管機關：**法案第 70 條規定，每個會員國應至少設立或指派一個通知機構及一個市場監督機構作為國家主管機關，以履行本法案賦予主管機關之權責，會員國並須向執委會提交機關資訊，執委會應推動各會員國主管機關間之交流，另會員國應在 2025 年 8 月 2 日前公開相關主管機關之電子聯絡方式

(五)AI 監理沙盒：法案第 57 條規定，會員國其主管機關應在國家層級建立至少一個 AI 監管沙盒(Sandbox)，並於 2026 年 8 月 2 日前投入運作，該 AI 監管沙盒機制將提供一個可受控環境，以促進創新和競爭力，並協助 AI 系統在投入市場前，可於有限時間內完成訓練、測試、驗證等階段性任務，推動 AI 生態

系統之發展，特別是協助新創及中小企業開發之 AI 系統進入歐盟市場，執委會並可為 AI 監管沙盒的建立和運作提供技術支援、建議和工具；法案第 58 條進一步規定執委會應採認施行細則(implementing act)，以明確規定 AI 監理沙盒之建立、執行、監督等細節；此外，第 59 條另明列，可在 AI 監管沙盒機制中利用個資開發 AI 系統之適用情形，例如減緩氣候變遷、疾病檢測、改善環境品質等目的。

(六)對中小企業及新創之措施：法案第 62 條規定會員國應針對在歐盟擁有註冊辦事處或分支機構的中小企業(包括新創)，在符合資格前提下，提供可優先進入AI 監管沙盒、使用訓練計畫等資源，並協助回復對本法案之疑問，另需減免中小企業依據法案第 43 條進行符合性評鑑之相關費用。此外，AI 辦公室應開發單一資訊平台，方便歐盟境內所有營運商(Operator)使用，並透過宣傳活動，提高公眾對本法案相關義務之認識。

(七)罰款：依據法案第 99 條規定，相關罰則簡述如下：

1. 違反法案第 5 條禁用 AI 應用相關法規，其罰款最高可達企業全球年營業額之 7%或 3,500 萬歐元(取較高者)；

2. 違反法案第 16、22-24、26、31、33-34、50 條等相關義務，罰款最高可達企業全球年營業額之 3%或 1,500 萬歐元(取較高者)；

3. 向主管機關或公告機構提供不正確資訊，罰款最高可達企業全球年營業額之 1%或 750 萬歐元(取較高者)。爰裁罰金額或計算比例將因適用情況而不同，細節請詳法案第 99 條相關規定。

三、法案實施時間表：依據法規第 113 規定，目前法案已於 2024 年 8 月 1 日生效，並將於 2026 年 8 月 2 日起適用於歐盟全體會員國，其中，有關被禁止的人工智慧行為相關規定，將另於 2025

年 2 月 2 日適用；有關 GPAI、歐盟執行單位、罰款等相關規定，將另於 2025 年 8 月 2 日開始適用；與高風險人工智慧系統相關之義務規定，將另於 2027 年 8 月 2 日起適用。