發佈：2024-07-22, 週一 12:16
點擊數：6023



歐盟早在2019年就討論人工智慧法案（Artificial Intelligence Act, AI Act，以下簡稱AIA法案），依據法新社報導，直到2021年4月，歐盟執委會提出草案，歐洲聯盟高階官員表示，最初於2021年提出的這套規範旨在保障公民避免遭受可能風險影響之餘，期盼能促進歐洲的創新，也是全球首部全面規範人工智慧之法律架構，但在OpenAI獲微軟（Microsoft）大力支持的ChatGPT於202

Phoca PDF

發佈：2024-07-22, 週一 12:16
點擊數：6023

2年底問世後，掀起全球新一波AI熱潮，歐盟的立法者們又根據這些新工具調整了草案，到了2023年6月14日歐洲議會投票通過《人工智慧法案》的立法草案，同年12月8日達成了臨時協議，探其立法目的在於鼓勵人工智慧創新的同時，也限制人工智能遭到濫用，例如國家當權者利用生物辨識進行對反對者的監控，以及對於生成式AI的監管等等。歐盟立法者，羅馬尼亞議員DragosTudorache表示，「歐盟的這部新法規，將為全球人工智慧的發展和治理定下基調。」換言之，針對AI監管的內容與範圍已具有基本雛型。

由於AI人工智慧技術快速發展，在生活的各領域中應用日漸廣泛，現階段已成為國際間相關政策、規範、立法討論之焦點，前述法案以規則（règlement）形式實施，即以比照保護個資的《一般資料保護規則》（General Data Protection Regulation，GDPR)模式，於2024年3月13日歐洲議會以523票對46票，另有49票棄權的壓倒性票數，通過全球第一個AIA法案，該法案之目標是為了確保歐洲市場的人工智慧系統安全，促進當地業界投資與創新，保障歐盟基本權利與價值。參照經濟部國際貿易署

摘述AIA法案八大要點，包括：定義與範圍、針對高風險與禁用AI系統之分級、法律適用的例外、通用人工智慧系統與基本模型、新的治理架構、罰則、透明度與基本權利的保護以及支持創新之措施；其中重視風險分類分級管理、擴大禁用清單、加強對基本權利的保護、歐盟理事會下成立人工智慧專處，以比例分級罰款制裁違規業者等。

承上所述，了解AIA法案的內容大致包括：1.確保於歐盟使用人工智慧系統是安全的、可信賴的2.對於人類基本權利及歐盟價值觀須保障且尊重3.於創新及權利義務中尋求平衡。而根據歐盟公告，對於人工智慧可能對社會造成之危害風險等級進行了分類，即以風險為基礎模式（risk-basedapproach），也就是說風險越高，所受到的規範愈嚴格，例如提供高風險AI的廠商，必須先執行

Phoca PDF

風險評估並確保產品符合法規，才能讓產品上市。進一步來說，現階段將風險區分為：最小風險（Minimal risk）、有限風險（Limited risk）、高風險（High-risk）及無法接受的風險（Unacceptable risk）。因此若立法者預測AI應用的危險程度，例如歐洲立法者認為「執法部門的AI犯罪行為預測系統」不可接受，它就會被管制；又立法者認為「高風險」的技術，例如1.可以影響選民想法的工具2.社群網站的推薦演算法3.
利用AI進行社會評分制度4.透過AI操縱特定族群的弱點等，也會被設定新的管制。

另據資訊工業策進會科技法律研究所從臨時協議結論來看AIA法案的適用：1.確立域外適用之範圍，包含但不限於在歐盟內提供或使用人工智慧系統的企業2.針對通用AI（GeneralpurposeAI）模型，訂定相關規定以確保價值鏈之透明度3.針對可能造成系統性風險之強大模型，訂定風險管理與重要事件監管、執行模型評估與對抗性測試等相關義務4.針對通用AI系統整合至高風險系統5.就基礎模型部分商定具體規則，其於投放市場之前須遵守特定之透明度義務6.對於情緒識別系統有義務在自然人接觸到使用這種系統時通知他們7.針對違反禁止之AI應用，處以罰款，即中小及新創企業違反人工智慧法之行政罰款將設定適當之上限，例如未遵守法規的廠商將可能被處以750萬歐元至3500萬歐元（約新台幣2.6億至12億元）或企業全球營收1.5%至7%範圍內的罰款，此部分視其違規類型和企業規模而定。由此可知，其中的關鍵是強調透明度和問責機制，也就是說開發AI系統的公司，將被要求提供詳細的技術文件，包括使用的訓練數據資訊及確保相關智慧財產權
合乎法規
所採取的措施，藉
由這種透明度也提高了一般大眾的信
任度，並有助於對這些人工智慧模型進行審查。然而AIA法案並

Phoca PDF

不適

用於：1.

專門用於軍事或

國防目的之系統2.不適用於研究和

創新目的之人工智慧系統3.不

適用於非專業原因之個人AI使用。至於相關的這些義務將由執委會與企業界、科學社群、民間團體及其他利害關係人共同制定行為準則。

綜上內容，研究者陳稚寰觀察AIA法案的重要意涵有二：1.統整法規：從本次該法的法律位階層級看出，歐盟刻意使用具約束力且有直接效力（DirectEffect）的「規則」（Regulation），意涵著當法規正式實施時，將立即對歐盟成員國家生效，而且AIA法案的地位優先適用於各會員國法律，可有效整合會員國的法律2.建立制度引領全球：歐盟關於AI技術發展雖不如美中兩國成熟，卻急著推出全面性的AIA法案，而這部法

律甚至是全球第一部人工智慧法，意味歐盟有意自我塑造成人工智慧

領域的制度領航者。有鑑於AI的內容涉及科技倫理、著作權、文化、教育、影視以及利用AI犯罪等問題，加上AI處理資料不夠公開透明，其錯綜複雜、具誤差且難以預測的特性，為了避免不當發展人工智慧

，自2024年所通過的AIA法案，如中央通訊社於2024年3月13日報導內容，對於監管規則的訂定可從三個層面分析，體現出其具有特殊性及重要性：第一層面，屬於最高風險而被禁止的AI應用方式，例如1.使用敏感的個人特癥來建立生物辨識歸類系統2.政治立場、宗教信仰、種族或性傾向3.從網路或監視器（CCTV）蒐集不特定對象的臉部畫面，用以開發臉部辨識資料庫4.在工作場所或教育機構進行情緒辨識5.根據個人特性或行為進行社會評分等。然而有關於社會評分、監看

Phoca PDF

特定人投入程度的情緒辨識及各種人臉資訊蒐集等，經常見於中國社會生活裡相關報導中的人工智慧運用現象。另外為了打擊犯罪等執法需求前提下，AIA法案也有適用的例外情形，例如為了尋找遭到綁架肉票等犯罪被害人、為了公共安全預先防範特定恐怖活動的發生、在重大刑事案件中搜尋定位犯罪嫌疑人等情況，均可利用AI系統進行前述禁止行為，但為了避免侵害人民基本權利例如自由權、隱私權等，須依法定程序事先取得法院同意並限定時間和區域，此部分相類似於台灣的《通訊保障及監察法》。第二層面，AIA法案也禁止1.將AI用來挖掘使用者的弱點，例如行動不便、年齡、社會經濟地位等2.透過AI操弄人類行為，使其失去自由意志3.運用在關鍵基礎設施、教育、僱用、健康或金融服務等領域的人工智慧系統等，故類此之情形則被列為「高風險」，系統開發經營者有義務評估並降低風險、透明化並確保系統運作時有負責的自然人進行監督。第三層面，AIA法案針對沒有特定使用目的之「一般用途型AI」（General Purpose AI），要求須有一定透明度，也就是說系統開發經營者須公布訓練模型所用到的內容，並遵守著作權法規，例如ChatGPT就屬一般用途型AI，可用於寫語文創作、音樂編曲、藝術作品、科技製程等，然而近年來卻已發生多起不當運用AI造成侵害智慧財產權的犯罪事件，探究原因之一在於ChatGPT所訓練的大型語言模型（LLM）品

質優劣，實與其收集的資料多寡呈現高度正向關係，惟文字與資料探勘（Text and Data Mining；簡稱TDM）過程涉及著作權問題，引發諸多爭議，例如2023年底《紐約時報》開出第一槍，向紐約地方法院提起OpenAI及微軟侵犯著作權訴訟，認其未經其同意使用網站新聞內容來訓練AI模型，侵害其聲譽及營運獲利能力。由此可知，對一般用途型AI在資訊安全、模組資料來源揭取的透明度和風險管

理上必須具有基本要求，為了在防止弊端發生與創新謀利之間尋求平衡點，因此AIA法案也設有歐盟各成員國可訂定為鼓勵創新而暫免特定法律管制的沙盒（sandbox）等規定。

Phoca PDF

發佈：2024-07-22, 週一 12:16
點擊數：6023

近年來數位科技發展確實帶來人類生活的便利性，例如人工智慧、虛擬貨幣、區塊鏈等新興產品

或人工智慧工具的時候，企業除了面臨保障用戶個資不被侵犯的難題，也須同時注意使用的產品是否對人類基本權利與環境造成負面影響。如經濟日報於2024年3月14日報導內容，德國智庫「生態經濟研究所」近日發布報告，認為中小企業應合作成立「數位責任聯盟」，共同承擔數位轉型的環境與社會責任。進一步來說，企業數位責任（Corporate Digital Responsibility，CDR）是為解決數位技術發展造成的問題，近年在歐洲興起的概念，希望企業在數位化活動中主動承擔起保護人權、弱勢與環境的社會責任，當民間企業與政府間共同攜手努力，討論並提供一系列工具和指南，幫助企業建立CDR

相關的能力，並建立廣泛適用的CDR標準，使得企業能更了解如何在遵守現有法規的同時，也能自願承擔更多的數位責任，促使數位轉型更符合人權、公平正義和永續發展的原則。

有鑑於人工智慧對於人類未來的影響，而AI相關法律的應用不分國界、不分產業，宜抱持開放的立場，促

進國內外，產、官

、學、研的對話及交流，惟AI的發展

快速，如醒報社論於2024

年4月2日報導內容，令人擔憂法規是否能跟得上技術躍進的腳步，在AI相關法律的某些規定生效

Phoca PDF

發佈：2024-07-22, 週一 12:16
點擊數：6023

時，AI的實質內容或許已出現重大轉變，使得部分立法內容顯已過時或無法解決新興問題所產生的爭議。另外一方面，由於人工智慧系統具有高度的技術複雜性，如何能夠落實檢測AI生成的內容、推動有效的數位浮水印技術，以及確保訓練AI模型所使用數據符合相關法規，存在著現有科學知能與人工智慧立法要求之間的落差。台灣行政院於2023年8月31日通過由國科會所擬定的「行政院及所屬機關（構）使用生成式AI參考指引（草案）」，未來將由國科會持續觀察全球AI發展趨勢滾動調整。這份指引不只行政院所屬機關，也可供以外的其他機關參考，訂定自己的管理規範。行政院指示國科會未來持續觀察全球發展趨勢修正指引，供各機關參考，並請各部會依其業務需要，訂定使用生成式AI的規範或內控管理措施，數位部帶頭建立相關規範及訓練機制，讓政府部門運用AI提升行政效率。由此省思，政府已有預見人工智慧的未來發展，勢必會翻轉國家的競爭力，故宜未雨綢繆，加速人工智慧相關監管的法律訂定，致力於促進人工智慧技術的發展與維護隱私權益，鼓勵AI創新與保護人類基本權利和價值觀之間尋求平衡。

作者 紀博倫　為　法學博士，臺灣警察專科學校助理教授

Phoca PDF