

立法院議案關係文書 (中華民國41年9月起編號)
中華民國109年9月16日印發

院總第 1021 號 委員提案第 24935 號

案由：本院委員鄭麗文等 20 人，因應大數據、雲端、物聯網及 5G 時代來臨，為找回國家經濟發展動能，帶動台灣經濟、社會結構轉型並進一步驅動經濟發展，並實現保障數位人權之網路社會，促成政府肩負起人工智慧產業引領及制定人工智慧發展倫理規範角色，爰擬具「人工智慧發展基本法」草案。是否有當？敬請公決。

提案人：鄭麗文

連署人：費鴻泰 葉毓蘭 謝衣鳳 溫玉霞 鄭正鈴
曾銘宗 翁重鈞 萬美玲 蔣萬安 林文瑞
吳斯懷 洪孟楷 鄭天財 Sra Kacaw 徐志榮
魯明哲 陳雪生 廖婉汝 呂玉玲 陳玉珍

人工智慧發展基本法草案總說明

- 一、隨著寬頻網路與科技發展，國際工業 4.0 的發展趨勢，人工智慧商業化腳步已從實驗室的技术或原型走向市場，世界各國皆如火如荼推動國家級的 AI 發展策略。如美國今年簽署一項啟動「美國 AI 計劃」行政命令，要求聯邦機構將人工智慧的研發投入列於優先地位，同時擴大使用有利於人工智慧研發的政府數據權限；法國年度有 10 億歐元的 AI 研發經費，其中約 60% 來自政府、40% 來自企業與各產業；中國國務院更是發布「新一代人工智能發展規劃」，宣示中國將在 2030 年成為全球 AI 發展核心區域，並預估到時中國 AI 相關產業將有高達 1,500 億美元的產值。歐盟更在今年（2020 年）二月，提出「人工智慧白皮書」，歐盟的戰略是推廣數據的分享與使用，創造單一的歐盟數據市場，確保數據可安全而自由地在歐盟會員國之間流通，透過制定適當的激勵措施，加快包括中小型企業在內的人工智慧的發展，欲掌握人工智慧的規則制定權，領導全球人工智慧發展。
- 二、將人工智慧技術的研發應用與競爭力水準迅速提升，乃是世界各科技大國重要的發展目標，為實現前揭目標，我國亟待將研究、開發與整合人工智慧之技術運用於產業之中，藉以發揮我國之智慧產業創新能力。在人工智慧發展的同時，需兼顧人類生活之倫理規範，比免失控的人工智慧侵害當代各種基本價值與人權，政府需建立人工智慧發展之倫理規範，引導產業發展出良善的人工智慧。
- 三、為使我國在未來快速變遷的數據時代中居於人工智慧的領先群，盡速研究、開發與整合人工智慧之技術資源，制訂人工智慧發展基本法將能迅速凝聚社會共識、確立人工智慧作為國家政策中的重要內涵，以及認識到實際推動產業發展與轉型時應有的進步空間。此基本法參酌美國、英國、日本 AI 先進國家的法政策經驗，並整合我國國情，主要包含：
 - (一) 確定人工智慧之發展在國家政策中的定位，訂立發展綱領要求中央政府應在產業界和學術界優先推動人工智慧的研究、發展，並促進產業 AI 化、建立 AI 技術應用平台，以及形成 AI 產業生態系。
 - (二) 緣人工智慧發展牽涉大規模公眾數據的使用以及實驗場域落地試驗，與公共利益牽連甚深，須制定適當的人工智慧的開發標準原則。政府在符合開發標準原則下，應盡量滿足產業、學術界在人工智慧研發與應用之需求；建立與凝聚公眾對人工智慧的認識與信任，樹立人工智慧發展的基本倫理原則。
- 三、在上述內容考量下，爰擬具「人工智慧發展基本法」草案，其要點如下：
 - (一) 本法之制定目的。（草案第一條）
 - (二) 人工智慧之名詞定義。（草案第二條）
 - (三) 人工智慧開發原則。（草案第三條）

立法院第 10 屆第 2 會期第 1 次會議議案關係文書

- (四)人工智慧發展之倫理。(草案第四條)
- (五)人工智慧發展綱領。(草案第五條)
- (六)主管機關。(草案第六條)
- (七)補助、獎勵及輔導。(草案第七條)
- (八)個人資料相關法規調整及利用規範。(草案第八條)
- (九)特別委員會。(草案第九條)
- (十)特別審核機制。(草案第十條)
- (十一)智慧化政府推動。(草案第十一條)
- (十二)教育預算。(草案第十二條)
- (十三)沙盒計畫。(草案第十三條)
- (十四)施行日期。(草案第十四條)

人工智慧發展基本法草案

條 文	說 明
<p>第一條 （立法目的）</p> <p>推動智慧化國家及促進人工智慧產業發展，健全產業發展環境，建立人工智慧發展倫理規範，特制定本法。</p>	<p>將人工智慧技術的研發應用與競爭力水準迅速提升，乃是當前經濟發展優勢國家面臨的重要課題，透過人工智慧產業的發展可以改善科學創新產業環境，增強國家整體競爭力，達成國家永續發展。為此本法之目的即在，盡速研究、開發與整合人工智慧之技術資源，制訂人工智慧發展基本法將能迅速凝聚社會共識、確立人工智慧作為國家政策中的重要內涵，以及認識到實際推動產業發展與轉型時應有的進步空間。</p>
<p>第二條 （名詞定義）</p> <p>所謂人工智慧係指電腦軟體、硬體及其他開發中系統，符合下列任一款情形者：</p> <p>一、在沒有人為監督、操作，執行任務，且可以從經驗中學習，並自行改進結果、提高產出。</p> <p>二、任何運行模式與人類思考相似的系統，如人的認知架構和神經網絡。</p> <p>三、表現像人類的系統，例如通過圖靈測試或經由自然語言處理、知識呈現、自動推理、及學習等其他相當的測試。</p> <p>四、尋求逼近特定認知任務的技術，如機器學習。</p> <p>五、行為理性的系統，如智慧軟體代理人與通過感知、規劃、推理、學習、溝通，決策、及行動來實現目標的實體化機器人。</p>	<p>一、明定本法之用詞定義。</p> <p>二、參酌美國 2017 年人工智慧未來法案（FUTURE of Artificial Intelligence Act of 2017），對於人工智慧的定義為「（A）Any artificial systems that perform tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance. Such systems may be developed in computer software, physical hardware, or other contexts not yet contemplated. They may solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. In general, the more human-like the system within the context of its tasks, the more it can be said to use artificial intelligence.（B）Systems that think like humans, such as cognitive architectures and neural networks.（C）Systems that act like humans, such as systems that can pass the Turing test or other comparable test via natural language processing, knowledge representation, automated reasoning, and learning.（D）A set of techniques, including machine learning, that seek to approximate some cognitive task.（E）Systems that act rationally, such as intelligent software agents</p>

	<p>and embodied robots that achieve goals via perception, planning, reasoning, learning, communicating, decision-making, and acting.」於本條定義人工智慧的概念與意義。</p>
<p>第三條（人工智慧開發原則）</p> <p>任何適用本法之人工智慧項目於技術開發過程中，開發者應在技術許可範圍內遵循以下原則：</p> <p>一、透明性原則。</p> <p>二、使用者中心原則。</p> <p>三、可控性原則。</p> <p>四、安全保護原則。</p>	<p>一、參酌日本總務省於 2016 年 10 月起召開 AI 聯網社會推進會議，該會議於 2018 年 7 月 17 日公布「報告書 2018—邁向促進 AI 運用及 AI 聯網化健全發展」。該案制定目的在於促進 AI 開發及運用，藉由 AI 聯網環境健全發展，實現以人為中心之「智連社會」。本法借鏡日本對於人工智慧發展所設想的情境，提出的開發原則，使任何人工智慧項目的開發者於技術開發過程中皆遵循，以利人工智慧之發展符合國際潮流，同時確保兼顧公共利益，爰於第一項予以明定。</p> <p>二、人工智慧系統之運作與應用須具備透明性，即得以確保該人工智慧之可驗證性與可解釋性，爰於第一項第一款予以列舉。</p> <p>三、人工智慧系統之開發，應以使用者為中心進行系統設計，並提供使用者選擇與反饋的機會，爰於第一項第二款予以列舉。</p> <p>四、為處理人工智慧系統資訊網絡上，可能出現的各種非預期事件，人工智慧的應用開發者應將風險評估和可控制管理方案納入開發計畫中，並定期檢討該計畫，爰於第一項第三款予以列舉。</p> <p>五、人工智慧系統之開發應盡可能確保資訊安全、防止任何可能危害用戶和第三方生命和身體安全的威脅和漏洞，爰於第一項第四款予以列舉。</p>
<p>第四條（人工智慧發展之倫理）</p> <p>人工智慧應朝可信賴之方向發展，在技術或非技術層面追求以下要素：</p> <p>一、確保人工智慧系統應促進人的能動性與基本權利，而非限制或錯誤地引導人類的自我治理。</p> <p>二、人工智慧的演算法應將穩固性和安全性列為優先事項。</p> <p>三、人工智慧的數據資料使用應確保個人享有資訊自主權。</p>	<p>一、參酌 2018 年 12 月 18 日，歐盟人工智慧高級別專家組正式向社會發佈了一份人工智能道德準則草案，該草案被視為是「可信賴人工智慧」之重要文件。草案共 37 頁為值得信賴的人工智慧制定了一個框架，本法參酌該架構並將適切之內容加入本章，期我國人工智慧之發展得有前瞻性的追求方向與目標。</p> <p>二、確保人性尊嚴與基本人權之保障，人工智慧之發展應促進而非限制人的自主展現，</p>

<p>四、人工智慧系統之設計應具備多樣性、非歧視性和公平性。</p> <p>五、人工智慧之發展應有助於社會的永續發展，並負擔環境及生態責任。</p> <p>六、人工智慧之系統應被訂有相應的問責機制，使法所不容許之風險發生時有相應者承擔責任。</p> <p>主管機關應訂定相關的施行辦法，推動督促政府、產業，以及學術單位於人工智慧的研發與應用確實遵循前項要素。</p>	<p>爰定第一項第一款。</p> <p>三、智慧的技術掌握度會直接影響到使用者的安全性，因此須將穩固性和安全性列為人工智慧的演算法的優先事項，爰定第一項第二款。</p> <p>四、參酌歐盟的 GDPR，人工智慧發展應以保障個人資訊自主權為追求的方向，爰定第一項第三款。</p> <p>五、人工智慧系統會因為所蒐集的數據和演算法的設計影響應用的多樣性，甚至構成歧視性與公平性問題，爰定第一項第四款。</p> <p>六、承科學發展基本法之立法意旨，人工智慧亦屬科學發展的一環，應特別重視社會的永續發展，並負擔環境及生態責任，爰定第一項第五款。</p> <p>七、人工智慧有許多應用涉及設會中的日常生活，如自駕車的交通應用，此時若發生法所不容許之風險，應訂有專為人工智慧設計問責機制，使相應者承擔責任，爰定第一項第六款。</p> <p>八、主管機關應透過訂定相關的施行辦法在產官學面落實人工智慧發展之倫理，爰定第二項。</p>
<p>第五條（人工智慧發展綱領）</p> <p>政府應將人工智慧發展列為優先推動政策，並落實以下發展綱領：</p> <p>一、推動智慧化國家及促進智慧化產業發展。</p> <p>二、政府應深化人工智慧產學合作生態系，在國家財政能力之範圍內，持續充實人工智慧研發與投資所需經費。</p> <p>三、政府應持續強化人工智慧雲端運算、儲存、高速網路傳輸、大數據分析與人工智慧軟體之整合環境，使科研創新與產業發展得取得高質量和可追溯的數據。</p> <p>四、政府應培養科學、技術、工程和數學重點學科之人才，及從事人工智慧研究與應用之人員。</p> <p>五、政府應以跨部會、跨領域、跨國際的方式，推動人工智慧創新研究中心，並以我國具優勢的人工智慧領域為主題，包含但不限於智慧製造、智慧服務及生技醫療。</p>	<p>一、鑑於鼓勵人工智慧的產學合作，政府應持續撥補預算建構優質產學生態圈，並為人工智慧產業注入活水，促進智慧機器人相關產業創新應用發展，爰明定第一項第一款。</p> <p>二、人工智慧發展首重數據資料的整合運用，政府針對雲端運算、大數據資料分析，有必要確保科研創新與產業發展得以取得高質量和可追溯的數據，爰明定第一項第二款。</p> <p>三、發展人工智慧產業所需技術研發必須仰賴高階人才的培育，透過懂得運用 AI 技術或工具、解決產業問題，以及協助產業 AI 化的人才，方能完整奠定人工智慧的發展基礎，爰明定第一項第三款。</p> <p>四、我國人工智慧發展的優勢包含但不限於智慧製造、智慧服務及生技醫療等應用，政府應以跨部會、跨領域、跨國際的方式推動人工智慧創新研究中心，爰明定第一項</p>

<p>六、為避免我國人工智慧發展成果遭受惡意資訊攻擊，政府應訂定適當資安標準，確保供政府和國人使用的人工智慧系統、軟體、硬體，或演算法等之安全性。</p> <p>本法公布施行後一年內，行政院應提出人工智慧產業推動施政方針。</p> <p>中央目的事業主管機關應訂定人工智慧產業發展施政計畫，報行政院核定，並定期檢討。</p>	<p>第四款。</p> <p>五、人工智慧相關技術與應用奠基於資通訊系統和數據資料庫，一旦遭到駭客攻擊入侵，將造成嚴重的財產、人身安全的危害，故政府推動人工智慧發展應特別重視提高資安標準，確保供政府和國人使用的人工智慧系統、軟體、硬體，或演算法等之安全性，爰於第一項第五款及第六款予以明定。</p>
<p>第六條（主管機關）</p> <p>本法之主管機關：在中央為科技部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。</p> <p>本法所定事項，涉及各目的事業主管機關職掌者，由各該目的事業主管機關辦理。</p>	<p>人工智慧發展之主管機關為科技部，職掌跨部會人工智慧計畫之協調與整合。</p>
<p>第七條（補助、獎勵及輔導）</p> <p>各中央目的事業主管機關得以補助、獎勵或輔導方式，推動下列事項：</p> <ol style="list-style-type: none"> 一、促進人工智慧產業創新或研究發展。 二、提供人工智慧產業技術移轉輔導。 三、鼓勵企業設置人工智慧創新或研究發展中心。 四、協助設立人工智慧創新或研究發展機構。 五、促進產業、學術及研究機構之合作。 六、鼓勵企業對學校人才培育之投入。 七、充裕人工智慧產業人才資源。 八、協助地方人工智慧產業發展。 九、鼓勵企業運用巨量資料、政府開放資料，以研發創新商業應用或服務模式。 十、其他促進產業創新或研究發展之事項。 <p>前項補助、獎勵或輔導之對象、資格條件、審核基準、申請程序、核定機關及其他相關事項之辦法，由各中央目的事業主管機關定之。</p>	<ol style="list-style-type: none"> 一、人工智慧產業之活動，除企業本身之研發、人才投入外，透過企業間或企業與學術單位間之相互合作等活動之進行，亦可創造加速之效果。另為強化產學交流，得運用補助方式，鼓勵企業提供在學學生實習機會，使學校培育之人才得符合職能所需，俾對產業亦有加乘效果。而為協助人工智慧產業，爰於第一項明定各中央目的事業主管機關得運用補助或輔導方式，推動人工智慧產業發展。 二、第二項授權各中央目的事業主管機關訂定產業補助或輔導辦法，俾資適用。
<p>第八條（個人資料相關法規調整及利用規範）</p> <p>為發展人工智慧而涉及個人資料之蒐集、處理、利用，主管機關應於一年內進行國內法規調整，在保護個人隱私條件下，開放個人資料用於人工智慧之研發與運用。</p>	<ol style="list-style-type: none"> 一、我國雖有個人資料保護法用於規範個人資料之蒐集、處理、利用，惟人工智慧發展過程中，充斥不確定性，應適度開放對於個資之管制，增加資料之可開發性，爰授權行政機關對於因人工智慧發展所涉之個人資料蒐集、處理、利用制訂特別法。

立法院第 10 屆第 2 會期第 1 次會議議案關係文書

<p>為推動人工智慧的研發和人工智慧技術的產業應用，主管機關應基於上開特定目的，就政府部門所蒐集之國民個人數據資料或非個人數據資料，訂定明確的授權使用辦法，並於該辦法中訂明相關申請使用流程、確保使用目的查驗、資料保護方案，以及匿名或去識別化標準。</p>	<p>二、大數據資料乃是人工智慧發展的重要基礎，因此主管機關有必要針對政府所蒐集的數據訂定授權辦法，使基於推動人工智慧的研發和人工智慧技術的產業應用之特定目的，得依據授權使用之辦法中所訂之申請使用流程獲取所需的數據資料，並應訂明確保使用目的查驗、資料保護方案，以及去識別化標準以兼顧個資保護，爰予第二項以明確規範，以資因應。</p> <p>三、本條第一項與前條第二項授權行政機關對於因人工智慧發展所涉之個人資料蒐集、處理、利用，為個人資料保護法之特別規定。</p>
<p>第九條（特別委員會） 政府應成立人工智慧特別委員會，專司跨部會人工智慧的數據資料整合、基礎人工智慧的研發、人工智慧技術應用部署之諮詢與研究。</p>	<p>人工智慧所涉之層面極為廣泛，在政府職能分工上亦涉及國家發展、經濟、財政、金融、內政、交通、通訊傳播、衛生福利、資通安全、科技、公平交易等部會。為排除人工智慧發展障礙，需要行政院針對跨部會議題進行規劃與協調。</p>
<p>第十條（特別審核機制） 如人工智慧發展計畫涉及大規模處理高敏感性個人資料、弱勢族群之資料，且有違反倫理規範之疑慮，影響第三人權益時，人工智慧特別委員會應進行審核。</p>	<p>人工智慧發展之不確定性主要來自於資料蒐集、處理、利用方式，尤其人工智慧計畫涉及大規模處理敏感性個資，應該經由公正第三方檢視有無違反開發原則、倫理規範，爰規定應由委員會進行審核，確保第三人權益，且委員會審核時不得干預開發之自由。</p>
<p>第十一條（智慧化政府推動） 政府一級機關、二級機關、三級機關及獨立機關應設立人工智慧辦公室，負責推動智慧化政府工作及相關聯繫工作。</p>	<p>推動政府整體智慧化工作，要求政府一級至三級機關及獨立機關應設立人工智慧辦公室，專責推動政府智慧化工作，以及協助聯繫整體政府智慧化業務聯繫相關工作。</p>
<p>第十二條（教育預算） 教育部應匡列預算，於國民基本教育實施人工智慧教育課程。</p>	<p>人工智慧教育應從小扎根，立法要求教育部訂定相關課程，在不同的學齡階段給予適當的教學內容。</p>
<p>第十三條（沙盒計畫） 政府應規劃、研擬得實施人工智慧計畫之場域或實驗空間，並提供相關協助，且於實驗階段內豁免與該計畫相關之法規限制，並適時評估修法之必要性。</p>	<p>人工智慧之發展涉及不確定性與風險性，惟發展結果可能有助於公共利益及社會發展，為協助我國人工智慧計畫於實驗階段能獲得一定程度支持，爰規定政府應仿照沙盒（Sandbox）的精神，提供場域及必要協助，開放人工智慧之發展，並於實驗階段中豁免人工智慧計畫遭遇之法規限制，並隨時評估相關之法規限制是否有修正之必要。</p>
<p>第十四條（施行日期） 本法自公布日施行。</p>	<p>本法條施行日期。</p>