　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110093750000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11009375 | 號 |  |  |

案由：本院委員楊瓊瓔、黃健豪、廖偉翔、馬文君、羅廷瑋等26人，鑑於人工智慧技術近年發展快速，被世界普遍認為可為整體產業與社會活動帶來廣泛之經濟和社會效益。故為確立我國推動人工智慧技術與應用發展之方向及作法，建構人工智慧技術與應用之良善運作環境，為政府刻不容緩之責任，爰擬具「人工智慧基本法草案」，期使我國人工智慧發展促進創新兼顧人權與風險，進而帶動國家整體產業數位轉型，並進而引導科技正向發展。是否有當？敬請公決。

提案人：楊瓊瓔　　黃健豪　　廖偉翔　　馬文君　　羅廷瑋

連署人：翁曉玲　　黃　仁　　蘇清泉　　許宇甄　　丁學忠　　顏寬恒　　陳超明　　王育敏　　呂玉玲　　徐欣瑩　　張嘉郡　　游　顥　　牛煦庭　　林德福　　廖先翔　　盧縣一　　邱鎮軍　　葛如鈞　　張智倫　　魯明哲　　羅明才

|  |  |
| --- | --- |
| 人工智慧基本法草案 | |
| 條文 | 說明 |
| 第一條　（立法目的）  為建設智慧國家，促進人工智慧產業發展，建構人工智慧安全環境，保障人民基本權利，增進社會福祉，提升國際影響力，特制定本法；本法未規定者，適用其他法律之規定。 | 一、鑑於人工智慧發展之國際趨勢，相關研發及利用涉及諸多領域，應有整體規劃之必要。  二、政府及民間應協力合作，共同促進人工智慧產業發展，建構人工智慧安全環境，保障人民基本權利，增進社會福祉，提升國際影響力，俾利達成智慧國家之建設，爰制定本法。 |
| 第二條　（主管機關）  本法所稱主管機關：在中央為數位發展部；在地方為直轄市、縣（市）政府。  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。 | 一、數位發展部之設立目的，為促進數位經濟發展，加速國家數位轉型，建設智慧國家。依數位發展部組織法第二條可知，數位發展部掌理國家數位發展政策之擘劃，建構數位科技應用與創新發展環境及人才培育，促進數位經濟產業，以及數位發展國際合作等事項，均與人工智慧發展有密切關係。人工智慧作為數位科技發展之重要部分，與數位發展部之職掌有密切關係，故以數位發展部為主管機關。  二、人工智慧之發展，中央及地方應協力合作，故在地方，以直轄市、縣（市）政府為地方主管機關。又，為顧及各種事業發展之特性，應由各該目的事業主管機關辦理本法所定事項。 |
| 第三條　（人工智慧之定義）  本法所稱人工智慧，指接收人類或機器資料輸入，以下列各款全部或部分方式，實現預測、建議、決策或其他特定目的之軟體、硬體及其他相關之系統：  一、使用監督式學習、非監督式學習、強化學習或其他利用資料建立模型之機器學習方式。  二、使用各種知識表示方式建立之知識庫系統，以推理引擎進行歸納、演繹、反證或其他模仿人類邏輯推理能力之方式。  三、使用統計、搜尋、剖析、優化或其他方法，建立決策或推理模型之方式。  四、使用前三款以外之模仿人類思考及反應模式，進行感知、規劃、推理、學習、溝通、生成、修正或其他之方式。 | 一、本條規範之人工智慧，係指使用可以體現或模仿人類行為及反應之方式，作為預測、建議或決策等特定目的之軟體、硬體或其他開發中之系統。  二、第一款為「機器學習」之方式。機器學習之方式繁多，諸如監督式學習、非監督式學習、強化學習或其他機器學習方式（如深度學習、生成式模型或建立類似架構之模型），皆屬之。  三、第二款係指前款機器學習外，其他得以體現人工智慧之方式。所謂「知識表示（knowledge representation）」係指描述、呈現知識之表達文字、圖型；知識庫則是以歸納（induction）、演繹或推理（deduction）、反證法（contradiction）等計算方式，以推理（演繹）引擎，實現類似人類之邏輯推理（logic inference）能力。  四、第三款所稱「統計」，指統計學習及推理；另，「搜尋（search）、剖析（parsing）或優化（optimization）」，指搭配由人為或機器學習所建立之搜尋策略、剖析規則、目標函數等運作之方式。  五、第四款為概括條款，指非前三款所體現之人工智慧方式，只要有使用其他仿效人類思考及反應模式，進行感知、規劃、推理、學習、溝通、生成、修正或其他方式，亦為本法所稱之人工智慧。 |
| 第四條　（研發及利用之基本原則）  人工智慧之研發及利用，應以人為本、普惠人民、永續發展及值得信賴為目標，並遵行下列基本原則：  一、自主原則：尊重人性尊嚴及個人自主。  二、保密原則：尊重人民隱私及營業秘密。  三、安全原則：保障人民生命、身體、自由及財產之安全。  四、包容原則：重視多元包容，確保公平，避免歧視。  五、透明原則：強化可解釋性及可追溯性，確保問責可能性。 | 一、人工智慧研發及利用之倫理原則，應以人為本，非僅為特定人或事業謀求利益，更應重視永續發展理念，遵循本法之基本原則及規定，期使人工智慧之研發及利用具有自主性、保密性、安全性及透明性，成為值得信賴之人工智慧。  二、人工智慧之研發及利用，應確保人性尊嚴與個人自主控制及監督之權利。  三、人工智慧之研發及利用，涉及個人隱私及營業秘密，對相關資料之蒐集及處理，應採取尊重及保護措施。  四、人工智慧之研發及利用，應確保其安全可靠，以避免造成人民重要權益之侵害。  五、人工智慧之研發及利用，應重視多元價值觀，避免人工智慧因身分、性別、種族、年齡等因素，造成歧視或偏見。  六、人工智慧之研發及利用，為使人民信賴，應具有可解釋性及可追溯性，確保人民知悉人工智慧之決策內容，並提高問責之可能性。 |
| 第五條　（推動人工智慧主要政策）  政府應落實下列人工智慧發展之主要政策，並重視跨領域及國際合作：  一、促進人工智慧研發創新。  二、重視人工智慧基本教育。  三、培育人工智慧專業人才。  四、推動人工智慧產業發展。  五、深化人工智慧產學合作。  六、鼓勵人工智慧發展投資。  七、建立資訊通訊基礎設施。  八、其他人工智慧發展政策。 | 一、為因應人工智慧產業發展趨勢，政府應加速推動人工智慧及產業發展，建構完善之產業環境，透過跨領域及國際合作之方式，維繫我國在全球產業價值鏈之關鍵地位。  二、人工智慧之主要政策應在於促進人工智慧之研發創新，重視人工智慧之專業教育及基本教育，開設人工智慧課程，開展國際交流合作，培育與人工智慧有關之科技、工程、電腦、法律、社會、文化等多方面人才，從事人工智慧研發及利用之人員，推動人工智慧產業發展，以及協助人工智慧產業及學術機構進行產學合作。 |

|  |  |
| --- | --- |
| 第六條　（發展計畫）  中央主管機關應依前條政策，擬訂人工智慧發展計畫，報行政院核定，並定期檢討修正。  中央目的事業主管機關應依前項計畫，擬訂或訂定法規或具體方案，辦理本法所定事項。 | 一、為落實第四條人工智慧之主要政策，促進人工智慧之發展，推動跨領域及國際合作，適時因應人工智慧發展可能附隨之負面效應及風險，應由中央主管機關統籌擬訂發展計畫，參考科學技術基本法第十條及中醫藥發展法第五條規定，為第一項規定。  二、為落實推動人工智慧政策發展，各中央目的事業主管機關應配合辦理本法所定事項，為第二項規定。 |
| 第七條　（政府預算經費之確保）  中央政府應於國家財政能力範圍內，寬列預算，採取必要措施，持續確保經費符合推行人工智慧政策發展所需。 | 政府應積極落實本法第四條人工智慧之主要政策；惟政策之推動，有賴持續投入穩定且充足之資源，故參考中醫藥發展法第四條及文化創意產業發展法第八條之規定，明定政府應寬列經費，確保落實人工智慧政策之經費穩定充足。 |
| 第八條　（財稅及金融優惠）  中央政府應積極協助、輔導人工智慧產業，結合財稅及金融優惠制度，提供產業穩健發展，培植國內人工智慧人才及產業鏈，促成人工智慧及經濟發展。 | 一、政府應積極投入資源發展人工智慧，促成人工智慧產業發展經濟規模，鞏固我國在數位科技產業鏈之全球地位，故參考海洋基本法第九條規定，於本條規定政府應建構健全之產業環境，持續培育人才完備人工智慧產業鏈。  二、所稱財稅及金融優惠制度，係指所涉中央目的事業主管機關依第五條第二項辦理之具體人工智慧發展相關措施。為保留其廣泛適用性，於本法揭示原則性、綱要性之精神。 |
| 第九條　（保護及監督機制）  人工智慧資料之蒐集、處理及利用，應審酌人民隱私、資訊自主及產業發展之均衡維護，建立必要之保護及監督機制。 | 人工智慧資料之蒐集、處理及利用，對人民隱私、個人資料有重大影響，政府應衡平其與人工智慧相關產業之發展，建立必要之保護及監督機制。 |
| 第十條　（保護需要協助族群）  人工智慧之研發及利用，應優先考量身心障礙者、高齡者、兒童及其他需要協助族群之權益。 | 一、人工智慧之研發及利用，可能造成社會資源分配不平等，或因而加深身心障礙者、高齡者及兒童等需要協助族群，在社會上或經濟上被孤立之問題。  二、基於包容原則，人工智慧之研發及利用，應優先考量身心障礙者、高齡者及兒童等需要協助族群權益之保護。 |
| 第十一條　（保障勞工權益）  各級政府應就人工智慧利用所致之非自願性失業者，依其工作能力，予以輔導就業。 | 為減緩人工智慧對勞動市場之衝擊，政府應就人工智慧利用所致之非自願性失業，適時提供就業輔導，並依相關勞動法規，保障勞工權益。 |
| 第十二條　（保護公平交易）  政府應防止人工智慧之研發或利用者，以其優勢地位為資料之不當蒐集、處理、利用，或從事不公平競爭，確保交易秩序及消費者權益。 | 政府為確保交易秩序及消費者權益，應防止人工智慧之研發或利用者，以其優勢地位進行不當資料蒐集或實行不公平競爭。 |
| 第十三條　（救濟、補償及保險制度）  政府應審酌人工智慧研發及利用所生之風險，建立必要之救濟、補償及保險制度。 | 人工智慧具有相當程度之風險，若正常或合理使用人工智慧受有損失，應有救濟管道，故政府應審酌人工智慧難以預測之風險，建立必要之救濟、補償及保險制度。 |
| 第十四條　（合於規範標準）  人工智慧之研發及利用，應符合國家標準或相關法規；未訂有國家標準或相關法規未規定者，依各目的事業主管機關所認定得採行之其他先進國家標準或國際標準。 | 人工智慧之研發及利用，與人民權益息息相關，應符合國家標準或國內相關法規。至於國內未訂有國家標準或相關法規未規定者，依各目的事業主管機關所認定得採行之其他先進國家標準或國際標準，俾維護人民基本權利。 |
| 第十五條　（風險評估及監管機制）  政府應控制人工智慧研發及利用之潛在風險，就人工智慧風險訂定分級及判定原則，並建立風險評估及監管機制，進行適當管制。 | 一、人工智慧之發展迅速且利用場域多元，其研發及利用提升產業競爭力，對社會及環境產生明顯之效益，但同時也具有複雜性、不透明性、資料依賴性等特性，可能涉及大量消費者之種族、膚色、基因資料、生物辨識資料、健康、性別、刑事犯罪紀錄、宗教、家庭背景、社經地位等個人資訊，亦可能是系統性監控大型公眾可近用空間，其所產生之後果，可能侵害人民基本權利或造成不利之影響。  二、參考歐盟2021年《人工智慧法案－主席國妥協文本（Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence（Artificial Intelligence Act）and Amending Certain Union Legislative Acts）》草案，以及美國《2022年演算法課責法（Algorithmic Accountability Act of 2022）》草案之規定，為平衡人工智慧新科技可能帶來之風險，避免過度限制或阻礙新技術之發展，政府應建立風險評估及監管機制，依風險特定及高低程度，進行適當管制。  三、政府於建立風險評估及監管機制時，宜參酌歐盟2021年《人工智慧法案－主席國妥協文本》草案，其第二章第五條將最高風險之人工智慧規定為「被禁止之人工智慧」（包含為執法之目的，在公共場所使用即時遠程生物特徵之辨識系統等），其他非屬該條所定之「被禁止之人工智慧」者，則依其風險高低而有不同之監督管理措施。 |
| 第十六條　（品質管理機制）  政府應訂定人工智慧品質管理機制，定期進行安全性、穩定性、可追溯性與可解釋性之評估及監督。 | 一、鑑於人工智慧之風險及特性，政府應有義務督促及監督業者，訂定人工智慧之品質管理機制。  二、為能有效監督及避免人工智慧之風險，政府所訂定之品質管理機制，應包含定期評估人工智慧是否安全、穩定及可追溯。例如，為有效監控高風險人工智慧之研發及利用，確保其安全性及可追溯性，各目的事業主管機關可於國家標準或通用規格規定應具備自動記錄功能，或保存自動生成之日誌。 |
| 第十七條　（技術文件及安全監測計畫）  人工智慧於上市或提供服務前，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向中央目的事業主管機關提出符合法規規定之技術文件，並予公開。  人工智慧之研發及利用，經評估有風險者，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向各目的事業主管機關提出安全監測計畫；其為高風險者，應經核定後，始得為之。 | 一、為確保人工智慧之安全性，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向中央各目的事業主管機關提出符合法規規定之技術文件。例如，利用人工智慧開發之藥品或結合人工智慧運用之醫療器材，為能讓政府適當監管，相關技術文件，應有必要提供予中央目的事業主管機關知悉。另，基於人工智慧之透明性及可解釋性之確保，相關技術文件應予公開，惟涉及營業秘密或專利技術之內容，依相關法令之規定，自當不予公開。  二、再者，為確保人工智慧研發及利用之安全性，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向各目的事業主管機關提出安全監測計畫。例如，新開發之藥品上市後，臨床上為能確保病人藥物使用安全，主管機關及業者應當進行藥品上市後之安全及風險等監控事宜。衡酌人工智慧之運用，與醫療之不可預測性等相近，相關風險之控管，中央目的事業主管機關協力應要求上開人員提供安全監測計畫。高風險人工智慧之安全監測應更嚴格，故其安全監測計畫，應經目的事業主管機關核定。 |
| 第十八條　（安全監測報告）  高風險人工智慧於上市或提供服務後，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應定期向目的事業主管機關提出安全監測報告。 | 一、為因應人工智慧應用之風險及變動性，確保其上市或提供服務後仍符合本法相關規定以及確保安全無虞，主管機關應有必要適時掌握人工智慧之研發、產品與服務之風險及安全。  二、據此，人工智慧之研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應有義務定期向目的事業主管機關提出安全監測之報告，以利目的事業主管機關得確實掌握人工智慧於上市或提供服務後，能持續監管其潛在之風險。 |
| 第十九條　（嚴重不良事件通報）  人工智慧於研發、上市或提供產品、服務後，發生嚴重影響人民生命、身體、自由、人格或財產之情事，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應立即通報目的事業主管機關。 | 為控制人工智慧之風險，人工智慧於研發中、上市或提供產品、服務後，發生嚴重影響人民生命、身體、自由、人格（包括名譽、信用、隱私等）或財產之情事時，參考食品衛生安全管理法第七條第五項，食品業者於發現產品有危害衛生安全之虞時，應通報直轄市、縣（市）主管機關之規定，如人工智慧之利用發生上述情形，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，亦負擔即時通報義務。 |
| 第二十條　（獎勵）  政府對於從事人工智慧研究或推動著有功績之自然人、法人、機構或團體，應給予獎勵，並表揚之。 | 各目的事業主管機關對於相關事項得進行獎勵。相關事項包括：產業之研發創新、技術移轉；政府、產業、學術及研究機構之合作；政府及企業投入學校人才之培育；國際人才之引進等人工智慧發展事項。從事人工智慧研究或施行之機構、人員，對人工智慧之發展有相當貢獻者，政府應予獎勵及表揚。 |
| 第二十一條　（創新實驗環境）  中央目的事業主管機關應建構人工智慧完善且安全之創新實驗環境，輔導相關產業實施實驗；並對符合中小企業發展條例之中小企業，採取適當之補助措施。 | 一、人工智慧創新技術及服務上市前，政府應設置創新實驗環境，提供相關研發及利用之安全場域及實驗空間，以妥善評估創新技術之潛在效益及風險，必要時，得排除相關法規之限制。在現行法下，金融科技發展與創新實驗條例、無人載具科技創新實驗條例，對於人工智慧創新實驗之監理沙盒（Regulatory Sandbox）場域，均以「創新實驗環境」稱之，故本法從之。  二、為促進人工智慧產業發展，政府應協助相關產業進入人工智慧監理沙盒實驗。因中小企業之規模與大型企業存有現實差距，為鼓勵中小企業投入人工智慧產業，政府應對符合相關條件之中小企業，提供積極輔及補助措施。至於中小企業之條件、資格，依中小企業發展條例之規定。 |
| 第二十二條　（促進產業訂定指引及規範）  政府應促進相關產業自行訂定產業指引及行為規範。  前項指引及規範之訂定，應由人工智慧之研發者，或提供產品、服務之自然人、法人、機關、機構或團體及其他利害關係人共同參與。 | 一、基於專業考量，人工智慧企業及機構對其領域特性、產業需求及應用風險最為熟悉，政府應鼓勵及促進多元參與，合作訂定符合產業現況及執行需求之指引及規範。  二、與人工智慧研發及利用相關之研發者，或提供產品、服務之自然人、法人、機關、機構或團體及其他利害關係人，應共同參與討論人工智慧相關產業指引及行為規範之訂定，廣泛匯聚各利害關係人之意見，促進產業之合理規範及健全發展，最佳化產品與服務之標準、實踐及監督。 |
| 第二十三條　（施行日期）  本法自公布日施行。 | 明定本法之施行日期。 |