　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110136320000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11013632 | 號 |  |  |

案由：本院委員陳秀寳、莊瑞雄、許智傑等25人，人工智慧相關技術近年成為全球科技發展趨勢，在世界各國皆有積極發展的動向。人工智慧科技發展可為臺灣整體產業帶來可觀的經濟效益，亦可為社會帶來便捷的服務與資訊的整合；在各個不同的專業領域，如：環境永續、氣候變遷、醫療系統、金融秩序、交通服務、農業發展及公共領域，可望帶來突破性的發展與轉型。臺灣科技相關產業蓬勃發展，位居世界一二，為協助人工智慧相關科技持續發展，政府應建構人工智慧技術發展與應用之良善運作環境，爰擬具「人工智慧基本法草案」，訂定人工智慧相關技術發展應遵守之基本原則及治理方針，提升我國人工智慧科技發展之競爭力。是否有當？敬請公決。

提案人：陳秀寳　　莊瑞雄　　許智傑

連署人：林月琴　　郭昱晴　　黃秀芳　　陳俊宇　　王美惠　　蔡易餘　　王正旭　　邱志偉　　羅美玲　　張雅琳　　李昆澤　　陳培瑜　　陳素月　　徐富癸　　林俊憲　　吳沛憶　　黃　捷　　蔡其昌　　林宜瑾　　陳亭妃　　王世堅　　賴惠員

人工智慧基本法草案總說明

人工智慧相關技術近年成為全球科技發展趨勢，在世界各國皆有積極發展的動向。人工智慧科技發展可為臺灣整體產業帶來可觀的經濟效益，亦可為社會帶來便捷的服務與資訊的整合；在各個不同的專業領域，如：環境永續、氣候變遷、醫療系統、金融秩序、交通服務、農業發展及公共領域，可望帶來突破性的發展與轉型。

人工智慧相關技術預期帶來豐碩的社會及經濟效益，同時卻也可能對個人及社會帶來新型態的風險或影響，世界各國在發展人工智慧時，也傾向在不妨礙人工智慧技術發展的前提下，建立人工智慧治理方針與原則。經濟合作暨發展組織（Organisation for Economic Cooperation and Development，OECD）二○一九年五月通過《人工智慧建議書》（OECD Recommendation on Artificial Intelligence），列出基本價值原則，並提供人工智慧相關政策制定之建議，歐盟亦於同年發布《可信賴AI倫理準則》（Ethics Guidelines for Trustworthy AI），揭示人工智慧發展需留意之共同倫理原則。二○二二年美國發布《AI權利法案藍圖》（Blueprint for an AI Bill of Rights），加拿大亦於同年提出《人工智慧資料法草案》（Artificial Intelligence and Data Act），二○二四年歐盟接著審議通過《人工智慧法》（Artificial Intelligence Act），皆著重於建立人工智慧相關技術發展之原則；日本亦於二○二四年公布《AI業者指引草案》（AI事業者ガイドライン案），提出人工智慧業者應遵守之共通性原則外，並明示具體注意事項，韓國則於二○二四年通過《人工智慧發展與建立信任基本法》（Basic Act on the Development of Artificial Intelligence and the Establishment of Trust），是全球第二部人工智慧專法，著重建立人工智慧信賴基礎並提高國家人工智慧技術之競爭力及風險規範事項。

臺灣科技相關產業蓬勃發展，位居世界一二，為協助人工智慧相關科技持續發展，政府應建構人工智慧技術發展與應用之良善運作環境，並訂定人工智慧相關技術發展應遵守之基本原則及治理方針，提升我國人工智慧科技發展之競爭力；爰擬具「人工智慧基本法」草案，其要點如下：

一、本法之立法目的。（草案第一條）

二、人工智慧之定義。（草案第二條）

三、人工智慧研究發展、應用與監管之基本原則。（草案第三條）

四、政府應積極推動人工智慧研發、應用及基礎建設，並辦理人工智慧相關產業輔導及提供財政優惠措施。（草案第四條）

五、政府應建立或完備人工智慧創新實驗環境，促進人工智慧技術創新與永續發展。（草案第五條）

六、政府應推動人工智慧公私協力與國際合作。（草案第六條）

七、政府應提升國民人工智慧素養，並培育人工智慧人才。（草案第七條）

八、政府應提供或建議評估驗證之工具或方法，以利防止人工智慧違法應用。（草案第八條）

九、政府應推動人工智慧風險分類規範。（草案第九條）

十、政府應根據風險分類，評估潛在弱點及濫用情形並建立緊急應變措施，提升人工智慧之可驗證性及人為可控性。（草案第十條）

十一、政府應建立人工智慧應用負責機制，明確責任歸屬要件。（草案第十一條）

十二、政府應保障勞工權益，輔導因人工智慧利用所致之失業者就業。（草案第十二條）

十三、政府應避免不必要之個人資料蒐集、處理或利用，並應促進個人資料保護納入預設及設計之相關措施或機制，以保障國民隱私權益。（草案第十三條）

十四、政府應提升資料利用性及人工智慧使用資料之品質與數量，並避免使用錯誤或虛偽之資料；確保人工智慧訓練及生成結果維繫國家文化價值與維護智慧財產權。（草案第十四條）

十五、政府使用人工智慧執行業務或提供服務，應進行風險評估，規劃風險因應及緊急應變措施；訂定使用規範或內控管理機制。（草案第十五條）

十六、政府應檢討與人工智慧相關之主管法規，在符合本法第三條基本原則之前提下，由中央目的事業主管機關協同中央科技主管機關，依本法規定解釋、適用之。（草案第十六條）

十七、本法之施行日期。（草案第十七條）

|  |  |
| --- | --- |
| 人工智慧基本法草案 | |
| 條文 | 說明 |
| 第一條　為促進以人為本之人工智慧研發與應用，保障國民人格尊嚴及權利，提升國民生活福祉、維護國家主權、延續文化價值及厚植科技實力，促進永續發展及國家競爭力，特制定本法。 | 一、明定本法之立法目的。  二、人工智慧為攸關未來國家發展之重點科技，為積極發展與應用人工智慧，強化與深耕以人為本之人工智慧技術，促進相關技術之應用與科技產業發展，同時保障憲法賦予之人格尊嚴及包括生命、身體、健康、安全等國民權利。人工智慧之發展應重視人文與社會發展所需，並以提升國民生活福祉、維護國家主權、延續文化價值及厚植科技實力為首要目標，進而促進社會永續發展。 |
| 第二條　本法所稱人工智慧，係指具自主運行能力之系統，該系統透過輸入或感測，經由機器學習與演算法，可為明確或隱含之目標實現預測、內容、建議或決策等影響實體或虛擬環境之產出。 | 參酌美國國家AI創新法案（National AI Initiative Act of 二○二○）美國法典（U.S. Code）第九四○一章、國際標準化組織（ISO）及國際電工委員會（IEC）聯合制定技術規範（ISO/IEC）四二○○一：二○二三人工智慧管理系統、美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）人工智慧風險管理框架（Artificial Intelligence Risk Management Framework），以及歐盟人工智慧法（Artificial Intelligence Act）對於人工智慧系統之定義，人工智慧必須被設計為具備不同程度之自主運行能力，透過輸入或感測，可為明確或隱含之特定目的，經過機器學習與演算法實現諸如預測、內容、建議或決策等影響實體或虛擬環境之產出，與其他軟體系統有別。 |
| 第三條　人工智慧之研發、應用與監管，應在兼顧社會公益與數位平權之前提下，發展良善治理，並遵循下列原則：  一、永續性：應兼顧社會公平及環境永續，降低可能之數位落差，使國民適應人工智慧帶來之變革。  二、人類自主性：應以支持人類自主權、尊重人格權等個人基本權利與文化價值，並允許人類監督，落實以人為本並尊重法治及民主價值觀。  三、隱私保護與資料治理：應妥善保護個人資料隱私，避免資料外洩風險，並採用資料最小化原則；及在符合隱私權保障之前提下，促進非敏感資料之開放及再利用。  四、安全性：人工智慧研發與應用過程，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性與安全性。  五、透明與可解釋性：人工智慧之產出應有適當資訊揭露或標記及避免使用不實資訊，以利評估可能風險，並瞭解對相關權益之影響，進而提升人工智慧可信任度。  六、公平性：人工智慧研發與應用過程中，應盡可能避免演算法產生偏差及歧視等風險，不應對特定群體造成歧視之結果。  七、可問責性：確保人工智慧研發與應用過程中不同角色承擔相應之責任，包含內部治理責任及外部社會責任。 | 一、我國發展人工智慧應衡平創新發展與潛在風險，發展以人為本之人工智慧，並視人文及社會所需，並以提升國民生活福祉、維護國家主權、延續文化價值及厚植科技實力為目標。爰參考國際協議及各國相關政策方針、法規或行政命令，訂定具有指標與引導功能之基礎準則，以作為人工智慧之研發與應用之基本原則。  二、人工智慧研發與應用應兼顧社會公平與環境之發展，以追求對社會有益之結果，並從而促進永續發展，爰參考G7廣島AI國際行動規範（Hiroshima Process Code of Conduct for Organizations Developing Advanced AI Systems），於第一款明定。  三、人工智慧研發與應用應在人工智慧系統之整個運行過程中尊重法治、人權及民主價值觀，爰參考經濟合作暨發展組織（OECD）二○一九年公布之人工智慧建議書（OECD Recommendation on Artificial Intelligence），於第二款明定應支持人類自主性及尊重人格權等個人基本權利、與文化價值，落實以人為本之基本價值。  四、人工智慧發展仰賴大量的資料，惟資料之蒐集、處理以及利用，須保障資料安全與個人資料隱私，爰參考美國二○二二年AI權利法案藍圖（Blueprint for an AI Bill of Rights）於第三款明定人工智慧研發與應用，應避免資料外洩風險，並採用資料最小化原則；即指各階段蒐集之個人資料，皆須適當且具相關性，並僅止於符合資料處理目的所需之程度。同時，促進非敏感資料之開放及再利用。  五、人工智慧研發與應用應確保系統穩健性與安全性，爰參考美國二○二二年AI權利法案藍圖（Blueprint for an AI Bill of Rights）及新加坡二○二三年生成式AI治理架構草案（Proposed Model AI Governance Framework for Generative AI），於第四款明定，以防範人工智慧有關安全威脅與攻擊。  六、人工智慧所生成之內容將對使用者及社會帶來重大影響，蓋須保障人工智慧運行過程之公正性。人工智慧研發與應用階段，應致力維持生成內容之準確性，避免使用不實資訊，並提升可讓使用者及受影響者理解其影響及運行過程之可解釋性，進而提升人工智慧可信任度；爰參考歐盟二○一九年可信賴AI倫理準則（Ethics Guidelines for Trustworthy AI）於第五款明定透明與可解釋性之原則。  七、人工智慧研發與應用須公平、完善且演算法應避免產生偏差或歧視之結果，爰參考美國二○二二年AI權利法案藍圖（ Blueprint for an AI Bill of Rights），於第六款明定公平性原則，強調應重視社會多元包容，避免產生偏差與歧視等風險，且不應對特定群體造成歧視之結果。  八、研發與應用人工智慧應致力於建立人工智慧應用負責機制，以維護社會公益。爰參考新加坡二○二三年生成式AI治理架構草案（Proposed Model AI Governance Framework for Generative AI）對於人工智慧開發運用的運行過程中，確保不同角色應承擔相應之責任；爰於第七款訂定可問責性原則。 |
| 第四條　政府應積極推動人工智慧研發、應用及基礎建設，妥善規劃資源整體配置，並辦理人工智慧相關產業之補助、委託、出資、獎勵、輔導，或提供租稅、金融等財政優惠措施。 | 人工智慧發展與應用涉及領域甚廣，整體資源規劃與國家政策之未來發展，由政府各機關依其業務職掌負責辦理，爰參考《產業創新條例》第九條及《科學技術基本法》第六條，明定政府機關應積極推動人工智慧發展及可運用之推動方式。 |
| 第五條　為促進人工智慧技術創新與永續發展，各目的事業主管機關得針對人工智慧創新產品或服務，建立或完備人工智慧研發與應用服務之創新實驗環境。 | 參考歐盟人工智慧法，鼓勵建立人工智慧實驗沙盒制度，提供一個受控環境，以促進人工智慧之創新，在人工智慧投放市場或投入使用前，可全面開發、測試和驗證。爰明定各目的事業主管機關得建立或完備有關人工智慧研發與應用之創新實驗環境，促進人工智慧之發展。 |
| 第六條　政府宜以公私協力方式，與民間合作，推動人工智慧創新運用。  政府應致力推動人工智慧相關之國際合作，促進人才、技術及設施之國際交流與利用，並參與國際共同開發與研究。 | 一、考量人工智慧應用與發展事務涵蓋範圍廣泛，故於第一項明定政府除應就其業務權責範圍內，推動人工智慧之研發與應用外，亦宜與民間合作推動人工智慧創新運用，帶動人工智慧發展。  二、參考《科學技術基本法》第二十一條，明定政府應積極發展人工智慧相關之國際合作，促進人才及技術等相關國際交流；並參與國際共同開發與研究，爰為第二項規定。 |
| 第七條　為加強國民對人工智慧之關心與認識，政府應持續推展各級學校、產業、社會及公務機關（構）之人工智慧教育，以提升國民人工智慧之素養及培育人工智慧人才。 | 為落實二○二三年行政院科技顧問會議結論全面推動人工智慧素養教育，爰參考《科學技術基本法》第二十二條，明定政府應推動各級學校、產業、社會及公務機關（構）之人工智慧教育，以提升國民人工智慧之素養；並未因應未來發展人工智慧之需求，培育相關人才投入人工智慧發展。 |
| 第八條　政府應避免人工智慧之研發及應用，造成國民生命、身體、自由或財產安全、社會秩序、生態環境之損害，或出現利益衝突、偏差、歧視、不實資訊、資訊誤導或造假等問題而違反相關法規之情事。  數位發展部及其他相關機關應提供或建議評估驗證之工具或方法，以利各目的事業主管機關辦理前項事項。 | 一、參考美國總統二○二三年發布之人工智慧行政命令（Executive Order on Safe,Secure,and Trustworthy Artificial Intelligence）於第一項明定政府應避免人工智慧之研發過程及實際應用造成國民權益受損或生態環境損害；同時亦應避免出現利益衝突、偏差、歧視、不實資訊、資訊誤導或造假等問題，違反如：《兒童及少年福利與權益保障法》、《公平交易法》、《消費者保護法》及《個人資料保護法》等相關法規之情事。  二、為利各目的事業主管機關辦理前項業務，數位發展部及其他相關機關應研議並提供國內外評估驗證之工具或方法，以利各目的事業主管機關辦理前項事項，並保障國民權益，爰為第二項規定。 |
| 第九條　數位發展部應參考國際標準或規範，推動與國際介接之人工智慧風險分類框架。  各目的事業主管機關得循前項風險分類框架，訂定其主管業務之風險分類規範。 | 一、政府推動人工智慧之研發與應用，應以風險為基礎，確保人工智慧安全、穩定運行並避免造成國民權益損害。為使人工智慧風險分類規範與配套驗證確保機制與國際接軌，爰於第一項明定由數位發展部參考國際標準或規範，推動人工智慧風險分類框架。  二、各目的事業主管機關因所涉專業領域不同，得循前項風險分類框架再訂定主管業務適用之風險分類及相關管理規範，爰為第二項規定。 |
| 第十條　政府應識別、評估及降低人工智慧之使用風險，透過法規、標準或指引等，於促進人工智慧研發與應用之同時，根據風險分類，評估潛在弱點及濫用情形並建立緊急應變措施，提升人工智慧決策之可驗證性及人為可控性。 | 為利各機關落實分類評估及管理，透過法規、標準（包括產業標準、國家標準、國際標準）或指引等方式，協助各界採取因應風險之措施，爰參考美國總統二○二三年發布之人工智慧行政命令定之，並在評估潛在弱點及濫用情形後，建立緊急應變措施，於人工智慧發生危害時，政府有即時應變能力，防止損害擴大；以提升人工智慧決策之可驗證性及人為可控性。 |
| 第十一條　政府應依人工智慧風險分類，透過標準、驗證、檢測、標記、揭露、溯源或問責等機制，提升人工智慧應用可信任度，並建立人工智慧應用條件、責任、救濟、補償或保險等相關規範，明確責任歸屬與歸責條件。  人工智慧技術開發與研究，於應用前之任何活動，除應遵守第三條之基本原則外，不適用前項應用責任相關規範，以利技術創新發展。 | 一、人工智慧應用時，應有明確方式降低可能風險，爰參酌美國NIST AI風險管理框架所訂定之安全標準與驗證機制、人工智慧產出之標記或資訊揭露機制、透明可解釋之溯源或問責機制等；於第一項要求各機關應建立歸責機制，且應包含外國人工智慧產品落地規範，以保障國民權益。  二、為避免影響學術研究自由及產業前端研發，參酌歐盟人工智慧法第二條第八項之規定，人工智慧投入市場實際運用前的任何研究、測試或開發活動僅需根據適用之歐盟法律進行，除於真實世界測試外，不適用人工智慧法相關規範；爰訂定第二項，人工智慧技術開發與研究，於應用（包含人工智慧商品或服務之應用或於真實世界測試）前之任何活動，除應遵守第三條之基本原則外，不適用應用責任相關規範，以利人工智慧科技創新發展。 |
| 第十二條　政府為因應人工智慧發展，應避免技能落差，並確保勞動者之職業安全衛生、勞資關係、職場友善環境及相關勞動權益。  政府應就人工智慧利用所致之失業者，依其工作能力予以輔導就業。 | 一、因應人工智慧發展，為避免勞動者於需使用及應用人工智慧技術從事及執行該職務工作時，欠缺人工智慧相關技能，並須確保勞動者的權益，包含職業安全衛生、勞資關係及職場友善環境等。爰參酌美國總統二○二三年發布之人工智慧行政命令訂定第一項之規定，以保障國民勞動權益。  二、為避免人工智慧造成之失業情事，爰於第二項明定政府應提供因人工智慧利用所致之失業者輔導就業措施。 |
| 第十三條　個人資料保護主管機關應協助各目的事業主管機關，在人工智慧研發及應用過程，避免不必要之個人資料蒐集、處理或利用，並應促進個人資料保護納入預設及設計之相關措施或機制，以維護當事人權益。 | 為保障國民個人資料及隱私權益，參考美國二○二二年AI權利法案藍圖（Blueprint for an AI Bill of Rights）及美國總統二○二三年發布之人工智慧行政命令，由個人資料保護主管機關協助各目的事業主管機關，在人工智慧研發及應用過程，避免不必要之個人資料蒐集、處理或利用，並配合其業管法規建立個人資料保護納入預設及設計之相關措施或機制。 |
| 第十四條　政府應建立資料開放、共享與再利用機制，提升人工智慧使用資料之可利用性，並定期檢視與調整相關法令及規範。  政府應致力提升我國人工智慧使用資料之品質與數量並避免使用錯誤或虛偽之資料，確保人工智慧訓練及生成結果維繫國家多元文化價值與維護智慧財產權。 | 一、資料為人工智慧發展之重要基礎，政府有必要確保人工智慧之創新與產業發展，爰參酌歐盟人工智慧法及美國總統二○二三年發布之人工智慧行政命令，爰於第一項明定政府須定期檢視相關法規並為必要調整，俾利人工智慧發展。  二、為確保人工智慧訓練及生成結果之正確性及維繫國家多元文化價值，避免影響國民權益，於第二項明定政府應致力提升人工智慧使用資料之品質與數量，並避免使用錯誤或虛偽之資料，以完善我國資料治理機制。 |
| 第十五條　政府使用人工智慧執行業務或提供服務，應進行風險評估，規劃風險因應及緊急應變措施。  機關（構）應依使用人工智慧之業務性質，訂定使用規範或內控管理機制。 | 一、考量政府使用人工智慧協助執行業務或提供服務，有助於行政效率之提升，爰參酌英國二○二四年「生成式人工智慧治理框架」，按本法第九條之風險分類規範，要求政府機關（構）執行公務應進行風險評估、規劃風險因應及緊急應變措施，以保障國民權益。  二、為促使各機關依一致的原則使用人工智慧，於第二項明定機關（構）應依使用人工智慧之業務性質，訂定使用規範或內控管理機制。 |
| 第十六條　政府應於本法施行後依本法規定檢討及調整所主管之職掌、業務、法規或訂定指引，以落實本法之目的。  前項法規制（訂）定或修正前，既有法規未有規定者，在符合第三條基本原則之前提下，以促進新技術與服務之提供為原則，由中央目的事業主管機關協同中央科技主管機關，依本法規定解釋、適用之。 | 一、為確保人工智慧技術之有效推動發展並兼顧國民權益，爰參酌《教育基本法》第十六條、《通訊傳播基本法》第十六條、《原住民族基本法》第三十四條、《海洋基本法》第十六條，於第一項明定檢討職掌、業務、法規或訂定指引，以落實本法。  二、依第一項規定應訂修或廢止之相關法規，於未完成法定程序前，為使相關事務能符合本法規定，參酌《海洋基本法》第十六條，明定中央目的事業主管機關應依本法規定完善人工智慧發展相關法規之解釋及適用。爰於第二項明定由中央目的事業主管機關協同中央科技主管機關，依本法規定解釋、適用之。 |
| 第十七條　本法施行日期，由行政院定之。 | 明定本法施行日期。 |