　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110146260000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11014626 | 號 |  |  |

案由：本院委員伍麗華Saidhai Tahovecahe、許智傑等21人，鑒於近年人工智慧技術發展快速，在各領域皆已具有一定程度之影響力，為免社會大眾使用相關技術時無所措其手足，其法規之建制刻不容緩。為促進以人為本之人工智慧發展，爰擬具「人工智慧基本法草案」，以建構優良之人工智慧技術應用環境。是否有當？敬請公決。

提案人：伍麗華Saidhai Tahovecahe　　　　許智傑

連署人：邱議瑩　　范　雲　　徐富癸　　黃秀芳　　陳俊宇　　陳素月　　李柏毅　　林楚茵　　王世堅　　蔡易餘　　吳沛憶　　賴瑞隆　　沈伯洋　　郭昱晴　　王義川　　王美惠　　張雅琳　　陳　瑩　　王定宇

人工智慧基本法草案總說明

人工智慧技術近年來飛躍性成長，世界各國已普遍將之運用於各個領域，帶來廣泛之經濟和社會效益。我國身為科技大國，人工智慧之運用更是發展關鍵及競爭優勢之所在，亦須積極採用人工智慧技術已推動數位轉型與永續發展。因此，相關法規之建制刻不容緩。

一、本法之制定目的。（草案第一條）

二、人工智慧定義。（草案第二條）

三、人工智慧研究發展及應用之基本原則。（草案第三條）

四、政府應推動人工智慧研究發展與應用。（草案第四條）

五、政府應建立或完備人工智慧創新實驗環境。（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、政府應推動人工智慧人才培育與素養教育。（草案第七條）

八、政府應評估驗證人工智慧防止違法應用。（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、政府應強化人工智慧人為可控性（草案第十條）

十一、政府應建立人工智慧應用負責機制。（草案第十一條）

十二、政府應保障勞工權益。（草案第十二條）

十三、政府應落實對於需要協助族群之保護（草案第十三條）

十四、政府應保障個資隱私。（草案第十四條）

十五、政府應提升資料利用性與國家文化價值。（草案第十五條）

十六、政府公務使用人工智慧之原則。（草案第十六條）

十七、政府應檢討主管法規。（草案第十七條）

十八、本法施行日。（草案第十八條）

|  |  |
| --- | --- |
| 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、確保公平正義、維護國家主權及文化價值，健全人工智慧安全與治理環境，強化永續發展及國家競爭力，特制定本法。 | 一、本法之立法目的。  二、人工智慧為攸關國家發展之戰略性科技，發展人工智慧相關條例刻不容緩，包含強化以人為本的人工智慧技術、促進技術與產業發展、保障人民與國家安全、邁向永續發展等、建立法律基礎等。期望透過本次立法，達成技術進步與社會福祉的平衡，推動國家邁向智慧永續的未來。 |
| 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。 | 人工智慧系統需具備一定程度的自主運行能力，透過輸入（input）或感測（sensing），以實現明確（explicit）或隱含（implicit）之特定目的（objectives）。系統經由機器學習（machine learning）與演算法（algorithms）產出預測、內容、建議或決策，對實體或虛擬環境產生影響，並與一般軟體系統有本質差異。該定義參考《美國國家人工智慧創新法案》（National AI Initiative Act of 2020）、ISO/IEC 42001：2023、NIST AI風險管理框架及歐盟《人工智慧法》。 |
| 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：平衡社會公平與環境永續，提供適當的教育與培訓，縮小數位落差，協助國民適應人工智慧帶來的變革。  二、人類自主性：支持人類自主權，尊重人格權及其他基本權利，維護文化價值，允許人類監督，並落實法治與民主價值觀。  三、隱私保護與資料治理：妥善保護個人資料隱私、尊重企業營業秘密、避免資料外洩風險，並應盡可能於適當情形採用資料最小化原則；同時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，防範不實資訊、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：人工智慧之產出應在技術上可行的情形下，做適當資訊揭露或標記，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、公平性與反歧視：人工智慧之研發與應用，應致力防止演算法偏差與歧視風險，對特定群體造成偏見之結果應予以最小化。  七、合於規範標準：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國家標準或國際標準。  八、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、政府應在推動人工智慧研發與應用時，平衡創新發展與可能風險，訂定引導性原則，作為各機關推動相關政策的基礎，以回應國內人文與社會需求。  二、永續發展與福祉：人工智慧利益相關者應積極參與可信任人工智慧的負責管理，追求對人類及地球有益的結果，促進永續發展與社會福祉。此原則參考G7《廣島AI國際行動規範》（Hiroshima Process Code of Governance Framework for Generative AI Systems）。  三、人類自主與基本權利：人工智慧系統需尊重法治、人權及民主價值，確保支持人類自主，尊重基本權利、人格權（含姓名、肖像、聲音）與文化價值，落實以人為本的核心價值。此原則參考OECD《人工智慧建議書》（OECD Recommendation on Artificial Intelligence）。  四、隱私保護與資料治理：人工智慧發展依賴大量資料，需確保資料蒐集、處理與利用的安全性與隱私保護，遵循資料最小化原則，降低外洩風險，同時促進非敏感資料的開放與再利用。此原則參考美國《AI權利法案藍圖》（Blueprint for an AI Bill of Rights）。  五、資安與安全：人工智慧研發與應用應建立穩健性與安全性，防範安全威脅與攻擊，確保系統運行的可靠性。此原則參考《AI權利法案藍圖》（Blueprint for an AI Bill of Rights）及新加坡《生成式AI治理架構草案》（Proposed Model AI Governance Framework for Generative AI）。  六、透明與可解釋：人工智慧生成的決策需對利害關係人具有重大影響，應致力於提升決策過程的透明性與可解釋性，保障使用者與受影響者的權益。此原則參考歐盟《可信賴人工智慧倫理準則》（Ethics Guidelines for Trustworthy AI）。  七、公平與不歧視：人工智慧系統應避免演算法偏差與歧視，確保公平性，並促進多元包容。此原則參考美國《AI權利法案藍圖》（Blueprint for an AI Bill of Rights）。  八、問責機制：人工智慧的研發與應用者需建立負責機制，維護社會公益與利害關係人利益，確保技術應用的可問責性。此原則參考新加坡《生成式AI治理架構草案》（Proposed Model AI Governance Framework for Generative AI）。 |
| 第四條　政府應積極推動人工智慧之研發、應用及基礎建設，妥善規劃整體資源配置，並得以補助、委託、出資、獎勵、輔導等方式，支持人工智慧相關產業之發展，同時提供租稅、金融等財政優惠措施，以促進其持續成長。 | 人工智慧發展與應用涉及領域甚廣，其整體資源規劃，應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之相關規定，定明政府機關應推動人工智慧發展之運用方式。 |
| 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就人工智慧創新產品或服務，建立或完善人工智慧研發與應用服務之創新實驗環境。 | 本條規定建立或完善現有人工智慧研發與應用服務的創新實驗環境，參考歐盟人工智慧法，鼓勵各國政府設立人工智慧實驗沙盒（Regulatory Sandbox）制度，提供一受控環境，促進人工智慧創新。此環境使得人工智慧可在投入市場或實際應用前，於限定時間內進行開發、測試與驗證，從而讓國民受惠於人工智慧的創新科技。 |
| 第六條　政府宜以公私協力方式與民間合作，共同推動人工智慧之創新應用。  政府應積極推動人工智慧相關之國際合作，促進人才、技術、設施及應用之國際交流與利用，並參與國際間之共同開發與研究。 | 一、考量人工智慧應用與發展事務涵蓋範圍相當廣泛，明定政府各機關除應就其業務權責推動、辦理外，亦應積極與民間合作推動人工智慧發展。  二、參考科技基本法第二十一條國際科學技術合作相關規定，於第二項明定政府應積極就人工智慧與國際交流及合作。 |
| 第七條　為增進國民對人工智慧之關注與認識，政府應持續推動各級學校、產業、團體、社會及各級公務機關（構）之人工智慧及其倫理教育，以提升國民之人工智慧素養。 | 為落實二○二三年行政院科技顧問會議全面推動人工智慧素養教育之結論，本條參考科技基本法二十二條，明定政府應於各機關（構）推動人工智慧教育。 |
| 第八條　政府應避免人工智慧之應用對國民生命、身體、自由或財產安全、社會秩序與生態環境造成損害，並應防止因利益衝突、偏差、歧視、廣告不實、資訊誤導或造假等情形，致違反相關法規之情事。  數位發展部及其他相關機關得提供或建議具可行性且明確之評估驗證工具或方法，以利各目的事業主管機關辦理前項事項。 | 一、第一項參考美國總統二○二三年發布之AI行政命令（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence），明定政府應避免人工智慧之應用違反相關法規（例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），而侵害國民生命、身體、自由或財產安全，或造成社會秩序、生態環境損害，或出現利益衝突、偏差、歧視、廣告不實、資訊誤導或造假等情事。  二、數位發展部應會同各目的事業主管機關提供前項之評估驗證工具、方法及其相關事項。 |
| 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、政府在推動人工智慧研發與應用時，應著重於人工智慧資訊安全保護、風險分級與管理，並推動與國際標準接軌的人工智慧風險分級框架。各主管機關可依此風險分級框架，訂定適用於其領域的風險分級規範，確保人工智慧系統的安全與穩定運行。為了使風險分級規範與國際標準相符，數位發展部應參考國際標準或規範，推動人工智慧風險分級框架，例如歐盟人工智慧法中所訂定的四級風險分類，並涵蓋禁止的人工智慧行為（prohibited AI practices）等。  二、由於各主管機關所管轄的領域不同，應依照前述風險分級框架，為各自的業務範疇制定相應的風險分級及管理規範。 |
| 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，提升人工智慧決策之可驗證性及人為可控性。  政府應建立人工智慧濫用與危害的即時偵測、緊急應變與緊急處分的能力。 | 為利各機關落實分級評估及管理，爰參考美國二○二三年發展與使用安全且可信任的AI行政命令（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence）定其標準、規範或指引等方式，協助各界採取因應風險之措施，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，建立人工智慧應用之條件、責任、救濟、補償或保險等相關規範，以明確責任歸屬及歸責條件。  人工智慧技術開發與研究，於應用前之任何階段，除應遵循第三條所定之基本原則外，不適用前項應用責任相關規範，以利技術創新發展。 | 一、在人工智慧應用過程中，應採取明確措施來降低可能的風險，這包括遵循美國NIST AI風險管理框架所設的安全標準與驗證機制、對AI產出進行標記或資訊揭露、以及建立透明且可解釋的溯源與問責機制等。此外，各機關應建立負責的應用機制，包括針對外國AI產品的落地規範，以降低民眾遵守法律的成本。  二、為避免影響學術研究自由及產業前端研發，歐盟人工智慧法第二條第八項規定，在AI投入市場前的任何研究、測試或開發活動僅需依照適用的歐盟法律進行，不受人工智慧法的規範。因此，人工智慧技術開發與研究在應用前的任何活動，除應遵循第三條的基本原則外，不適用應用責任相關規範，以促進技術創新與發展。 |
| 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。  政府應對因人工智慧利用所致之失業者，依其工作能力提供就業輔導與協助。 | 一、為應對人工智慧的發展，政府應確保勞動者具備必要的人工智慧相關技能，避免因技能落差影響其勞動條件與權益，並保障職業安全衛生、勞資關係及職場友善環境等勞動者基本權利。此舉應參照美國二○二三年《發展與使用安全且可信任的AI行政命令》（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence）之規範。  二、政府應針對人工智慧技術應用所可能引發的非志願性失業，提供適當的就業輔導措施。並依照相關勞動法規，保障勞工權益，減少人工智慧對勞動市場造成的衝擊，協助勞動者適應職業轉型與技能提升。 |
| 第十三條　人工智慧之研發及利用，應促進多元性，避免對特定族群產生偏見，並應優先考量原住民族、身心障礙者、高齡者、兒童及其他不利處境群體之權益。 | 參考韓國《智慧資訊化基本法》（Framework Act on Intelligent Informatization），在立法層面上強調人工智慧與數據資料的結合，並重視數位基礎設施的完善，以防止在人工智慧時代出現新的資訊落差。同時，爰引用聯合國及我國人權會之用字，特別保障原住民族、高齡者、身心障礙者等不利處境族群之權益，以避免智慧資訊化發展帶來潛在的負面影響。 |
| 第十四條　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。 | 為降低資料外洩風險及避免蒐集過多不必要的敏感資訊，參考美國二○二二年《AI權利法案藍圖》（Blueprint for an AI Bill of Rights）及二○二三年《發展與使用安全且可信任的AI行政命令》（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence），建議由我國個人資料保護法主管機關協助各目的事業主管機關，依其業管法規推動將個人資料保護納入預設與設計的相關措施或機制（data protection by design and by default）。例如，數位發展部已發布的隱私強化技術應用指引，即為參考範例，旨在全面提升個人資料保護水準。 |
| 第十五條　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，確保人工智慧訓練及產出結果維繫國家多元文化價值與維護智慧財產權。 | 一、資料是推動人工智慧發展的核心資源，政府應確保人工智慧創新及產業發展能獲取高品質且可追溯的資料。參考歐盟《人工智慧法》中支援高品質資料可近用的規定，以及美國《AI行政命令》要求聯邦資料長委員會制定資料開放指引的措施，爰於第一項規範，政府應定期檢視相關規範，並視需要進行調整，以促進人工智慧發展所需的資料環境。  二、為確保人工智慧訓練結果能維護國家文化價值，並避免損害弱勢及多元族群的權益或侵犯人民的智慧財產權，於第二項明定各機關應積極推動完善資料治理機制，以促進公平、包容及合乎社會期待的人工智慧發展環境。 |
| 第十六條　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。 | 考量政府各機關使用人工智慧協助執行業務或提供服務，能有效提升行政效率，應參酌第十條規範之風險分級機制，進行全面的風險評估並規劃適切的因應措施。參考英國二二○二四年《生成式人工智慧治理框架》，要求政府機關在執行公務時，應進行風險評估並制定風險因應措施，以確保符合第三條所揭示的基本原則。此舉可促進各機關在共同原則與一致認知下，制定人工智慧應用的內部使用規範及內控管理機制，確保人工智慧應用的穩健性與公信力。 |
| 第十七條　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、業務及法規，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推動與發展能落實於實際運作，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》第三十四條及《海洋基本法》第十六條，於第一項明定由行政院統籌各部會，全面檢討現行法規及相關機制措施，以促進人工智慧相關政策的有效執行。  二、針對依第一項檢討結果需修訂或廢止的相關法規，於法定程序完成前，為確保相關事務能符合法律精神，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，依據本法規定進行解釋與適用，以確保人工智慧發展的連續性與法規調適的靈活性。 |
| 第十八條　本法施行日期，由行政院定之。 | 本法施行日。 |