　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110129290000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11012929 | 號 |  |  |

案由：本院委員林宜瑾、許智傑等26人，鑒於人工智慧技術發展一日千里，為產業及社會活動帶來嶄新變革。惟其大量資訊儲存等特性，以及日後可能持續發展的自我學習模型，將對人類社會帶來未知的資訊應用風險。參考國外規範，諸多國家都已針對當前最新型人工智慧技術訂定規範或指引，我國應跟進並制定基本原則以規範人工智慧使用，實有在不妨礙產業創新之前提下，建構人工智慧安全使用環境、落實法律治理之必要，爰擬具「人工智慧基本法草案」。是否有當？敬請公決。

提案人：林宜瑾　　許智傑

連署人：張雅琳　　吳秉叡　　蘇巧慧　　邱議瑩　　林淑芬　　沈伯洋　　吳琪銘　　賴惠員　　黃　捷　　徐富癸　　張宏陸　　陳培瑜　　王義川　　郭昱晴　　李坤城　　黃秀芳　　蔡其昌　　范　雲　　吳沛憶　　王正旭　　李昆澤　　李柏毅　　沈發惠　　鍾佳濱

人工智慧基本法草案總說明

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，並為我國企業及國家發展提供關鍵之競爭優勢。在氣候變遷、環境、醫療、金融、交通、內政、農業、公共服務等對民眾具廣泛影響力之領域中，更亟需積極採用人工智慧技術以推動數位轉型與永續發展。

人工智慧技術雖帶來社會及經濟效益，同時也可能對個人或社會帶來新的風險或影響。鑑於人工智慧技術創新之速度及可能面臨之挑戰，全球主要國家皆致力在不妨礙技術發展下，尋求建立人工智慧之治理方針與原則。經濟合作暨發展組織（Organisation for Economic Cooperation and Development，OECD）於二○一九年五月通過「人工智慧建議書」（OECD Recommendation on Artificial Intelligence），提出基本價值原則，並給予各國政策制訂者相關建議；同年歐盟發布「可信賴AI倫理準則」（Ethics Guidelines for Trustworthy AI），確保人工智慧發展所需之共同倫理原則。於此之後，如歐盟於二○二一年提出「人工智慧法」（Artificial Intelligence Act），二○二四年通過審議、美國於二○二二年發布「AI權利法案藍圖」（Blueprint for an AI Bill of Rights）、加拿大亦於二○二二年提出「人工智慧資料法草案」（Artificial Intelligence and Data Act），皆著重於建立人工智慧技術發展之原則並建立大眾信任；美國總統復於二○二三年發布「發展與使用安全且可信任的人工智慧行政命令」（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence）訂立聯邦各部門人工智慧發展之推動任務。就鄰近之亞洲國家而言，日本於二○一七年提出「人工智慧技術戰略」（人工知能技術戰略），旨在促進AI的研發、應用以及與各行業的融合。二○一九年「人工智慧社會原則」（AI社會原則）提出了AI應用的倫理標準。該指南強調AI技術的透明性、公平性、隱私保護以及對人類尊嚴的保護，並希望AI技術的發展能夠造福社會，而不是導致新的不平等或問題。

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。故此，制定人工智慧發展之基本法律，從基本原則、政府推動重點等構面提出基本價值、治理原則及施政方針，期使我國人工智慧發展促進創新兼顧人權與風險，進而提升我國競爭力，爰擬具「人工智慧基本法」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、維護國家主權及文化價值，建構人工智慧安全環境，增進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科技，為積極發展與應用人工智慧，強化與深耕以人為本（human-centered）之人工智慧技術，促進技術應用與產業發展，同時保障憲法規定之人格尊嚴及國民權利、建構人工智慧安全環境，以期人工智慧可回應人文與社會發展所需，邁向社會永續發展。因此，發展與應用人工智慧之同時，有賴於制定具有指標與引導性原則之立法，以作為發展並管制人工智慧之規範與促進應用之法源基礎。 |
| 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。 | 參考美國國家人工智慧創新法案（National AI Initiative Act of 2020）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，說明人工智慧必須被設計為具備不同程度之自主運行能力（AI systems are designed to operate with varying levels of autonomy），透過輸入（input）或感測（sensing），可為明確（explicit）或隱含（implicit）之特定目的（objectives），經過機器學習（machine-learning）與演算法（algorithms）實現諸如預測、內容、建議或決策（such as predictions ,content, recommendations,or decisions）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、尊重人格權等人類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、人權及民主價值觀。  三、隱私保護與資料治理：應妥善保護個人資料隱私、尊重企業營業秘密、減輕資料外洩風險，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：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，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、我國發展人工智慧應衡平創新發展與可能風險，以回應國內人文及社會所需。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、經濟之協調發展，以追求對人類和地球有益之結果，從而促進永續發展（Sustainable development），爰參考G7廣島AI國際行動規範（Hiroshima Process  Code of Conduct for Organizations Developing Advanced AI Systems），於第一款定明之。  三、人工智慧研發與應用應在人工智慧系統之整個生命週期中尊重法治、人權及民主價值觀，為此，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），於第二款定明應支持人類自主性（Human Autonomy），並尊重人格權（含姓名、肖像、聲音）等個人基本權利、與文化價值，確保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，能否確保資料安全與個人資料隱私，是目前人工智慧發展最多討論與疑慮之議題。同時，企業的營業祕密能否得到確保，是產業界關注之所在。爰參考美國二○二二年AI權利法案藍圖（Blueprint for an AI Bill of Rights）於第三款定明人工智慧研發與應用，應盡可能避免、減輕資料外洩風險，並採用資料最小化原則，而所謂資料最小化原則（data minimization），係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（非個人或機敏）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（robustness）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），於第四款定明之，以防範人工智慧有關不實資訊、安全威脅與攻擊。  六、人工智慧所生成之決策對於利害關係人有重大影響，需保障決策過程之公正性。人工智慧研發與應用階段，應致力權衡決策生成之準確性，並提升可讓使用者及受影響者理解其影響及決策過程之可解釋性，兼顧使用者及受影響者權益。爰參考歐盟二○一九年可信賴AI倫理準則（Ethics Guidelines for Trustworthy AI）於第五款定明透明與可解釋性（Transparency and Explainability）之原則。另考量到進行資訊揭露與標記，在科技上恐有其侷限，爰為「應在技術上可行的情形下」之條文規範。  七、人工智慧研發與應用需公平、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），於第六款定明公平性原則（Fairness），強調應重視社會多元包容，避免產生偏差與歧視等風險。惟不論開發中或已運行之人工智慧系統，難免有些許出差錯之可能，故為「對特定群體造成偏見之結果應予以最小化」之規範。  八、基於安全與人民信賴等考量，人工智慧之研發及利用，應符合國家既有之標準或相關法規。如未有相關標準者，則應認定得採行之其他國家標準或國際標準。爰於第七款規定應合於標準之原則。  九、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生命週期中，應確保不同角色（如開發者、部署者、最終使用者等）能承擔相應之責任。爰於第八款訂定可問責性原則（Accountability）。 |
| 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，擬定發展計畫，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，其整體資源規劃，與相關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，定明政府機關應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，鼓勵其會員國政府建立人工智慧實驗沙盒制度（Regulatory Sandbox），提供一個受控環境，以促進人工智慧之創新，使其於投放市場或投入使用之前，可於有限時間開發、測試和驗證。爰定明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，進一步使國民受益於人工智慧創新科技。 |
| 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、設施與應用之國際交流與利用，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，故於第一項定明政府各機關除應就其業務權責推動、辦理外，亦宜與民間合作推動人工智慧發展。  二、參考科學技術基本法第二十一條，定明政府各機關應積極發展人工智慧國際合作、接軌國際，並參與國際共同開發與研究、技術與應用之交流，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，政府應持續推動各級學校、產業、團體、社會及公務機關（構）之人工智慧與其倫理教育，以提升國民人工智慧之素養。 | 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，定明政府應推動各級學校、產業、團體、社會及公務機關（構）之人工智慧與其倫理教育，以提升國民人工智慧之素養。 |
| 第八條　政府應避免人工智慧之應用，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、廣告不實、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、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）於第一項定明政府應避免人工智慧之應用造成國民生命安全或生態環境損害，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得提供或建議國內外具可行性且明確之評估驗證工具或方法，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，確保人工智慧安全與穩定運行。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，爰於第一項定明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，例如美國NIST AI風險管理框架所訂定之風險分類或歐盟人工智慧法訂定四級風險等。  二、各目的事業主管機關因所涉領域不同，得循前項風險分類框架訂定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，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。 | 一、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，以提升人工智慧決策之可驗證性及人為可控性。  二、為完善因應風險之措施，政府本身應建立人工智慧濫用與危害之即時偵測、緊急應變與緊急處分之能力，以即時防止人工智慧之濫用或危害對社會產生的損害擴大。 |
| 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，透過如美國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。爰於第一項要求各機關應建立應用負責機制，包含外國人工智慧產品落地規範，以降低人民法遵成本。  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，人工智慧投入市場前的任何研究、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。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，以利技術創新發展。 |
| 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。爰參考美國總統二○二三年發布之人工智慧行政命令定之，為第一項規定。  二、為避免人工智慧造成之失業情事，爰於第二項定明政府應向非自願失業者提供輔導就業措施。 |
| 第十三條　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。 | 參考韓國智慧資訊化基本法（Framework Action Intelligent Informatization），立法上強調人工智慧與數據資料的連結，重視數位基礎建設避免人工智慧時代的資訊落差，保障高齡者、身心障礙者等需要協助族群的權益等，避免因智慧資訊化造成負面影響。 |
| 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。 | 為避免個人資料外洩風險以及蒐集過多不必要之敏感資訊，爰參考美國二○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，由我國個人資料保護法主管機關協助各目的事業主管機關，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（data protection by design and by default），例如數位發展部發布之隱私強化技術應用指引等。 |
| 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、資料為人工智慧發展之重要元素，政府有必要確保人工智慧之創新與產業發展得以取得高品質的資料。參考歐盟人工智慧法有關支援高品質資料近用之規定，以及美國總統二○二三年發布之人工智慧行政命令要求聯邦資料長委員會研擬資料開放相關指引等規定。爰於第一項定明政府需就相關規範定期檢視並為必要調整，俾利人工智慧發展所需。  二、為確保人工智慧訓練及產出結果維繫國家文化價值，避免影響弱勢、多元族群權益及人民之智慧財產權，於第二項定明各機關應致力推動之事項，以完善我國資料治理機制。 |
| 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。 | 一、考量政府各機關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，且應參酌第九條風險分類規範進行風險評估與規劃因應措施。爰參考英國二○二四年「生成式人工智慧治理框架」，要求政府機關（構）執行公務應進行風險評估及風險因應措施。  二、為促使各機關依一致之認知及原則使用人工智慧，於第二項定明機關（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，並由行政院統籌協調，盤點政府單位的人工智慧應用情形。 |
| 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、為落實本法，確保人工智慧技術之有效推動發展，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，於第一項定明檢討職掌、業務、法規或訂定指引，以利行政院統籌各部會檢討現行法規與相關機制措施。  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，參考海洋基本法第十六條、韓國國家資訊化架構法第十七條、澳洲二○二三年安全且負責任之AI政策討論書（Safe and Responsible AI in Australia Discussion Paper），定明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。爰於第二項定明由中央科技主管機關協同中央目的事業主管機關，依本法規定解釋、適用之。 |
| 第十八條　本法施行日期，由行政院定之。 | 本法施行日。 |