　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110139890000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11013989 | 號 |  |  |

案由：本院委員林思銘、廖偉翔等17人，鑒於人工智慧（AI）之發展與應用，將成為未來推動產業升級與經濟成長的關鍵科技技術，亦將深遠影響未來人類的生活模式。故為促進經濟與社會生活環境的轉變，並保障數位人權與相關應用規範，應如其它先進國家，訂立人工智慧發展與相關應用之法制規範，以確保人工智慧技術之發展，與未來民眾之生活權益，能同步往智慧邁進，爰擬具「人工智慧基本法草案」，以完善相關機制。是否有當？敬請公決。

提案人：林思銘　　廖偉翔

連署人：鄭天財Sra Kacaw　　　賴士葆　　林倩綺　　李彥秀　　羅智強　　顏寬恒　　謝龍介　　邱鎮軍　　牛煦庭　　翁曉玲　　黃珊珊　　陳超明　　羅廷瑋　　馬文君　　林沛祥

|  |  |
| --- | --- |
| 人工智慧基本法草案 | |
| 條文 | 說明 |
| 第一條　為促進人工智慧產業發展及應用，並建立使用人工智慧之安全性與合規性，進而增進國人生活品質與社會創新，提升國家整體競爭力，特制定本法。本法未規定者，適用其他法律之規定。 | 一、本法之立法目的。  二、人工智慧之研發與應用，為未來國家發展之科技趨勢，亦為國際趨勢所向，對於未來人類之生活影響，有著舉足輕重之地位。故應訂定相關法制規範，建立使用人工智慧之安全性與合規性，進而增進國人生活品質與社會創新，提升國家整體競爭力。 |
| 第二條　本法所稱主管機關，在中央為國家科學及技術委員會；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、訂定本法之主管機關。  二、人工智慧應定位為國家科技發展，因其未來將影響之層面，不僅包含民眾生活環境亦包含國家經濟、國防防護以及國際競爭，而國科會是我國科技發展最高主管機關，並負責國家整體科技政策規劃與產學資源分配。爰於第一項明定本法之主管機關為國家科學及技術委員會。 |
| 第三條　本法所稱之人工智慧，係指基於具有自主運作能力之機器系統與技術，經由機器或人類之輸入與互動，達成針對人類所給定的目標，分析產生可能影響真實或虛擬環境的內容、預測、建議或決策。其運作方法包含機器學習與邏輯統計，運作系統環境包含軟體、硬體、資料系統、開發工具、應用工具及系統程式等。 | 參考美國「安全、可靠、可信賴的人工智慧開發與使用行政命令」（Executive Order on Safe,Secure, and Trustworthy Artificial Intelligence），以及歐盟人工智慧法對於人工智慧系統之定義，說明人工智慧為基於具有自主運作能力之機器系統與技術，經由機器或人類之輸入與互動，達成針對人類所給定的目標，分析產生可能影響真實或虛擬環境的內容、預測、建議或決策。其運作方法包含機器學習與邏輯統計，運作系統環境包含軟體、硬體、資料系統、開發工具、應用工具及系統程式等。 |
| 第四條　政府應積極落實推動下列人工智慧發展之工作政策：  一、促進人工智慧之研發創新。  二、規劃人工智慧之各級教育。  三、獎助人工智慧之專業人才。  四、推動人工智慧之產業發展。  五、輔助人工智慧之產學合作。  六、建置人工智慧之應用環境。  七、參與人工智慧之跨國合作。  八、引進人工智慧之國際資源。  九、其他人工智慧發展之政策。 | 因應人工智慧產業發展趨勢，政府應積極從各方面，落實各項不同之工作政策，加速推動人工智慧及產業發展，培育相關人才與推動完善之產業環境，並建置人工智慧應用之環境並與國際合作，建立我國在全球人工智慧舉足輕重之地位。 |
| 第五條　政府推動人工智慧之研發與應用，應在兼顧民眾安全、社會公益與數位平權之前提下，發展良善治理與基礎建設，並遵循下列原則：  一、永續發展與福祉：應兼顧社會公平及環境永續。提供適當之教育及培訓，降低可能之數位落差，使國人適應人工智慧帶來之變革。  二、人類自主：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；同時促進非敏感資料之開放及再利用。  四、資安與安全：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：人工智慧之產出應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、公平與不歧視：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應用與結果。  七、可問責：人工智慧之開發目的與應用，，不應違反其他相關法規，而進行欺詐或傷害使用者之財產與生命。應確保承擔相應之法律責任，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本原則，以作為政府各機關就其權責推動人工智慧之研發與應用之基礎。  二、人工智慧利益相關者應積極參與可信任人工智慧之負責任管理，以追求對人類和地球有益之結果，從而促進永續發展與福祉（Sustainable Development and Well-being），爰參考G7廣島AI國際行動規範（Hiroshima Process Code of Governance Framework for Generative AI），於第四款定明資安與安全Conduct for Organizations Developing Advanced AI Systems），於第一款定明之。  三、人工智慧參與者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（Human Autonomy），並尊重人類基本權利、人格權（含姓名、肖像、聲音）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訊隱私，是目前人工智慧發展最多討論與疑慮之議題。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注意隱私與資料治理（Privacy and Data Governance）。  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（Security and Safety），以防範AI有關安全威脅與攻擊。  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與可解釋性，兼顧使用者及受影響者權益。爰參考歐盟二○一九年可信賴人工智慧倫理準則（Ethics Guidelines for Trustworthy AI）於第五款定明透明與可解釋（Transparency and Explainability）之原則。  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），於第六款定明公平與不歧視原則（Fairness and Non-discrimination），強調應重視社會多元包容，避免產生偏差與歧視等風險。  八、研發或利用人工智慧之組織或個人應致力於建立人工智慧系統、軟體、演算法等技術之應用負責機制，以維護社會公益與關係人利益。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）於第七款訂定問責原則（Accountability）。 |
| 第六條　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，與發展人工智慧時所需之能源供應，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，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，定明政府機關應推動人工智慧發展等運用之方式，並確保所需之電力等能源之供應。 |
| 第七條　政府應致力完善人工智慧研發與應用之法規調適，相關法規之解釋與適用，在符合第五條基本原則之前提下，以不妨礙新技術與服務之提供為原則。 | 為促成人工智慧技術必要發展與普及，爰參考通訊傳播基本法第六條、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），定明政府各機關應致力完善人工智慧發展與轉型相關法規之解釋及適用，以有利於該等技術或服務之提供，避免影響技術之發展。 |
| 第八條　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，建立或完備既有人工智慧研發與應用服務之創新實驗環境。 | 參酌歐盟人工智慧法，鼓勵其會員國政府建立人工智慧實驗沙盒制度，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前，有時間開發、測試和驗證。爰定明各目的事業主管機關應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。 |
| 第九條　為加強國人對人工智慧知識、應用之關心與認識，政府應持續推動各級學校、產業、社會及公務機關（構）之人工智慧教育，以提升國人開發與使用人工智慧之素養。 | 為落實2023年行政院科技顧問會議結論全面推動人工智慧素養教育，且人工智慧應用為未來趨勢，應讓我國人民有基礎人工智慧應用之素養，爰參酌「科技基本法」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。 |
| 第十條　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。  主管機關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、為避免人工智慧技術發展及應用時，造成我國人民權益受損，或影響社會秩序、生態環境之損害等違反法規之情事，爰參酌美國總統2023年發布之人工智慧行政命令明定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、俾利各該主管機關辦理前項業務，主管機關及其他機關應提供或建議國內外評估驗證之工具或方法。 |
| 第十一條　主管機關應參考國際標準或規範發展之人工智慧資訊安全保護、風險分級與管理，推動與國際介接之人工智慧風險分級框架。  各目的事業主管機關得循前項風險分級框架，訂定其主管業務之風險分級規範。 | 一、為使人工智慧風險分級規範與配套驗證確保機制與國際接軌，應由主管機關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訂定四級風險，包含被禁止之人工智慧行為等。  二、各目的事業主管機關因所涉領域不同，得循前項風險分級框架訂定風險分級及相關管理規範。 |
| 第十二條　政府應識別、評估及降低人工智慧之使用風險，透過標準、規範或指引，於促進人工智慧研發與應用之同時，根據風險分級，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。 | 為讓各機關落實分級評估及管理，透過標準、規範或指引等方式，協助各界採取因應風險之措施，爰參酌美國2023年發展與使用安全且可信任的AI行政命令，要求政府各機關應提出相關規範或指引，以提升人工智慧決策之可驗證性及可控性。 |
| 第十三條　政府應依人工智慧風險分級，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，除應遵守第五條之基本原則外，不適用前項應用責任相關規範，以利技術創新發展。 | 一、人工智慧應用同時，應有完整且明確方式降低風險，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、AI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。各機關亦應訂定完整人工智慧應用之責任、救濟、補償、資訊揭露及問責機制等相關規範，以降低人民法遵成本。  二、另參酌歐盟人工智慧法第二條第八項規定，為避免人工智慧之研究及研發過程中遭受阻礙，除應遵守第五條之基本原則外，不適用應用責任相關規範，以利技術創新發展。 |
| 第十四條　政府為因應人工智慧發展，應避免技能落差，並確保勞動者之安全衛生、勞資關係、職場友善環境及相關勞動權益，及輔助產業於引進人工智慧時，所需之員工教育訓練。  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或技能訓練。 | 一、為避免勞動者執行相關業務時，因缺乏人工智慧相關技能，或被人工智慧取代，使其權益受損，爰明定政府應保障勞動者之勞動權益，並維護職場友善環境與健全之勞資關係，及輔助產業於引進人工智慧時，所需之員工教育訓練。  二、避免人工智慧之應用造成之失業情事，爰明定政府應提供輔導就業措施或技能訓練。 |
| 第十五條　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，避免違法進行個人資料蒐集、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）及二○二三年發展與使用安全且可信任的AI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。 |
| 第十六條　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，確保訓練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和可追溯的資料。爰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AI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，以利人工智慧發展所需。  二、為確保AI訓練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。 |
| 第十七條　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，以符第五條基本原則。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。 | 鑒於人工智慧有助於行政業務效率提升，然政府執行業務中，亦多有具機密性之內容，故政府機關（構）於使用人工智慧時，應進行風險評估，故應促使各機關依一致之認知及原則，訂定使用規範或內控管理機制。 |
| 第十八條　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，由中央目的事業主管機關協同其它中央科技主管機關，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，於第一項定明檢討法規，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，爰於第二項定明由中央目的事業主管機關其它中央科技主管機關，依本法規定解釋、適用之。 |
| 第十九條　本法自公布之日起施行。 | 明定法案的施行日期。 |