　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110105660000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11010566 | 號 |  |  |

案由：本院委員萬美玲、林沛祥、廖偉翔等18人，鑒於近年來人工智慧發展快速，且其影響層面廣泛，能應用於各領域上，亦被國際視為未來趨勢，且經濟合作暨發展組織（以下簡稱OECD）於2019年通過「人工智慧建議書」，提出基本價值原則，給予各國相關建議；歐盟同年發布「可信賴人工智慧倫理準則」，且於2024年通過「人工智慧法」；美國則於2022年發布「AI權利法案藍圖」、加拿大亦於2022年提出「人工智慧資料法草案」，然我國迄今卻未有相關法規，恐讓我國人工智慧發展落後他國，且無相關法規亦將讓人工智慧發展受到限制，政府應積極推動相關法規，以協助、推動我國人工智慧發展，並規範人工智慧應遵守之基本原則，避免於人工智慧發展過程中，使國民權益受損，爰擬具「人工智慧基本法草案」。是否有當？敬請公決。

提案人：萬美玲　　林沛祥　　廖偉翔

連署人：張嘉郡　　鄭天財Sra Kacaw　　　牛煦庭　　黃　仁　　羅明才　　邱鎮軍　　翁曉玲　　呂玉玲　　洪孟楷　　林國成　　游　顥　　黃建賓　　柯志恩　　廖先翔　　陳菁徽

人工智慧基本法草案總說明

鑒於近年來人工智慧發展快速，且其影響層面廣泛，能應用於各領域上，亦被國際視為未來趨勢，且經濟合作暨發展組織（以下簡稱OECD）於2019年通過「人工智慧建議書」，提出基本價值原則，給予各國相關建議；歐盟同年發布「可信賴人工智慧倫理準則」，且於2024年通過「人工智慧法」；美國則於2022年發布「AI權利法案藍圖」、加拿大亦於2022年提出「人工智慧資料法草案」，然我國迄今卻未有相關法規，恐讓我國人工智慧發展落後他國，且無相關法規亦將讓人工智慧發展受到限制，政府應積極推動相關法規，以協助、推動我國人工智慧發展，並規範人工智慧應遵守之基本原則，避免於人工智慧發展過程中，使國民權益受損，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、訂定本法主管機關。（草案第二條）

三、人工智慧定義。（草案第三條）

四、人工智慧研究發展及應用之基本原則。（草案第四條）

五、政府應推動人工智慧研究發展與應用。（草案第五條）

六、政府應完善法規調適。（草案第六條）

七、政府應建立或完備人工智慧創新實驗環境。（草案第七條）

八、政府應推動人工智慧公私協力與國際合作。（草案第八條）

九、政府應推動人工智慧人才培育與素養教育。（草案第九條）

十、政府應評估驗證人工智慧防止違法應用。（草案第十條）

十一、政府應推動人工智慧風險分級規範。（草案第十一條）

十二、政府應強化人工智慧人為可控性。（草案第十二條）

十三、政府應建立人工智慧應用負責機制。（草案第十三條）

十四、政府應保障勞工權益。（草案第十四條）

十五、政府應保障個資隱私。（草案第十五條）

十六、政府應提升資料利用性與國家文化價值。（草案第十六條）

十七、政府公務使用人工智慧之原則。（草案第十七條）

十八、政府應檢討主管法規。（草案第十八條）

十九、本法施行日。（草案第十九條）

|  |  |
| --- | --- |
| 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，維護國民生命、身體、健康、安全及權利，提升國民生活福祉、維護國家文化價值及國家競爭力，增進社會國家之永續發展，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，亦為國際主要發展趨勢，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，促進技術應用與產業發展，同時維護人民安全、國家安全及保障人民權利，邁向社會永續發展，以期回應社會及人文需求，並儘速達到智慧國家之目標，且人工智慧為新興領域，涉及面相極廣，實有修法之必要。  三、此外，發展與應用人工智慧之同時，應制定具有指標與引導性原則之立法，作為發展人工智慧之規範與促進應用之法源基礎。 |
| 第二條　本法所稱之主管機關，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，由各目的事業主管機關辦理。 | 一、界定本法之主管機關。  二、查，國科會為我國科技發展最高主管機關，並負責國家科技政策規劃與資源分配。且國科會與產官學研界連結緊密，對各界相當熟捻，亦能因應當前狀況，即時修正科技政策。  三、此外，本法為國科會擬定，若主管機關由其他部會主管，恐產生管轄重疊、協調困難、科技資源分配不均等問題，導致人工智慧發展進度緩慢，為確保人工智慧技術發展及其法規規範與產業應用三者並進，爰於本條文規定主管機關為國科會。 |
| 第三條　本法所稱人工智慧，係指以機器為基礎之系統，該系統具自主運行能力，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，美國法典第九四○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）42001：2023人工智慧管理系統、美國國家標準暨技術研究院AI風險管理框架，以及歐盟人工智慧法對於人工智慧系統之定義，說明人工智慧必須被設計為具備一定程度之自主運行能力，透過資料訓練，實現預測、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。 |
| 第四條　政府推動人工智慧之研發與應用，應在兼顧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，使國民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、智慧財產權之保護：人工智慧之發展及應用，應遵守智慧財產權相關條文，使其不受侵害。  五、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。  六、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。  七、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結果。  八、問責：應確保承擔相應之責任，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考量創新發展與可能風險，並參酌各國相關政策方針、法規，訂定具指標與引導功能之基本原則，做為各部會推動之基準。  二、人工智慧利益相關者應以追求對人類和地球有益結果，促進永續發展與福祉，爰參考G7廣島AI國際行動規範，於第一款明定。  三、參酌經濟合作暨發展組織（OECD）2019年公布之人工智慧建議書，於第二款明定人工智慧應支持人類自主，並尊重人權、人格權（含姓名、肖像、聲音）與文化價值等，以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，亦於義大利曾發生OpenAI在未具適當法律依據時，將用戶個資用來訓練ChatGTP之情事，未避免我國發展人工智慧技術時侵害個人資料。爰參考美國2022年AI權利法案藍圖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。  五、鑒於經濟部智慧財產局於2022、2023年陸續闡明對生成式AI模型（如生成文字之ChatGPT、生成圖像之Midjourney及生成影片之Pictory）的開發者蒐集提供大量資料給AI模型訓練學習的行為，涉及「重製」原始著作之行為，亦於2023年6月16日經授智字第11252800520號函，針對AI侵害著作權部分提出見解，指出除有著作權法第四十四條至第六十五條合理使用之情形外，應取得著作財產權人之同意或授權，始得為之。智慧財產局亦表示，生成式AI模型以演算法利用網路上之該等著作進行學習不屬於著作權法第四十四條至第六十三條規定之適用情形，需參酌著作權法第六十五條第二項所定的合理使用四個判斷因素依個案綜合判斷，且美國近期已有多起著作權人對AI工具開發商提起的侵權訴訟，為避免人工智慧之發展侵害他人智慧財產權，爰訂定第四款。  六、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2022年AI權利法案藍圖及新加坡2023年生成式AI治理架構草案，且為避免於人工智慧發展過程中出現資安漏洞或被攻擊，導致他人權益受損，於第四款定明資安與安全，以防範人工智慧有關安全威脅與攻擊。  七、人工智慧所生成之決策對於利害關係人有重大影響，除須保障決策之公正性，致力權衡決策生成之準確性與可解釋性外，亦應使受人工智慧決策影響之民眾，充分了解其結果，以兼顧使用者及受影響者權益。爰參考歐盟2019年可信賴人工智慧倫理準則於第五款明定透明與可解釋之原則。  八、人工智慧研發與應用之過程中，應重視社會多元及包容，避免其演算過程，產生偏差或歧視之結果，爰參考美國2022年AI權利法案藍圖，於第六款明定公平與不歧視原則，強調AI研發與應用過程中，應重視社會多元包容，避免產生偏差與歧視等風險。  九、研發或利用人工智慧之組織或個人，應建立相對應技術應用之完善問責機制，用以維護社會公益及人民權益。爰參考新加坡2023年生成式AI治理架構草案於第七款訂定問責原則。 |
| 第五條　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所涉領域甚廣，政府各機關應依其業務職掌推動相關人工智慧技術及配套法規，以加速人工智慧技術發展及應用，爰參酌「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運用及相關配套措施。 |
| 第六條　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，在符合第三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。 | 鑒於人工智慧愈發普及，然我國於人工智慧相關法規尚未完善，恐造成法規漏洞，使人民權益受損，且法規之不完善，亦將造成人工智慧之發展與應用進程緩慢，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2023年安全且負責任之AI政策討論書，明定政府各機關應完善人工智慧發展與轉型相關法規之解釋及適用，俾利於AI技術發展及應用，避免影響技術發展。 |
| 第七條　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。 |
| 第八條　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、鑒於人工智慧應用及發展涉及範圍廣泛，政府應與民間合作，提升我國人工智慧相關產業之發展進程，為避免政府自行研發，未能與民間接軌，爰明定第一項，要求政府應以公私協力方式，推動人工智慧創新應用。  二、政府於發展人工智慧技術時，應積極與國際交流相關技術、人才與設施，爰參酌「科技基本法」第二十一條，明定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。 |
| 第九條　為加強國民對人工智慧知識之關心與認識，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，以提升國民人工智慧之素養。 | 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。  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、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AI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，數位發展部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　數位發展部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，應由數位發展部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AI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、人工智慧應用同時，應有完整且明確方式降低風險，各機關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，避免國民權益受損。  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，除應遵守第三條之基本原則外，不適用應用責任相關規範。 |
| 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。  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、為避免勞動者執行相關業務時，因缺乏人工智慧相關技能，使其權益受損，爰增訂第一項，明定政府應保障勞動者之勞動權益，並維護職場友善環境。  二、另為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。 |
| 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。 | 為避免於人工智慧研究、研發及應用過程中，過度蒐集或利用不必要之個人資料，爰參酌美國2022年AI權利法案藍圖及2023年發展與使用安全且可信任的AI行政命令，由個人資料保護法主管機關協助各目的事業主管機關，配合相關法規建立個資保護相關措施或機制，例如數發部發布之隱私強化技術應用指引等。 |
| 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、資料為發展人工智慧不可或缺的元素之一，為確保人工智慧之發展可取得相關資料，爰於第一項明定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、另為確保人工智慧訓練結果符合國家多元文化價值及智慧財產權，爰於第二項明定各機關應致力提升人工智慧使用資料之品質與數量。 |
| 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，以符第三條基本原則。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效率之提升，然政府執行業務機密度高，政府應進行風險評估，訂定使用規範或內控管理機制，避免各機關應用人工智慧提升行政效率時，產生相關爭議。 |
| 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，確保人工智慧技術得到有效推動發展，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，於第一項訂定檢討法規機制，俾利行政院統籌各部會檢討現行法規，以符合本法目的。  二、為免本法及相關法規於訂定或修訂前，未有規定者，得由中央目的主管機關協同本法主管機關，依本法解釋、適用之。 |
| 第十九條　本法施行日期，由行政院定之。 | 本法施行日。 |