　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110105800000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11010580 | 號 |  |  |

案由：本院委員許宇甄、鄭正鈐、萬美玲等20人，鑑於人工智慧（Artificial Intelligence, AI）技術迅速發展，深刻改變產業結構、社會運作與國家治理模式，為建構具前瞻性之法制架構，推動人工智慧之創新應用，並兼顧人民基本權利、社會倫理、數位平權與國家競爭力之提升，爰擬具「人工智慧基本法草案」。是否有當？敬請公決。

提案人：許宇甄　　鄭正鈐　　萬美玲

連署人：徐欣瑩　　林沛祥　　林德福　　黃健豪　　黃建賓　　張智倫　　翁曉玲　　邱鎮軍　　陳超明　　丁學忠　　高金素梅　呂玉玲　　盧縣一　　游　顥　　謝龍介　　鄭天財Sra Kacaw　　　廖先翔

人工智慧基本法草案總說明

有鑑於人工智慧為現代科技發展之關鍵領域，已成為驅動未來社會、經濟、教育、文化、國安等全面轉型之基礎引擎。為因應人工智慧技術快速演進與跨領域應用擴張，亟需建立具整體性、原則性與彈性調適機制之基本法，統合我國人工智慧政策，指引公共治理方向，並促進科技創新與社會共融。

本草案參酌歐盟《人工智慧法案》（AI Act）、美國《AI行政命令》及經濟合作暨發展組織（OECD）、美國國家標準與技術研究院（NIST）等國際規範與實務經驗，綜整台灣科技、產業、教育及社會現況，制定具體法源，以回應人工智慧對社會帶來之潛在風險與發展契機。

草案內容涵蓋人工智慧之定義、發展原則、政策機關、跨域協調、公私協力、風險監理、法規調適、資料治理、產業支持、數位平權及勞動權益保障等，為我國未來智慧治理與科技戰略奠定法制基礎，提升我國於全球人工智慧發展之治理能量與競爭地位。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、本法之主管機關。（草案第二條）

三、人工智慧之定義。（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、數位平權之精神。（草案第五條）

六、國家應避免人工智慧之應用有侵害基本人權或違法之情事。（草案第六條）

七、國家人工智慧戰略特別委員會之設立與組成。（草案第七條）

八、國家應積極推動政府機關之人工智慧布建及應用。（草案第八條）

九、政府應提升國民對於人工智慧之知識與技能。（草案第九條）

十、人工智慧之跨域及國際合作。（草案第十條）

十一、國家對於發展人工智慧之預算確保。（草案第十一條）

十二、國家為推動人工智慧之研發、應用及基礎建設，應給予財政優惠措施。（草案第十二條）

十三、人工智慧研發、訓練及應用之法規調適。（草案第十三條）

十四、人工智慧創新應用之公私協力。（草案第十四條）

十五、資料開放、共享及再利用機制。（草案第十五條）

十六、個人資料之保護措施。（草案第十六條）

十七、國家應積極運用人工智慧確保勞動權益。（草案第十七條）

十八、主管機關應協調其他相關機關參考國外標準或規範，推動風險分級框架。（草案第十八條）

十九、各級政府之法規完備。（草案第十九條）

二十、本法施行日期。（草案第二十條）

|  |  |
| --- | --- |
| 人工智慧基本法草案 | |
| 條文 | 說明 |
| 第一條　為建設智慧國家，促進人工智慧研發與人工智慧產業發展，建構人工智慧安全應用環境，落實數位平權，確保技術應用符合社會倫理，保障人民基本權利，增進社會福祉，維護國家文化價值及提升國際競爭力，特制定本法。 | 一、本法之立法目的。  二、為積極研發與應用人工智慧，達成以人為本、落實數位平權並保障人民基本權利並提升國家競爭力之目標，因此制定具有指標性及原則性之法律，以作為人工智慧研發與應用之法源基礎。 |
| 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執掌者，由各目的事業主管機關辦理。 | 一、本法之主管機關。  二、世界各國常以掌管科學研究的政府部門作為人工智慧政策之主管機關，如美國以國家科學技術委員會（NSTC）主導國家人工智慧研究發展戰略計畫；澳洲以工業科學資源部（Department of Industry, Science, Energy and Resources）制定公共部門AI使用指引與治理架構，為使人工智慧於研發階段蓬勃發展，與我國科學研究無縫接軌，爰將人工智慧之主管機關訂為國家科學及技術委員會。  三、考量人工智慧政策涉及各政府部會之業務職掌，故明定本法所定事項，涉及各目的事業主管機關執掌者，由各目的事業主管機關辦理。 |
| 第三條　本法所稱人工智慧，係指具備自主運行能力，並能透過數據分析、機器學習或演算法決策，以影響實體或虛擬環境之系統。 | 一、參考歐盟《人工智慧法案》（Artificial Intelligence Act）第一章第三節、經濟合作暨發展組織（OECD）2019年二月由數位經濟政策委員會（CDEP）所提出之《人工智慧建議》（Recommendation of the Council on Artificial Intelligence），以及美國國家標準與技術研究院（NIST）於2023年公布之《人工智慧風險管理架構》（AI RMF），明定人工智慧之定義。  二、突顯人工智慧具備「自主性」與「影響力」兩大核心特徵，並涵蓋目前主流技術路徑如機器學習、深度學習及演算法預測等。  三、本條所述之「自主運行能力」並不等同完全自律，而是指系統在不需持續人為介入下，能根據接收到的資訊進行特定程度之分析與行動；「影響實體或虛擬環境」則涵蓋AI對人類決策、社會互動、資訊生成等層面的實際影響。  四、本條定義採「技術中立原則」，不限於特定應用領域，亦未拘泥於特定開發技術，目的在於提供未來技術演進下具有彈性且普遍適用之基礎法源。 |
| 第四條　國家推動人工智慧之研發與應用，應在以人為本、數位平權、永續發展及值得信賴之前提下，並遵行下列基本原則：  一、自主原則：尊重人性尊嚴及個人自主。  二、保密原則：尊重人民隱私及營業秘密。  三、安全原則：保障人民生命、身體、自由及財產之安全。  四、包容原則：重視多元包容，確保公平，避免歧視。  五、透明原則：強化可解釋性及可追溯性，確保問責可能性。  六、永續發展原則：促進人工智慧之發展與應用兼顧環境、生態及世代正義。 | 人工智慧之研發與應用應以人為本，以達成數位平權為目標，並落實永續發展理念，確保技術進步不以犧牲環境與世代正義為代價。爰此，國家應依據自主性、保密性、安全性、包容性、透明性及永續性等基本原則推動人工智慧發展，使人工智慧系統具備可信賴性，並兼顧人權保障、社會正義與長期公共利益。 |
| 第五條　人民無分性別、年齡、能力、地域、族群、宗教信仰、政治理念、社經地位及其他條件，接觸人工智慧之機會一律平等。對於原住民、身心障礙者及其他弱勢族群，應考慮其自主性及特殊性，依法令予以特別保障，並扶助其發展。 | 參考教育基本法第四條，揭示本法保障數位平權之精神，人民無分性別、年齡、能力、地域、族群、宗教信仰、政治理念、社經地位及其他條件，接觸人工智慧之機會一律平等。對於原住民、身心障礙者及其他弱勢族群，政府應給予特別保障。 |
| 第六條　國家應推動人工智慧技術於公共服務之應用，確保應用過程符合社會公平性與可問責性；並應避免人工智慧之應用，有侵害人民生命、身體、自由或財產，破壞社會秩序或生態環境，或偏差、歧視、廣告不實、資訊誤導或造假等違反相關法規之情事。  主管機關應協調其他相關機關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、參考美國總統於二○二三年發布之《安全、可信與負責任的人工智慧行政命令》（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence），明定政府在推動人工智慧技術於公共服務領域應用時，應同時確保其符合社會公平性與可問責性，避免人工智慧應用侵害人民基本權利，或對社會秩序、生態環境造成破壞，亦不得出現偏差、歧視、廣告不實、資訊誤導或造假等違反相關法規之情事。  二、為利各目的事業主管機關執行相關監督與管理業務，主管機關應協調數位發展部及其他相關機關，提供或建議合適之國內外評估工具與驗證方法，作為各目的事業主管機關實施風險評估與法遵檢核之參據，確保人工智慧系統於公共領域之導入具備信賴性與合法性。 |
| 第七條　行政院應成立國家人工智慧戰略特別委員會，由行政院院長召集學者專家、人工智慧相關民間團體及產業代表、政務委員、相關機關首長或代表、直轄市及縣（市）政府首長組成，協調、推動及督導全國人工智慧事務，並訂定國家人工智慧發展綱領。  前項委員會每年至少召開會議一次，並審議國家人工智慧發展綱領；遇突發緊急或重大事件，應召開臨時會議。  第一項委員會之幕僚作業，由國家科學及技術委員會辦理。 | 一、考量人工智慧所涉及之層面範圍極廣，需要行政院針對跨部會議題進行規劃與協調，因此明定由行政院成立國家人工智慧戰略特別委員會，由行政院院長擔任召集人，召集學者專家、人工智慧相關民間團體及產業代表、政務委員、相關機關首長或代表、直轄市及縣（市）政府首長組成，協調、推動及督導全國人工智慧事務，並訂定國家人工智慧發展綱領。  二、明定國家人工智慧戰略特別委員會每年至少召開會議一次，並審議國家人工智慧發展綱領；遇突發緊急或重大事件，應召開臨時會議。  三、國家人工智慧戰略特別委員會之幕僚作業明定由國家科學及技術委員會辦理之。 |
| 第八條　為加速建構具有我國特色，並符合國家人工智慧戰略之人工智慧，以確保我國數位主權，有效提升政府效能，國家應積極推動政府機關（構）之人工智慧布建及應用。 | 為提升政府效能，加速構建我國主權人工智慧（Sovereign AI），國家應積極推動政府機關（構）之人工智慧布建及應用。 |
| 第九條　為提升國民對於人工智慧之知識與技能，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，並厚植國民之數位素養。 | 參考科學技術基本法第二十二條，明定政府應提升國民對於人工智慧之知識與技能，並厚植國民之數位素養。 |
| 第十條　國家應落實人工智慧發展政策並鼓勵產官學界，就下列事項，積極進行跨域合作及國際交流：  一、促進人工智慧研發創新。  二、重視人工智慧基本教育。  三、培育人工智慧專業人才。  四、推動人工智慧產業發展。  五、深化人工智慧產學合作。  六、鼓勵人工智慧發展投資。  七、建立資料中心、能源設備等有利於人工智慧發展之基礎設施。  八、其他人工智慧發展政策。 | 一、人工智慧發展政策在於促進人工智慧研發創新、重視人工智慧基本教育、培育人工智慧專業人才、推動人工智慧產業發展、深化人工智慧產學合作、鼓勵人工智慧發展投資。  二、政府應鼓勵有利於人工智慧發展之基礎設施，如建立資料中心、能源設備等。 |
| 第十一條　為利我國人工智慧蓬勃發展，各級主管機關皆應編列預算，並逐年由中央主管機關會商直轄市、縣（市）主管機關，檢討並調整運行策略，以確保經費符合人工智慧政策之所需。 | 為促進我國人工智慧蓬勃發展，且相關政策均得以落實，各級政府應編列預算，並依照運行策略調整預算編列，以確保我國之人工智慧政策具有充足且穩定的資源投入。 |
| 第十二條　國家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、投資、獎勵、輔導，或提供租稅、金融等財政優惠措施。 | 為確保人工智慧之研發、應用及基礎建設具有足夠之資源投入，爰參考產業創新條例第九條及科學技術基本法第六條，明定政府為推動人工智慧之發展，應給予財稅及金融等優惠措施。 |
| 第十三條　國家應於人工智慧開發、訓練、測試及驗證新興技術運作之影響時，提供合理使用、扶持及補助措施，並完善人工智慧研發及應用之法規。  前項合理使用、扶持之管理規則，由中央主管機關於符合本法第四條基本原則下定之。 | 人工智慧之研發，無法避免與傳統法令發生法規範衝突。舉凡訓練資料之合理利用、研發資金之補助、人工智慧產業之扶持、研發責任之歸責範圍等，於符合本法第四條基本原則之情況下，國家應積極予以扶持或保障，以利新興技術與服務之發展。 |
| 第十四條　國家應基於公私協力原則，積極與民間共同推動人工智慧之創新運用。  對於人工智慧發展所需之關鍵基礎設施，若政府機關於特定期間內無法提供所需設施容量，得由民間廠商依相關法令規定，自行籌建所需之基礎設施設備。 | 一、考量人工智慧應用與發展事務涵蓋範圍廣泛，並涉及大量計算、儲存與傳輸資源，故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，共同推動人工智慧創新與發展。  二、然生成式人工智慧、大規模預訓練模型等新興技術，其研發與部署對基礎設施（例如電力、資料中心、冷卻設施等）需求極高，若政府無法於短期內提供足額資源，為不妨礙產業發展動能，應允許民間廠商於符合法規條件下，得以自建所需設施（如專用電廠或能源供應系統），以確保台灣在全球人工智慧競爭中之技術自主與基礎韌性。 |
| 第十五條　國家應本於資料具有永久性、可加解密之再利用性，以及價值可追溯紀錄之特性，建立資料開放、共享及再利用機制，以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。  國家應致力提升我國人工智慧使用資料之品質與數量，確保訓練結果足以展現國家多元文化價值與維護智慧財產權。 | 一、考量資料具有永久性、可加解密之再利用性，以及價值可追溯紀錄之特性，均為人工智慧發展之重要元素，國家應建立資料開放、共享及再利用機制，以提升人工智慧使用資料之可利用性，並為將來建立合理分潤機制保留可行性。  二、為確保人工智慧之訓練成果，國家應致力提升資料之品質及數量，並確保人工智慧訓練結果能夠展現我國多元文化價值並維護智慧財產權。 |
| 第十六條　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，並促進個人資料保護納入預設及設計相關措施或機制，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（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence），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），如數位發展部發布之隱私強化技術應用指引等。 |
| 第十七條　國家應積極運用人工智慧確保勞動者之勞動權益。  政府應制定人工智慧發展影響下之勞動政策，確保受人工智慧自動化影響之勞工能獲得適當職能培訓與轉型機會，提升勞動參與，保障經濟安全，並落實尊嚴勞動。 | 一、參考歐盟《人工智慧法案》、美國勞工部相關政策建議以及OECD就AI與就業影響所發表之政策原則，明定國家應積極運用人工智慧技術，作為強化勞動權益保障之手段，促進科技與勞動市場之共融發展。  二、人工智慧及自動化技術可能導致部分職位被取代或工作型態改變，為降低科技發展對勞工權益之衝擊，政府應擬訂相應之勞動政策，並提供勞工職能轉型、培訓資源及社會支持機制，協助其適應產業結構轉型，實現人工智慧技術發展與就業安全之雙贏。 |
| 第十八條　主管機關應協調其他相關機關參考國際標準或規範，建立人工智慧風險評估機制，並依據風險等級實施適當監管：  一、低風險人工智慧：指對個人權益、社會秩序或公共安全影響程度極低，不涉及敏感資料處理或自動化決策之應用。得自由發展，無須特定監管。  二、中風險人工智慧：指涉及特定程度之個人資訊分析或判斷，對個人權益或產生社會影響具有潛在風險，但可透過技術或管理措施予以控制者。應提供可解釋性報告，並接受主管機關抽查。  三、高風險人工智慧：指涉及對人身安全、基本權利或重大公共利益產生重大影響之應用，若失誤將導致難以回復之損害者。應取得主管機關許可，並接受定期安全測試與合規審查。  四、禁止性人工智慧：指具高度侵害人權、自由或隱私風險，且其技術或制度設計本質即不符合法治國原則者。  主管機關應每年檢討風險分類標準，並公布最新規範。違反規範者，得處罰鍰，情節重大者得勒令停止應用。  前項規範之制定，由中央主管機關擬訂，報請行政院核定之。  各目的事業主管機關得循第一項風險分級框架，訂定其主管業務之風險分級規範。 | 一、參考歐盟《人工智慧法案》（Artificial Intelligence Act）所提出之風險導向監管架構（risk-based approach），並結合美國國家標準與技術研究院（NIST）於2023年發布之《人工智慧風險管理架構》（AI RMF）及經濟合作暨發展組織（OECD）人工智慧政策準則，明定主管機關應協調相關機關，參酌國際標準，建立明確之人工智慧風險評估與分級監管制度。  二、依人工智慧技術對社會、個人及國家安全可能產生之風險程度，將人工智慧應用分類為低風險、中風險、高風險及禁止性四類：低風險應用得自由發展；中風險應用應具備可解釋性與可稽核性；高風險應用須通過主管機關核准並定期測試；禁止性應用則因其涉及人權侵害或公共危害，應全面禁止。  三、主管機關每年應檢討風險分類標準並對外公布，以確保監管架構能與技術發展同步調整。此外，為確保制度落實與法規統一性，風險分級原則由中央主管機關研擬並報請行政院核定，各目的事業主管機關則得依此原則，針對其所屬領域之AI應用訂定適用規範，落實分級治理原則並兼顧部會間政策一致性。  四、明定違反分級監管規範者之法律責任，主管機關得視情節輕重處以罰鍰，並得命其停止技術應用，以防杜高風險人工智慧技術對社會造成實質危害。 |
| 第十九條　政府應於本法施行後，依本法規定檢討及調整所主管之執掌、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偕同中央主管機關，依本法規定解釋、適用之。 | 一、為落實本法，確保人工智慧之研發與應用能有效推展，於第一項明定檢討法規，以利行政院統籌各部會檢討法規與相關機制。  二、依第一項推定應訂定、修正或廢止之相關法規，於未完成法定程序前，為使相關事務符合本法之規定，爰於第二項明定由中央目的事業主管機關偕同中央主管機關，依本法規定解釋、適用之。 |
| 第二十條　本法自公布之日起施行。 | 明定本法施行日期。 |