　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110103200000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11010320 | 號 |  |  |

案由：本院委員林倩綺、徐欣瑩、林沛祥等23人，鑒於大數據、雲端運算、物聯網及5G等科技發展趨勢，人工智慧（AI）已成為驅動產業升級與經濟成長的關鍵技術，為促進經濟與社會結構轉型，並保障數位人權，應積極引導人工智慧（AI）產業發展並建立倫理與法律規範，目前我國尚缺乏完善的法規與應用指引，相關發展仍欠缺統一架構與風險控管機制，鑑於多數先進國家已陸續推動相關立法並搶占國際標準制定主導地位，我國亟需完善法制，以確保技術發展同時兼顧資料隱私、演算法透明、公平決策等基本權益，爰擬具「人工智慧基本法草案」，以完善機制。是否有當？敬請公決。

說明：

一、隨著寬頻網路與科技發展，國際工業4.0的發展趨勢，人工智慧商業化腳步已從實驗室的技術或原型走向市場，世界各國皆如火如荼推動國家級的AI發展策略。人工智慧技術的發展，已成為當代科技與產業轉型的核心驅動力。伴隨電腦運算能力提升、資料儲存成本下降與半導體技術的進步，人工智慧自千禧年後迅速進入第三波發展階段，廣泛應用於交通、醫療、製造、金融等領域，帶來前所未有的效率與便利。近年生成式人工智慧與自駕科技等新應用更進一步加速了其技術滲透與商業應用。放眼國際，歐盟、美國、英國、OECD等已紛紛提出人工智慧監管架構與倫理準則，並朝向專法立法邁進。私人企業如Google、微軟等亦自律建立AI原則，可見「法律與制度」已成全球應對新科技風險的主流共識。我國若遲未建構對應法制，不僅難以因應產業發展所需，更可能在國際數位規範競逐中失去主動權，影響AI商品與服務的跨境通行性，並受限於他國所塑造的法律框架，如「布魯塞爾效應」（Brussels effect）所帶來的間接制約。

二、將人工智慧技術的研發應用與競爭力水準迅速提升，乃是世界各科技大國重要的發展目標，為實現前揭目標，我國亟待將研究、開發與整合人工智慧之技術運用於產業之中，藉以發揮我國之智慧產業創新能力。在人工智慧發展的同時，需兼顧人類生活之倫理規範，比免失控的人工智慧侵害當代各種基本價值與人權，政府需建立人工智慧發展之倫理規範，引導產業發展出良善的人工智慧。

三、為使我國在未來快速變遷的數據時代中居於人工智慧的領先群，盡速研究、開發與整合人工智慧之技術資源，制訂人工智慧發展基本法將能迅速凝聚社會共識、確立人工智慧作為國家政策中的重要內涵，以及認識到實際推動產業發展與轉型時應有的進步空間。此基本法參酌美國、英國、日本AI先進國家的法政策經驗，並整合我國國情，主要包含：

(一)確定人工智慧之發展在國家政策中的定位，訂立發展綱領要求中央政府應在產業界和學術界優先推動人工智慧的研究、發展，並促進產業AI化、建立AI技術應用平台，以及形成AI產業生態系。

(二)緣人工智慧發展牽涉大規模公眾數據的使用以及實驗場域落地試驗，與公共利益牽連甚深，須制定適當的人工智慧的開發標準原則。政府在符合開發標準原則下，應盡量滿足產業、學術界在人工智慧研發與應用之需求；建立與凝聚公眾對人工智慧的認識與信任，樹立人工智慧發展的基本倫理原則。

四、以「人本導向」與「風險為基礎」為核心理念，透過分級管理機制、可問責制度、資訊揭露義務、倫理規範與創新鼓勵措施，兼顧科技發展與社會公共利益，建立一套符合我國社會價值與國際接軌的法制框架。

五、在上述內容考量下，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)本法之主管機關。（草案第二條）

(三)本法用詞。（草案第三條）

(四)人工智慧開發原則。（草案第四條）

(五)人工智慧發展之倫理。（草案第五條）

(六)補助、獎勵及輔導。（草案第六條）

(七)培訓體系。（草案第七條）

(八)個人資料相關法規調整及利用規範。（草案第八條）

(九)特別委員會。（草案第九條）

(十)特別審核機制。（草案第十條）

(十一)智慧化政府推動。（草案第十一條）

(十二)教育預算。（草案第十二條）

(十三)沙盒計畫。（草案第十三條）

(十四)反歧視。（草案第十四條）

(十五)決策糾正。（草案第十五條）

(十六)國際合作與交流。（草案第十六條）

(十七)公布之日起施行。（草案第十七條）

提案人：林倩綺　　徐欣瑩　　林沛祥

連署人：蘇清泉　　黃健豪　　張嘉郡　　陳玉珍　　黃　仁　　楊瓊瓔　　廖偉翔　　黃建賓　　翁曉玲　　羅明才　　鄭天財Sra Kacaw　　　陳超明　　盧縣一　　顏寬恒　　林德福　　丁學忠　　游　顥　　張智倫　　洪孟楷　　邱鎮軍

|  |  |
| --- | --- |
| 人工智慧基本法草案 | |
| 條文 | 說明 |
| 第一條　（本法之制定目的）  為建設智慧國家，促進人工智慧產業發展，建構人工智慧安全應用環境，保障人民基本權利，增進社會福祉，提升國際競爭力與影響力，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、我國近年來於人工智慧相關領域發展進步迅速，而人工智慧發展為一新興領域，涉及複雜之管理，亟需要完善之法制基礎，建構相關發展體制。考量歐盟、日本、美國等先進國家多訂立有相關專法，組設專責機構推動人工智慧發展，我國亦成立數位發展部，正式將人工智慧列入其數位產業署之職掌範圍，自應及早進行相關法制規範，爰制定本法。 |
| 第二條　(本法之主管機關)  本法所稱主管機關，在中央為數位發展部；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、考量人工智慧、巨量資料等新興數位領域之產業發展業務已正式納入數位發展部數位產業署之掌理事項，爰於第一項明定本法之主管機關為數位發展部。  二、本法所規範事項，包含國家發展基金之挹注、政府資料公開、個人資料運用、智慧財產保障、人工智慧產業發展、人工智慧之跨領域應用及法規制（訂）定、修正或廢止等不同中央目的事業主管職掌之業務，爰為第二項規定。 |
| 第三條　(本法用詞)  本法用詞，定義如下：  一、人工智慧：指以巨量資料、機器學習、演算法、雲端運算、物聯網及其他相關技術使電腦系統具有人類知識及行為，並具有學習、推理判斷以解決問題、記憶知識或了解人類自然語言之能力。  二、人工智慧產業：指包含政府、法人單位、學術機構及民間廠商對於人工智慧研究、人工智慧技術關鍵基礎設施之研發、設計、製造、修護、組裝及檢驗、人工智慧應用服務（含營運）及其衍生之新型態服務產業等領域。  三、巨量資料：指規模巨大，且無從直接或間接識別特定個人之數據資料，並可藉由資料蒐集、數據儲存、資訊萃取、統計分析達到決策建議，創造創新價值。  四、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、種族、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動、政治意見、宗教信仰及其他得以直接或間接方式識別該個人之原始資料。  五、人工智慧安全：指防止人工智慧應用之相關資料、系統及裝置遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其準確性、完整性及可信賴性。  六、公務機關：指依法行使公權力之中央或地方機關（構）或行政法人。  七、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。  八、非公務機關：指前二款以外之自然人、法人或其他團體。 | 一、本法用詞之定義。  二、第一款所定人工智慧之定義，係參酌美國2017年人工智慧未來法案（FUTURE of Artificial Intelligence Act of 2017），對於人工智慧的定義為「（A）Any artificial systems that perform tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance.Such systems may be developed in computer software, physical hardware, or other contexts not yet contemplated.They may solve tasks requiring human-like perception,cognition, planning, learning, communication ,or physical action.In general, the more human-like the system within the context of its tasks, the more it can be said to use artificial intelligence.（B）Systems that think like humans, such as cognitive architectures and neural networks.（C）Systems that act like humans ,such as systems that can pass the Turing test or other comparable test via natural language processing ,knowledge representation, automated reasoning, and learning.（D）A set of techniques, including machine learning, that seek to approximate some cognitive task.（E）Systems that act rationally, such as intelligent software agents and embodied robots that achieve goals via perception, planning, reasoning, learning ,communicating, decision-making, and acting.」於本條定義人工智慧的概念與意義。  並依「產業創新條例」訂定之「公司或有限合夥事業投資智慧機械與第五代行動通訊系統及資通安全產品或服務抵減辦法」第二條所示，又考量人工智慧之展現，涉及巨量資料、機器學習、演算法、雲端運算、物聯網等相關技術之交互作用，爰將上述相關技術列入，以臻明確。  三、第二款所定人工智慧產業定義，係參酌現行「太空發展法」第三條條文內容，就類似型態之新興領域產業予以修正。  四、第三款所稱巨量資料，亦稱為「大數據」（big data）；其定義係參酌現行依「產業創新條例」訂定之「公司或有限合夥事業投資智慧機械與第五代行動通訊系統及資通安全產品或服務抵減辦法」第二條所示，又考量人工智慧領域之巨量資料，應以非屬個人資料之結構或非結構數據使用於機器學習或演算法等資料訓練過程，爰另與個人資料性質明確予以區分。  五、第四款所定個人資料定義，係參酌現行「個人資料保護法」第二條定之，另參酌歐盟「一般資料保護規則」（General Data Protection Regulation, GDPR）列舉之特殊具敏感性之個人資料範疇，將種族、政治意見及宗教信仰列入個人資料定義範圍。  六、第五款所稱人工智慧安全，係指第一款所列之人工智慧任一相關技術及其物聯網中任一連接裝置，遭受未經授權之侵害，導致不可預知之決策結果（例如自駕車判別錯誤導致意外發生等），其與一般所稱之資通安全應有所區別，爰予以明定。  七、第六款至第八款所定公務機關、特定非公務機關、非公務機關等定義，係考量本法涉及之政府資料公開及通用格式之巨量資料平臺應同時包含公務機關及特定非公務機關為原則，爰同時參照「個人資料保護法」第二條、「資通安全管理法」第三條規定予以明定。 |
| 第四條　（人工智慧發展綱領）  政府應將人工智慧發展列為優先推動政策，並落實以下發展綱領：  一、推動智慧化國家及促進智慧化產業發展。  二、政府應深化人工智慧產學合作生態系，在國家財政能力之範圍內，持續充實人工智慧研發與投資所需經費。  三、政府應持續強化人工智慧雲端運算、儲存、高速網路傳輸、大數據分析與人工智慧軟體之整合環境，使科研創新與產業發展得取得高質量和可追溯的數據。  四、政府應培養科學、技術、工程和數學重點學科之人才，及從事人工智慧研究與應用之人員。  五、政府應以跨部會、跨領域、跨國際的方式，推動人工智慧創新研究中心，並以我國具優勢的人工智慧領域為主題，包含但不限於智慧製造、智慧服務及生技醫療。  六、為避免我國人工智慧發展成果遭受惡意資訊攻擊，政府應訂定適當資安標準，確保供政府和國人使用的人工智慧系統、軟體、硬體，或演算法等之安全性。  本法公布施行後一年內，行政院應提出人工智慧產業推動施政方針。  中央目的事業主管機關應訂定人工智慧產業發展施政計畫，報行政院核定，並定期檢討。 | 一、鑑於鼓勵人工智慧的產學合作，政府應持續撥補預算建構優質產學生態圈，並為人工智慧產業注入活水，促進智慧機器人相關產業創新應用發展，爰明定第一項第一款。  二、人工智慧發展首重數據資料的整合運用，政府針對雲端運算、大數據資料分析，有必要確保科研創新與產業發展得以取得高質量和可追溯的數據，爰明定第一項第二款。  三、發展人工智慧產業所需技術研發必須仰賴高階人才的培育，透過懂得運用AI技術或工具、解決產業問題，以及協助產業AI化的人才，方能完整奠定人工智慧的發展基礎，爰明定第一項第三款。  四、我國人工智慧發展的優勢包含但不限於智慧製造、智慧服務及生技醫療等應用，政府應以跨部會、跨領域、跨國際的方式推動人工智慧創新研究中心，爰明定第一項第四款。  五、人工智慧相關技術與應用奠基於資通訊系統和數據資料庫，一旦遭到駭客攻擊入侵，將造成嚴重的財產、人身安全的危害，故政府推動人工智慧發展應特別重視提高資安標準，確保供政府和國人使用的人工智慧系統、軟體、硬體，或演算法等之安全性，爰於第一項第五款及第六款予以明定。 |
| 第五條　（人工智慧發展之倫理）  人工智慧應朝可信賴之方向發展，在技術或非技術層面追求以下要素：  一、確保人工智慧系統應促進人的能動性與基本權利，而非限制或錯誤地引導人類的自我治理。  二、人工智慧的演算法應將穩固性和安全性列為優先事項。  三、人工智慧的數據資料使用應確保個人享有資訊自主權。  四、人工智慧系統之設計應具備多樣性、非歧視性和公平性。  五、人工智慧之發展應有助於社會的永續發展，並負擔環境及生態責任。  六、人工智慧之系統應被訂有相應的問責機制，使法所不容許之風險發生時有相應者承擔責任。  主管機關應訂定相關的施行辦法，推動督促政府、產業，以及學術單位於人工智慧的研發與應用確實遵循前項要素。 | 一、參酌2018年12月18日，歐盟人工智慧高級別專家組正式向社會發佈了一份人工智能道德準則草案，該草案被視為是「可信賴人工智慧」之重要文件。草案共37頁為值得信賴的人工智慧制定了一個框架，本法參酌該架構並將適切之內容加入本章，期我國人工智慧之發展得有前瞻性的追求方向與目標。  二、確保人性尊嚴與基本人權之保障，人工智慧之發展應促進而非限制人的自主展現，爰定第一項第一款。  三、智慧的技術掌握度會直接影響到使用者的安全性，因此須將穩固性和安全性列為人工智慧的演算法的優先事項，爰定第一項第二款。  四、參酌歐盟的GDPR，人工智慧發展應以保障個人資訊自主權為追求的方向，爰定第一項第三款。  五、人工智慧系統會因為所蒐集的數據和演算法的設計影響應用的多樣性，甚至構成歧視性與公平性問題，爰定第一項第四款。  六、承科學發展基本法之立法意旨，人工智慧亦屬科學發展的一環，應特別重視社會的永續發展，並負擔環境及生態責任，爰定第一項第五款。  七、人工智慧有許多應用涉及設會中的日常生活，如自駕車的交通應用，此時若發生法所不容許之風險，應訂有專為人工智慧設計的問責機制，使相應者承擔責任，爰定第一項第六款。  八、主管機關應透過訂定相關的施行辦法在產官學面落實人工智慧發展之倫理，爰定第二項。 |
| 第六條　（補助、獎勵及輔導）  各中央目的事業主管機關得以補助、獎勵或輔導方式，推動下列事項：  一、促進人工智慧產業創新或研究發展。  二、提供人工智慧產業技術移轉輔導。  三、鼓勵企業設置人工智慧創新或研究發展中心。  四、協助設立人工智慧創新或研究發展機構。  五、促進產業、學術及研究機構之合作。  六、鼓勵企業對學校人才培育之投入。  七、充裕人工智慧產業人才資源。  八、協助地方人工智慧產業發展。  九、鼓勵企業運用巨量資料、政府開放資料，以研發創新商業應用或服務模式。  十、其他促進產業創新或研究發展之事項。  前項補助、獎勵或輔導之對象、資格條件、審核基準、申請程序、核定機關及其他相關事項之辦法，由各中央目的事業主管機關定之。 | 一、人工智慧產業之活動，除企業本身之研發、人才投入外，透過企業間或企業與學術單位間之相互合作等活動之進行，亦可創造加速之效果。另為強化產學交流，得運用補助方式，鼓勵企業提供在學學生實習機會，使學校培育之人才得符合職能所需，俾對產業亦有加乘效果。而為協助人工智慧產業，爰於第一項明定各中央目的事業主管機關得運用補助或輔導方式，推動人工智慧產業發展。  二、第二項授權各中央目的事業主管機關訂定產業補助或輔導辦法，俾資適用。 |
| 第七條　（培訓體系）  政府應加強人工智慧人才培養與引進並建立相應之教育培訓體系。 | 強化人才培育，建立完善的教育培訓體系，提升人工智慧專業水平。 |
| 第八條　（個人資料相關法規調整及利用規範）  惟人工智慧發展過程中，充斥不確定性，應適度開放對於個資之管制，增加資料之可開發性，爰授權行政機關對於因人工智慧發展所涉之個人資料蒐集、處理、利用制訂特別法：  一、為發展人工智慧而涉及個人資料之蒐集、處理、利用，主管機關應於一年內進行國內法規調整，在保護個人隱私條件下，開放個人資料用於人工智慧之研發與運用。  二、為推動人工智慧的研發和人工智慧技術的產業應用，主管機關應基於上開特定目的，就政府部門所蒐集之國民個人數據資料或非個人數據資料，訂定明確的授權使用辦法，並於該辦法中訂明相關申請使用流程、確保使用目的查驗、資料保護方案，以及匿名或去識別化標準。 | 一、我國雖有個人資料保護法用於規範個人資料之蒐集、處理、利用，惟人工智慧發展過程中，充斥不確定性，應適度開放對於個資之管制，增加資料之可開發性，爰授權行政機關對於因人工智慧發展所涉之個人資料蒐集、處理、利用制訂特別法。  二、大數據資料乃是人工智慧發展的重要基礎，因此主管機關有必要針對政府所蒐集的數據訂定授權辦法，使基於推動人工智慧的研發和人工智慧技術的產業應用之特定目的，得依據授權使用之辦法中所訂之申請使用流程獲取所需的數據資料，並應訂明確保使用目的查驗、資料保護方案，以及去識別化標準以兼顧個資保護，爰予第二項以明確規範，以資因應。  三、本條第一項與前條第二項授權行政機關對於因人工智慧發展所涉之個人資料蒐集、處理、利用，為個人資料保護法之特別規定。 |
| 第九條　（特別委員會）  政府應成立人工智慧特別委員會，專司跨部會人工智慧的數據資料整合、基礎人工智慧的研發、人工智慧技術應用部署之諮詢與研究。 | 人工智慧所涉之層面極為廣泛，在政府職能分工上亦涉及國家發展、經濟、財政、金融、內政、交通、通訊傳播、衛生福利、資通安全、科技、公平交易等部會。為排除人工智慧發展障礙，需要行政院針對跨部會議題進行規劃與協調。 |
| 第十條　（特別審核機制）  如人工智慧發展計畫涉及大規模處理高敏感性個人資料、弱勢族群之資料，且有違反倫理規範之疑慮，影響第三人權益時，人工智慧特別委員會應進行審核。 | 人工智慧發展之不確定性主要來自於資料蒐集、處理、利用方式，尤其人工智慧計畫涉及大規模處理敏感性個資，應該經由公正第三方檢視有無違反開發原則、倫理規範，爰規定應由委員會進行審核，確保第三人權益，且委員會審核時不得干預開發之自由。 |
| 第十一條　（智慧化政府推動）  政府一級機關、二級機關、三級機關及獨立機關應設立人工智慧辦公室，負責推動智慧化政府工作及相關聯繫工作。 | 推動政府整體智慧化工作，要求政府一級至三級機關及獨立機關應設立人工智慧辦公室，專責推動政府智慧化工作，以及協助聯繫整體政府智慧化業務聯繫相關工作。 |
| 第十二條　（教育預算）  教育部應匡列預算，於國民基本教育實施人工智慧教育課程。 | 人工智慧教育應從小扎根，立法要求教育部訂定相關課程，在不同的學齡階段給予適當的教學內容。 |
| 第十三條　（沙盒計畫）  政府應規劃、研擬得實施人工智慧計畫之場域或實驗空間，並提供相關協助，且於實驗階段內豁免與該計畫相關之法規限制，並適時評估修法之必要性。 | 人工智慧之發展涉及不確定性與風險性，惟發展結果可能有助於公共利益及社會發展，為協助我國人工智慧計畫於實驗階段能獲得一定程度支持，爰規定政府應仿照沙盒（Sandbox）的精神，提供場域及必要協助，開放人工智慧之發展，並於實驗階段中豁免人工智慧計畫遭遇之法規限制，並隨時評估相關之法規限制是否有修正之必要。 |
| 第十四條　（反歧視）  任何人工智慧系統的開發與應用都應遵循公平、公正、透明的原則，禁止利用人工智慧進行演算法歧視。 | 制定演算法歧視防範措施，保證人工智慧應用的公平性與正義。 |
| 第十五條　（決策糾正）  在重要領域與關鍵環節的人工智慧應用中，應保留人工干預之可能性，確保人工智慧系統的決策可被人類審核、糾正。 | 保留人工干預的空間，確保關鍵決策可被有效審核與糾正。 |
| 第十六條　（國際合作與交流）  政府應積極參與國際人工智慧規則之制定，推動國際合作與技術交流，共同應對人工智慧發展帶來的挑戰。 | 推動國際合作，參與全球人工智慧治理，共同面對挑戰。 |
| 第十七條　本法自公布之日起施行。 | 明定法案的施行日期。 |