美國公布人工智慧適用規範指南草案

賈棕凱 編譯

摘要

今（2020）年 1 月 7 日，美國以備忘錄形式公布「人工智慧適用規範指南」。該備忘錄尚為草案，其明列出十大原則，並且可以大致歸納為三大目標，分別為：（一）確保公眾參與制定人工智慧規則、（二）提倡聯邦政府應輕度監管、和（三）推動可信賴之人工智慧科技的發展。美國各界針對備忘錄草案已提出評論以及更為具體之建議。針對人工智慧的國際發展，美國業已與其他國家就人工智慧之相關議題展開合作。

（本篇取材自：Michael Kratsios, *AI that Reflects American Values*, BLOOMBERG: OPINION (Jan. 7, 2020), https://www.bloomberg.com/opinion/articles/2020-01-07/ai-that-reflects-american-values.）

人工智慧（artificial intelligence, AI）之創新正在創造個人化之癌症治療、改善災難搜索及救援應變措施，自動駕駛車的出現亦使道路更加安全，甚至也帶來其他發展之潛力。但隨著越來越多關於資料隱私、大型科技公司，以及在中國與其他國家興起的科技威權主義（technological authoritarianism）[1]之疑慮，許多人開始思索：我們必須在接納此新興科技及遵循道德規範之間做出抉擇嗎？實則不然，吾人得以反映自由、人權及尊重人性尊嚴價值之方式，推展新興科技。

為建立規範 AI 之準則，川普政府於去（2019）年 2 月公布「維持美國人工智慧領導地位行政命令（Executive Order on Maintaining American Leadership in Artificial Intelligence）」[2]。此命令要求預算管理局（Office of Management and Budget）之首長與白宮科技政策辦公室（Office of Science and Technology Policy）、國內政策委員會（Domestic Policy Council）、國家經濟委員會（National Economic Council）等機關首長合作，並於諮詢相關機關及重要利害關係人後，向其他機關首長公布一份備忘錄，以指引人工智慧適用規範之政策發展（Guidance for Regulation of Artificial Intelligence Applications）[3]。就此，預算管理局代理局長羅素·沃特（Russell T. Vought）於今（2020）年 1 月 7 日發布了此份備忘錄草案[4]。

[1] 學者認為，當資訊科技之發展讓國家得以壟斷資訊並加強對人民的控制，可稱為科技威權主義。王信賢，科技威權主義：習近平「新時代」中國大陸國家社會關係，展望與探索，16 卷 5 期，頁 111，117（2018 年）。

[2] Exec. Order No. 13,859, 84 Fed. Reg. 3967 (Feb. 14, 2019).

[3] *Id.* § 6(a).

[4] OFFICE OF MGMT. & BUDGET, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND

為了解此備忘錄草案所制定之 AI 相關原則，本文將於第壹部分簡介備忘錄草案之內容，第貳部分則說明產官學界對備忘錄草案之評論與建議，最後作一結語。

壹、美國人工智慧備忘錄草案簡介

因「美國 AI 倡議（the American AI Initiative）」[5]為川普執政時期美國 AI 策略之一部分，故白宮於今（2020）年 1 月 7 日公布之備忘錄草案中揭露首創之監管原則，以管理私部門之 AI 發展。在此些原則之指導下，創新者及政府官員將確保美國於接納 AI 的同時，也解決其所帶來的技術及道德挑戰。

此監管原則有十大原則[6]，主要為實現三項目標：確保公共參與、限制監管過度擴張、以及推廣可信賴的 AI 科技。針對第一項目標，川普政府鼓勵聯邦機關在制定 AI 規則時，提供公眾評論之機會[7]，包括來自美國大眾、學術界、產業領導者、非營利組織及公民社會之意見。針對第二項目標，監管原則提倡輕度管制方法。是以，川普政府指示聯邦機關避免預防性、繁複或重複的規則，以免不必要地阻礙 AI 的創新及發展[8]。在採取監管行動前，聯邦機關將被要求進行風險評估及成本效益分析，以評估監管特定 AI 科技的可能利弊[9]。鑑於 AI 之持續發展，聯邦機關將需要建立彈性的框架，以因應各個產業部門的快速變化與最新趨勢[10]。例如自動駕駛車、無人機及 AI 醫療設備均有不同的監管考量。針對第三項目標，監管原則要求推動可信賴之 AI 的發展。當監管者進行 AI 相關監管行為時，必須顧及公平性、透明性、安全性與保障性[11]。聯邦機關亦應為其政策決定尋求可驗證、客觀的證據，並根據最佳科學證據做成技術及政策決定[12]。此外，川普

AGENCIES, GUIDANCE FOR REGULATION OF ARTIFICIAL INTELLIGENCE APPLICATIONS (2020); 此份備忘錄之公眾評論期已於今（2020）年 3 月 13 日截止。Request for Comments on a Draft Memorandum to the Heads of Executive Departments and Agencies, Guidance for Regulation of Artificial Intelligence Applications, 85 Fed. Reg. 1825 (Jan. 13, 2020).

[5] 「美國 AI 倡議」共有六項關鍵政策及實踐方法，分別為：投資 AI 研發（Invest in AI research and development）、帶動 AI 資源（Unleash AI resources）、移除 AI 創新障礙（Remove barriers to AI innovation）、培養發展 AI 的勞動力（Train an AI-ready workforce）、促進支持美國 AI 創新的國際環境（Promote an international environment supportive of American AI innovation）、接納提升政府效能的可信賴 AI （Embrace trustworthy AI for government services and missions）。OFFICE OF SCIENCE AND TECHNOLOGY POLICY, AMERICAN ARTIFICIAL INTELLIGENCE INITIATIVE: YEAR ONE ANNUAL REPORT 4-25 (2020), https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf.

[6] 此十大原則分別為：建立公眾對 AI 的信任、推動公眾參與、重視科學誠信與資訊品質、實施 AI 應用的風險評估與管理、釐清 AI 帶來的效益與成本、採用彈性的規定、秉持公平與不歧視、落實 AI 應用的揭露與透明化、推動 AI 系統的安全性、以及各機關間的協調。OFFICE OF MGMT. & BUDGET, *supra* note 4, at 3-6.

[7] *Id.* at 3.

[8] *Id.* at 2.

[9] *Id.* at 4-5.

[10] *Id.* at 5.

[11] *Id.* at 5-6.

[12] *Id.* at 8.

政府要求聯邦機關，監管 AI 之方法應保護隱私並提升公民權利、公民自由及美國價值[13]。在制定監管方法中特別重要的是，聯邦機關應：檢驗 AI 應用的結果及決策是否導致非法歧視[14]、考慮適當的措施以揭露使用 AI 的時點[15]、以及考慮需要採取哪些控制措施，以確保 AI 系統中經過處理、儲存、及傳輸的資訊具有機密性及完整性[16]。

貳、綜合評論

為了解美國各界對備忘錄草案之意見，本文整理白宮科技政策辦公室官員與產學各界之看法，綜合評論此備忘錄。以下分別說明之：

白宮科技政策辦公室科技長邁克爾·克拉茨修奧斯（Michael Kratsios）認為，美國將根據美國價值持續發展 AI 創新，此與專制政府形成鮮明對比，因後者係一味支持並允許企業運用侵害個人自由及基本人權之 AI 科技。部分國家之政府正強迫企業與其合作，使用 AI 科技監控國家，此些政府監視並監禁異議者、社運人士和少數族群，例如：中國政府對待維吾爾族穆斯林之情形即是[17]。

針對備忘錄在實務上之影響，有論者認為美國需要花費一段時間才能評估此些原則於實務中之效用，且此備忘錄之發展亦將受到各界之密切關注[18]。亦有學者認為此備忘錄係在試圖建立美國 AI 政策之品質管制（quality control）[19]。惟有產業界人士指出，此份備忘錄在近期內不會對一般人產生太大影響[20]。

關於備忘錄之具體建議，則有卡內基大學加尼教授（Rayid Ghani）提出：首先，美國制定更具體之 AI 規範有兩種可行之方式。第一，在特定領域修正現行指導方針，例如僱傭、選舉、公共服務及交通運輸方面。第二，制定更多一般性的 AI 強制規範，而非僅為無拘束力之指導方針[21]。理想情況是結合前述兩種方

---

[13] *Id.* at 1.
[14] *Id.* at 5.
[15] *Id.* at 6.
[16] *Id*.
[17] James A. Millward, *What It's Like to Live in a Surveillance State,* THE NEW YORK TIMES (Feb. 3, 2018), https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html?_ga=2.63866927.1222235247.1581842303-1052500113.1571879499.
[18] Rebecca Heilweil, *AI Poses Risks, But the White House Says Regulators Shouldn't "Needlessly Hamper" Innovation*, VOX RECODE (Jan. 8, 2020), https://www.vox.com/recode/2020/1/8/21056809/artificial-intelligence-new-ai-principles-white-house (quoting Rashida Richardson).
[19] Maria Carnovale, *Guidance for Regulation of Artificial Intelligence Applications (Draft Memorandum)*, SCIPOL, https://scipol.duke.edu/track/guidance-regulation-artificial-intelligence-applications-draft-memorandum (last visited Mar. 21, 2020) (quoting R. David Edelman).
[20] Rebecca Heilweil, *supra* note 18, (quoting Aaron Rieke).
[21] Courtney Linder, *The Trump Administration Wants to Regulate Artificial Intelligence*, POPULAR MECHANICS (Jan. 9, 2020), https://www.popularmechanics.com/technology/a30430579/trump-artificial-intelligence-ai-guidelines/.

式[22]。更重要的是，美國在制定備忘錄後，需要能執行並審核此些規範的人員，並對其進行培訓[23]。產業界通常希望有快速施行或測試 AI 之自由，因此，新規則應透明，並在業者試圖從事可能影響人們生活的新事物時，得以提前回應產業界之疑問[24]。其次，加尼教授認為政府需要為不同類型之公共系統，制定不同級別的規範。此取決於不同系統可能對社會造成的損害、並導致不公平現象加劇的程度[25]。針對低風險之系統，政府也許可以給予更多發展 AI 之自由；針對高風險領域，例如刑事司法、公眾健康、就業等，政府則需要更加關注潛在危害[26]。再者，加尼教授認為川普政府下一步應採取以下措施[27]：第一，界定政府或產業界使用 AI 系統時應公布之事項。此些事項對人民生活所造成的影響程度不一，故應受權責機關查核。第二，界定應受關注之風險，並針對每一項風險提出緩解計畫。第三，建立負責法令遵循的機關。美國政府機關將如何檢驗此些規定是否被遵循、審核流程之內容為何，以及如何建立能夠完成稽查的團隊等議題，仍待制定規範。

肆、結論

美國政府藉由公開備忘錄草案徵詢公眾評論，強調公眾參與 AI 之承諾。白宮科技政策辦公室之目標係透過此備忘錄來推動 AI 共同指導方針之整合[28]。美國政府將藉各單位之合作，制定指導 AI 發展及使用之政策，以便所有人民及社群都能享有 AI 所帶來的利益及機會。針對 AI 之國際發展，川普政府業已加強 AI 研發之合作，其與盟國在國際經濟合作暨發展組織（Organization for Economic Co-operation and Development）中就國際原則達成共識，將在不阻礙 AI 創新之前提下，促進可供信賴的 AI 發展[29]。

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Maria Carnovale, *supra* note 19.
[29] *Forty-Two Countries Adopt New OECD Principles on Artificial Intelligence*, ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (May 22, 2019), https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm.