



建立健全法律制度體系 保障人工智能健康發展

人民政協

全國政協授權香港文匯報主辦
香港友好協進會協辦

專刊

第372期



人工智能是引領新一輪科技革命和產業變革的戰略性技術。它如同一把「雙刃劍」，深刻改變着人類的生存方式和社會交往方式，也帶來了一些倫理和法律方面的風險及挑戰。日前，就「人工智能發展中的科技倫理與法律問題」，全國政協副主席陳曉光、汪永清先後率全國政協社會和法制委員會調研組赴安徽省、江蘇省開展專題調研。委員們真切感受到我國人工智能發展的成就、優勢和潛力，進一步增強了推動我國經濟社會高質量發展的信心。

香港文匯報·人民政協專刊
綜合報道



復旦大學新生進行人臉識別報到。 資料圖片

委員們表示，要認真落實習近平總書記有關重要指示精神，尊重新一代人工智能發展規律，把握好創新發展和風險治理的「度」。要組織專門力量深入研究人工智能創新發展存在的倫理、法律等風險問題，進行風險評估、提出防範意見。需要下大力氣推動研發機構、應用主體加強內部自治，促進行業自律，強化研發、應用人員教育培訓，為人工智能發展營造良好環境。

「刷臉」安全隱患亟待解決

人工智能高度依賴對個人數據的採集和應用，在調研組看來，這是一個亟待重視的問題。

「電腦密碼可以換，但『人臉』這樣的生物數據是不可換的。一旦信息丟失或被攻擊，你就一張臉，怎麼辦？」調研中，全國政協委員談劍鋒多次提及這個問題，並很鮮明地亮出自己的觀點：「我反對用唯一的生物特徵信息作身份認證。」在他看來，目前還沒有足夠安全的方式來保證生物特徵數據不被濫用，如果將各類生物特徵數據集中保存在數據庫中，再被採集到不安全的網絡上，一旦數據庫遭受攻擊，可能造成社會風險。人臉數據洩露不僅會危及老百姓的隱私、財產和人身安全，一旦被境內外非法勢力攻擊獲取，將危及社會安全和國家安全。

如何防範？談劍鋒認為，生物數據一定不能上「雲」，生物數據上「雲」後則完全依賴於「雲」自身安全。世界上沒有任何一個「雲」敢於承諾自己是無懈可擊的、是100%安全的。如果一定要使用人臉識別等生物數據，則一定將生物數據存儲在手機等終端設備上。為進一步增強安全性，不能簡單地將生物數據存儲在手機存儲空間，一定要存儲在安全芯片中，並設置嚴格的安全策略以保護對安全芯片的訪問。談劍鋒還提醒：「對於每一個個體而言，要盡量少用生物數據，或僅僅將生物數據用在不太敏感的場合，不建議用於關鍵場合的身份認證、轉賬交易等，這也是保護自己的方式。」

目前我國數據安全和隱私保護水平總體較低，不能等到出現非常嚴重的生物數據洩漏事件後才亡羊補牢，這是調研組不少委員的一致看法。

現在，全國人大已經把個人信息保護法、數據安全法列入國家五年立法規劃第一序列，這讓委員們充滿期待。「問題的核心在於這些數據的所有權歸誰，現在始終沒有解決。」調研

組組長、全國政協社會和法制委員會副主任陳智敏說：「我認為『人臉』信息這類具有唯一性的數據主權在國家，企業可以使用，但現狀卻是誰搜集誰壟斷。」陳智敏打個比喻說，這就像原始社會向奴隸社會轉化時期，人們佔有土地，誰搶到就是誰的，這種野蠻生長到了需要規範的時候。

清華大學法學院院長申衛星認為，數據的權屬不清已成為人工智能發展的一大制度性障礙，「企業採集、加工個人隱私數據，並不足以讓他擁有所有權，就像一個人寫小說，被改成相聲小品，改編者是不能擁有著作權的。」申衛星認為，數據安全很重要，但如果只注重安全，沒有相應的權益激勵，問題也難以得到徹底解決，他建議根據風險的不同類型給予企業適當的數據財產權益，有使用權但不能有擁有權。

人工智能應遵循以人為本原則

調研中，委員們看到了人工智能在交通、製造、家居、醫療等眾多領域的應用場景，眼界大開。不過，全國政協社會和法制委員會駐會副主任呂忠梅提出了這樣一個問題：「當前我國人工智能的發展方向是什麼？」這也是不少委員一路思考的問題。事實上，每一項先進技術的出現都是為了讓人類的的生活變得更舒服更美好，以「模擬」人類為目標的人工智能就更是如此。

在江蘇省蘇州市極目機器人科技有限公司，調研組在大屏幕上看到了一個有趣的場景：一架無人機從綠油油的農田上方輕巧地飛過，機翼兩邊噴灑出如綿綿細雨般的藥水，重複性的繁重勞動由機器取代，能夠極大地提升生產效率。

與此類似的還有人工智能在醫學影像領域的應用。在無錫祥生醫療科技股份有限公司，一款「掌上超聲」產品吸引了委員們的目光：把一個「探頭」在人體上掃一番，超聲圖像信號就通過無線網絡傳到安裝了超聲App軟件的手機或電腦屏幕上，而且清晰度遠遠超過傳統的超聲儀。

一路上看到的應用場景引發了委員們的思考：我們還處於一個弱人工智能時代，即這些機器和技術能完成指定任務，尚不具備自主意識，更多是在增加人類能力的外延。對此，全國政協委員錢鋒認為，相對於在中高端消費領域的應用，人工智能如何與製造業深度融合、穩定產業鏈供應鏈是更緊迫的課題。在調研組看來，人工智能的發展也應遵循以人為本原則，服務人類才是技術發展的最終目的。

人工智能綜合性立法需慎重

該採取何種方式解決人工智能發展中的倫理規範問題，是委員們討論的熱點。「對人工智能的治理應該分五個層面：法律規範、政府引導、行業自律、企業自覺和公民共識。」科技部新一



第二屆進博會科技生活展區，參觀者觀看可以噴水的擦窗機器人。 資料圖片

代人工智能發展研究中心主任趙志耘認為，對人工智能進行立法很重要，但如果每一項技術都要通過立法去規範，有些技術很快會被新的技術顛覆，立法部門就得浪費大量人力物力。「立法需要確立的是基本的準則，範圍要寬泛。現在最欠缺的是行業自律，企業都在跑馬圈地，政府應該鼓勵做得好的、鞭策做得不足的，為人工智能的發展劃出邊界，給企業確立標準和規範。」

清華大學法學院院長申衛星認為，人工智能的技術發展給法律帶來了非常大的衝擊，而我們的法學研究還停留在「風車磨坊」的時代，沒有看到數據已經成為生產要素，缺乏更深入研究。

全國政協社法委駐會副主任呂忠梅認為，當前應該在數據安全、個人隱私保護等領域做一些制度性規範，處理好人工智能發展和隱私保護的關係，另外還要對從業人員進行倫理道德方面的教育與培養，在教育體制改革上做一些基礎性工作。

全國政協委員魏青松認為，對人工智能的發展進行綜合性立法要慎重，要充分考量公權和私權的邊界問題。現有的法律法規對人工智能領域一些違反倫理的問題是能夠發揮作用的，人工智能的未來究竟會有怎樣的發展，會產生怎樣的影響，目前還難以估算，不宜過早制定剛性法律，以免扼殺創新的可能性。

對此，調研組組長、全國政協社法委副主任陳智敏認為，處理人工智能發展存在的倫理和法律問題，一定要從我們處於「弱人工智能時代」這個基本前提出發，從中國的實際出發，尊重新一代人工智能發展規律，更好推動人工智能安全可控和高質量發展。



在四川省崇州市崇慶街道紅橋村，植保無人機進行農業噴灑作業。 新華社

智能汽車事故責任界定難

汽車的核心部件將不再是發動機、變速箱、底盤這三大件，而是由芯片、軟件以及數據等組成的「大腦」——在人工智能大潮下，這個夢想正在成為現實。

在此次調研中，調研組走訪了多家車企，看到了智能駕駛的各種場景。「車輛到達目的地後，用戶通過手機終端向T平台發送指令，車輛自動駛入車庫並完成自動泊車。利用手機終端發送召車請求信息，車輛能夠自車庫車位自動行駛至召車點……」

委員們認為，在機器決策情形造成事故損失時，責任如何劃分，這已成為一個非常具有挑戰性的法律難題。另外，發生事故時，應該優先考慮乘客安全還是行人的安全，這也是未來智能駕駛技術發展到L4級以後必須面對的倫理問題。

在一些委員看來，人工智能應用場景下，責任相關主體可能涉及

人工智能設計者、生產者、經銷商、使用者等，人工智能系統及其應用場景的複雜性、不確定性使得在事故發生時的責任主體界定困難。這樣的事件已有先例，比如谷歌、特斯拉等自動駕駛致人傷亡事件。

除了「誰擔責」的問題，調研中，委員們也在擔憂智能駕駛技術發展帶來的隱私洩露問題：如果這種技術得到普遍應用後，無論一個人開車要去哪裏、在車裏說了什麼或做了什麼，都不再有私密性，而成為車企或者是車聯網企業眼中的「數據」，可以隨時隨地使用，並從中獲益。對此，委員們建議，要重視數據的過度使用和數據洩露問題，這不僅要依靠企業、行業的道德自律，更要依靠管理部門的立法和監督。



日前，自動駕駛公交亮相鄭州。 新華社