



踏入人工智能 (AI) 時代，相關科技發展百花齊放。香港在面對全球生成式 AI

技術浪潮的衝擊，與科技自主創新的迫切需求中應該如何布局、迎難而上？香港科技大學首席副校長兼香港生成式人工智能研發中心主任郭毅可接受香港文匯報專訪時表示，發展 AI 對於國家以及香港而言均意義重大，而香港在制度、科研資源及政策方面都具備獨特優勢，有信心未來可在金融、醫療、教育領域中作出獨具香港特色的研究成果。

●香港文匯報
記者 鍾健文

AI 促進創新「零到一」研究成果添港味

郭毅可：港具制度政策等優勢 可助力金融醫療教育領域發展人工智能

香港生成式人工智能研發中心 (HKGAI) 於今年2月正式發布 HKGAI V1 大模型，郭毅可表示，這是業界首個基於 DeepSeek 671B 全參數微調並持續訓練產生的大模型，實現了香港本地知識和價值認知的注入，並顯著提高了模型在複雜應用場景中的效率和適用性，特別是在安全性和推理多樣性的性能突破，使其能夠更好地滿足香港本地及海外市場的多樣化需求。

那麼，未來的人工智能是什麼樣子？郭毅可指出，簡單而言，就是一個機器愈來愈具有人的思維能力，「換句話說，在我們的社會中，我們生活中有了一個更像人這樣能夠有主動思維的機器。」

他認為，這帶來的改變是革命性的，因為以前的機器都不可能主動去思考，只是聽人類的指令，「我們要求什麼它就去什麼。」不過現在不一樣，「它可以主動去思考問題，像人一樣去幫助做一些智力的勞動。」所以，「在這樣的一個情況下，它給人們帶來的變化是根本性的，你可以讓它幫你做很多事情，能夠做你不可能做的事情，這對人類本身的發展有重要的影響。」

對接國家戰略 融合國際化標準

郭毅可強調，發展 AI 對於國家以及香港都具有不可或缺的重大意義與貢獻。在「一國兩制」下，香港發揮連接世界和內地的橋樑作用，其高度國際化的環境可以促進東西方在重要、具有影響力的領域之間交流。同時，香港作為國家的窗口，很多 AI 乃至非常有前瞻性的應用，都會在香港做試驗田，例如用 AI 做醫療、教育、法律等，「這些都可以在香港做出很好的樣板，因為我們有健全的醫療體系，也有優秀的法律系統。」而 AI 對基礎研究最大的好處，就是能促進「從零到一」的創新。他表示，香港正在轉型，未來在金融、醫療、教育這些香港別具特色的領域發展中，AI 將起到巨大作用。

他指出，香港在此具備三方面的獨特優勢。在制度優勢方面，香港在「一國兩制」下，既能對接國家戰略，又能融合國際化數據與標準，例如 HKGAI V1 基於內地 DeepSeek 架構進行全參數微調，同時整合香港本地知識，形成符合香港特色的本地大模型。

頂尖科研資源方面，以港科大為主導，與香港



●郭毅可現場示範使用 HKGAI V1。 資料圖片

●郭毅可表示，發展 AI 對於國家以及香港而言均意義重大。 HKGAI 圖片

多所高校及新加坡國立大學等國際機構合作，形成跨學科協同創新。特區政府投入巨資推動建設 AI 超算中心，亦搭建 AI 發展的基座環境，同時積極推動 70 個部門試用 HKGAI 系統，及時予以用戶反饋，推進產品內容優化，加速技術落地，最終可以服務香港民眾。

港能作試驗田 做產業創新

儘管現時 AI 研發的競爭非常激烈，郭毅可提醒 AI 的市場發展還在嬰兒期，「連早期都談不上，我們很多的研究領域都是在初期」。而香港擁有一個非常好的條件，就是能夠作為試驗田做很多的產業創新。他舉例，像是區塊鏈、Web3 技術及虛擬貨幣這些領域，香港是世界上少有幾個可以發展的地區，而且也有很好的監管系統，「在這些特殊的優勢下，香港可以作出很有特色的研究。」

本地 AI「造血」育才

教育是核心機制

創科發展離不開人才的支撐，而培養人才更是人工智能 (AI) 可持續發展的重中之重。郭毅可認為，教育不僅是技術突破的基石，更是本地 AI 人才「造血」的核心機制。而教育在 HKGAI 的研發過程中，某種意義上就是「技術突破的發動機」。他以港科大為例，指大學把課堂變成「實戰戰場」，學生不是死讀書，而是直接參與模型開發，HKGAI 有大量的研究生和博士生作為中堅力量，他們一邊學算法，一邊

幫忙訓練模型分辨法律條文和構造訓練香港價值認知的數據，「在實踐中培養人才，人才也反向推動技術進步。」

郭毅可強調，教育在 AI 時代早就不是單向灌輸，而是讓人才和技術像齒輪一樣咬合轉動，這才是培養富有創新思想的香港人才的關鍵。

對未來有志投身 AI 領域的年輕人，郭毅可建議首要打牢基礎，深入學習數學、算法與硬件原理，例如分布式訓練技術是處理大模型的關鍵；以及擁抱跨學科，因為 AI 需與法律、醫學等領域結合，培養「技術+行業」雙重洞察力；並且以實踐為先，鼓勵積極參與開源項目或競賽，累積實戰經驗；同時亦要關注倫理，AI 發展需兼顧安全與社會責任，例如在訓練中嚴格審核數據合規性。

●香港文匯報記者 鍾健文

僱員用生成式 AI 私隱署指引助定政策

香港文匯報訊（記者 張弦）近年 AI 工具逐漸普及，惟使用生成式 AI 有可能造成公司或個人資料洩露，有外國公司職員曾將軟件代碼輸入至公開 AI 工具，一度導致該 AI 工具關閉。私隱專員公署昨日發表《僱員使用生成式 AI 的指引清單》，協助機構制定僱員在工作時使用生成式 AI 的內部政策或指引，包括訂明獲准使用的生成式 AI 工具，訂明僱員不能利用生成式 AI 進行非法或有害活動等。

私隱專員鍾麗玲表示，公署早前委託生產力促進局進行香港 AI 使用方面的調查，結果顯示近七成受訪機構認為，營運中使用 AI 會帶來私隱風險，而生成式 AI 在新興技術中存在最高私隱風險，已制定 AI 安全風險政策的機構卻僅有 28%。

指引建議，機構需訂明獲准使用的生成式 AI 工具，包括公眾可用或內部開發的工具，獲准許的用途，如列明可用 AI 的員工起草、總結資訊等。機構亦需提供清晰指示，說明批准及不可輸入生成式 AI 工具的資訊種類及數量，例如是否包含個人資料或其他資料。

訂明不能進行非法或有害活動

指引亦建議，機構訂明僱員不能為進行非法或有害的活動而使用生成式 AI 工具，並強調僱員有責任透過校對及查核事實等方式，核

實 AI 生成的結果是否準確，亦應訂明僱員違反政策或指引可引致的後果。

鍾麗玲強調，使用 AI 工具最需要留意信息安全，例如對外開放的 AI 工具不能輸入機構機密和敏感資料。「國外曾發生過有關事故，一家科技巨頭企業員工曾將軟件代碼等公司機密資料，輸入至公開 AI 工具中，導致要立即停用相關工具。」

私隱專員公署科技發展常務委員會委員、立法會議員黃錦輝相信，未來更多機構將在其業務流程中應用 AI，今次私隱專員公署推出指引，可協助機構及其僱員安全地使用生成式 AI，保障個人資料私隱，並促進 AI 在各領域的安全應用及加速培育新質生產力。

●私隱專員公署發表《僱員使用生成式 AI 的指引清單》及後思資料外洩事故調查結果。
香港文匯報記者萬霜靈 攝



遭黑客入侵洩逾 12 萬人個資 俊思違私隱例

香港文匯報訊（記者 張弦）連卡佛旗下的俊思集團去年遭受黑客入侵勒索，導致逾 12 萬人、約 68GB 資料外洩，涉姓名、電郵、電話、護照副本等。私隱專員公署昨日公布事故調查詳情，認為四大主因導致事故發生，包括俊思未有在修復系統故障後適時刪除臨時賬戶、使用已被終止支援的操作系統、資訊系統欠缺有效的偵測措施，及對資訊系統進行的保安風險評估及審計不足，裁定其違反《私隱條例》相關規定，已向俊思送達執行通知，指示其糾正違規事項。

私隱專員公署表示，俊思在去年 5 月 31 日向公署通報資料外洩事故。該公司於去年 5 月 15 日收到黑客勒索信息，聲稱竊取其資料並威脅出售相關資料。調查發現，黑客在設立相關賬戶的 10 天後入侵，相關賬戶是為供應商作系統緊急遠端支援用途所設立，黑客利用相關賬戶取得進入俊思網絡的訪問權限，之後在俊思的網絡進行橫向移動，並利用一個應用程式伺服器上已終止支援的操作系統的保安漏洞，進一步入侵網絡控制器及其他伺服器。

事件牽涉俊思營運的兩個會員計劃：ICARD 會員計劃及 Brooks Brothers 會員計劃，合共影響 127,268 人的個人資料，包括多名 ICARD 會員和 Brooks Brothers 會員，以及部分現職僱員及前僱員等，共四台伺服器及五個系統賬戶被入侵，約 68GB 資料外洩。

修復系統故障後未適時刪除相關賬戶

公署認為，有四大主因導致事件發生。其中，俊思未適時刪除臨時賬戶方面，雖然該公司知悉長期維持供遠端存取的賬戶存在被入侵的風險，但員工疏忽，未有在修復系統故障後適時刪除相關賬戶，最終導致黑客入侵。

公署裁定俊思沒有採取所有切實可行的步驟，以確保涉事的個人資料受保障，違反《私隱條例》相關規定，於上周五（28 日）向俊思送達執行通知，指示其全面審查轄下伺服器，查看是否仍使用不再受支持的軟件服務器等。

公署表示，俊思事後已通知所有受影響者，並進行暗網監控及設立特定電郵地址，以處理相關會員查詢；亦已刪除相關被入侵的賬戶，更換已終止支援的應用程式伺服器，以及安裝端點偵測及回應方案，以進行即時偵測及分析。

私隱專員鍾麗玲總結，事件由於人為疏忽，及欠缺足夠的保安措施保障資訊系統所引致，「假如俊思事前及時刪除相關賬戶，及停止使用已終止支援的操作系統，今次資料外洩事件是相當有機會可以避免。」她提醒所有持有個人資料的機構防患未然，採取適當措施加強資訊系統保安以抵禦惡意攻擊，定期檢視賬戶權限及刪除不必要賬戶；停止使用已被終止支援的軟件，或適時更新軟件；實施有效措施以預防、偵測及應對網絡攻擊等。

AI 指引

- ▶ **提高政策或指引的透明度：**定期向僱員傳達政策或指引，並及時告知僱員任何更新
- ▶ **提供僱員使用生成式 AI 工具的培訓及資源：**教育僱員如何有效及負責任地使用生成式 AI 工具，包括說明工具的能力及限制，提供實務建議及例子和鼓勵僱員閱讀工具的私隱政策及使用條款等
- ▶ **委派支援隊伍：**委派支援隊伍協助在工作上使用生成式 AI 工具的僱員、提供技術支援及解答僱員的疑問
- ▶ **建立反饋機制：**建立渠道讓僱員提供反饋，以協助機構識別可以改進的地方及根據情況更新政策或指引