私隱公署為機構提供指引 助人工智能產業健康發展

定框架護資料 防AI爆隱私

人工智能（AI）在香港日漸普及，根據香港生產力促進局預測，今年全港有近半機構使用人工智能，較去年的30%機構使用大幅增加。然而AI在多項應用場景中，都存在私隱洩露風險，個人資料私隱專員公署曾發現有AI系統要求用戶進行虹膜掃描，資料庫卻無法更新或刪除有關資料，或違反私隱條例，外國亦有AI聊天機器人洩露用戶的信用卡號。為應對有關私隱挑戰，該署昨日發布《人工智能（AI）：個人資料保障模範框架》，作為建議指引，協助機構在採購、實施及使用AI時遵從《私隱條例》，框架亦有助規範相關行業，促進AI在香港的健康發展。 ◆香港文匯報記者 唐文

◆私隱專員公署公布《人工智能(AI)：個人資料保障模範框架》。 香港文匯報記者涂穴 攝

個人資料私隱專員鍾麗玲昨日表示，AI技術近年取得突破性發展，正以超乎想像的方式改變世界，但AI是一把雙刃劍，只有在適當保障措施下，才能帶來更大益處，故該署推出《人工智能(AI)：個人資料保障模範框架》，為使用AI的機構提供國際認可、切實可行的逐步式建議。該框架建議機構對所使用的AI系統進行風險評估，視乎資料保安、資料敏感程度、對個人、社會的潛在影響等因素，較高風險的AI系統需要人類介入，對系統保持控制權，以減低或防止AI出錯。

識別「甩轆」有錯竟不能改

使用AI進行生物資料實施識別身份、求職者評估、工作表現評核、輔助醫學影像分析等均是較高風險應用情景。生物識別方面，鍾麗玲舉例指，該署一次執法行動中，發現有AI系統要求用戶進行虹膜掃描，但存儲的虹膜資料無法100%保證匹配，亦無法更新或刪除，對用戶造成安全隱患，「掃描虹膜後參加者的相關數據並非百分百找到，變相一些客戶或參加者如果想刪除自己的虹膜紀錄，或更正自己的登記紀錄，原來找不到，這便違反了私隱條例的相關規定。」

亦有面容識別系統，對有色人種識別率偏低，特別是黑人女性面容對比容易出錯，涉嫌歧視，亦屬高風險AI系統。醫學領域AI出錯亦不鮮見，鍾麗玲引述美國一宗個案，有護士懷疑AI診斷結果出錯，最後證實AI誤將血癌病人診斷為敗血病，「雖然護士成功推翻了AI的判決，但整個過程增加了病人的感染風險，醫藥費支出亦更高。」

聊天機器人或向「下一手」爆料

該框架又建議機構制定AI事故應變計劃，當AI出錯導致侵犯私隱、財產損失，或被黑客攻擊等情況時，作出及時處理。鍾麗玲提到，去年3月，有生成式AI聊天機器人發生震驚世界的資料外洩事故，部分用戶的對話標題、電郵地址、信用卡號碼等遭到洩露。「很多時候大型AI模型需要大量資料做分析，向AI提供資料時也要謹慎。例如有韓國企業的員工曾將公司機密資料、客戶資料等數據提供給聊天機器人，AI保存了這些資料，可能與下一個用戶聊天時洩露出來。」

公署制訂該框架，期望協助機構在採購、實施及使用人工智能時，遵守《私隱條例》的相關規定。鍾麗玲表示，該框架雖非強制性法律文件，但屬國際一般規則，對機構以合乎道德、負責任、保護私隱的方式使用AI。有倡導、指引作用，公署會向政府部門、醫院、學校、大型企業等主要使用者派發相關文件，亦會舉辦講座加強宣傳。至於香港目前的AI應用風險，鍾麗玲指暫未發現高危情況，公署自去年8月至今年2月審查了28間本地機構，當中10間機構會透過AI收集個人資料，均有相應保安措施，其中一間機構搜集完資料後會在大數據中刪除個人信息，署方會繼續展開下一輪審查。

數百人資料Tg洩密 勿轉載免犯起底罪

香港文匯報訊（記者 文森）個人資料私隱專員公署過去12個月，共收到1,044宗有關市民個人資料被套取作詐騙用途的查詢；單是上月就有超過130宗，較每月平均50宗大幅上升。同時，公署昨日表示高度關注一個懷疑由黑客營運的Telegram群組，該群組連日來上載多個涉及不同公司的個人資料樣本檔案，包括懷疑是客戶的姓名、身份證號碼及電話號碼等資料，公署正聯絡相關公司了解情況。公署前日亦收到其中一間公司就資料外洩事故的通報，暫時就事件收到1宗查詢，未有收到投訴。

該個懷疑由黑客營運的Telegram群組，上周三（5日）上載一個名為「香港快遞」的個人資料樣本檔案，內含299人的姓名、電話及地址，以及郵件追蹤編號等個人資料。懷疑涉及至少兩間快遞公司。

個人資料私隱專員鍾麗玲呼籲市民，如果在網上發現一些不當披露個人資料的帖文，切勿轉載，以免構成起底刑事罪行，而且有關連結多數含有手機或電腦程式病毒，隨意下載或有中毒風險。

四大範疇建議 持續修正防走歪

香港文匯報訊(記者 唐文)《人工智能(AI)：個人資料保障模範框架》涵蓋四個範疇的建議措施，包括制定AI策略及管治架構；進行風險評估及人為監督；實行AI模型的定製與AI系統的實施及管理；及促進與持份者的溝通及交流。

對於AI管治架構，個人資料私隱專員鍾麗玲表示，建議大型企業、公營機構等成立AI管治委員會，委員會應向董事會匯報，同時應建議內部匯報機制，匯報任何系統故障或提出有關資料保障或道德問題，以便AI管治委員會作出恰當監察。若是僱員很少的中小企，則可由老闆直接負責AI管治工作。鍾麗玲續指，管理AI系統不是一勞永逸，科技環境、監管環境時常發生變化，機構需要保持對AI系統的持續監察，妥善記錄存檔，定期審核，隨着風險因素演變而檢視現有機制。機構亦應盡可能了解AI系統的能力和限制，避免過分依賴AI輸出結果，當AI輸出結果異常時，可作出標記或在適當情況下推翻結果，甚至介入及中斷AI系統運作。

私隱專員公署科技發展常務委員會委員、立法會議員黃錦輝表示，適逢國家快速發展新質生產力，開展了「人工智能＋」行動，今次指引可協助企業善用AI技術，促進產業創新及升級轉型，幫助推進香港數字經濟發展、加速建設香港成為國際創科中心，積極融入國家發展大局。

黃錦輝並指，推出《人工智能（AI）：個人資料保障模範框架》的意義不在於規限企業，而是為新興數碼產品制訂安全標準，「就像工程行業有不同標準，我們這次訂立AI標準框架，顧問公司、中小企都可利用，令他們在數碼時代（利用標準化）接觸更廣，多做生意。」

AI事故應變計劃流程

01.界定
- 機構定義AI事故性質，例如因AI系統開發或使用對人、財產或環境造成損害的事件，包括侵犯私隱、歧視等

02.監察
- 留意和監察可預見的損害類別，並制定程序應對不可預見的損害
- 從AI事故資料庫中得知過去發生的AI事故

03.通報
- 制定內部政策和程序，以便員工就事故作出匯報，其他合作夥伴、客戶等亦應有反饋渠道

04.遏止
- 指派人員暫停或停止相關AI系統，並切斷涉事系統與其他職員系統的連接
- 在可行情況下，盡快通知監管機構和受影響人士

05.調查
- 徹底檢視和調查AI系統，並作出技術修補
- 只有在確定進一步損害、風險等降至最低後，才可恢復涉事AI系統運作

06.復原
- 記錄事故，根據調查結果進行AI相關內部政策修訂

資料來源：《人工智能(AI)：個人資料保障模範框架》
整理：香港文匯報記者 唐文

◆黃偉綸(前排左五)與應屆獎學金得主合照。

25位本地大學精英膺創新科技獎學金

香港文匯報訊(記者 莫楠)現今全球創科業競爭日益激烈，為鼓勵及培育更多本地科研人才，創新科技獎學金2024昨日舉行頒獎典禮，為25位本地大學學生頒發最高15萬港元獎學金，得獎學生並可參加由獎學金提供的多元精英培育項目，幫助培養他們成為具國際視野的未來創科領袖。有得獎學生受當醫生的爺爺啟發，期望透過獎學金支持參與耳鼻喉科的機械人手術研究，追尋當醫學研究員夢想。

今年獲頒創新科技獎學金的學生來自多所大學，就讀包括計算金融及金融科技、環球中國研究、醫學、獸醫學、生物科技及商學、生物醫學，以及藝術科技等不同學科。香港中文大學環球醫學領袖培訓專修四年級生張愷珊是其中之一。她自幼受到爺爺的啟發，立志成為醫生和醫學研究員。目前她正在跟隨名醫陳英權進行耳鼻喉科的機械人手術研究。張愷珊表示：「獎學金不僅提供了實質的經濟支持，也讓我有機會參與海外臨床實習和國際會議，這激勵着我繼續追尋夢想，積極參與在腫瘤學和手術領域的研究和發展，特別是耳鼻喉頭頸外科。」

另一位得獎者是香港城市大學理學士(計算金融及金融科技)的馮景培。他自小雙耳弱聽，學習語言相對困難，但未能得到助聽器和助學金的支持。因自身的遭遇，讓他立志通過研究，幫助非政府機構(NGO)量化成果，建立專為NGO而設的永續投資分析平台，內設數據庫和不同分析指標，以有效計算和評估其成效，穩定NGO的資金流，幫助更多弱勢群體。

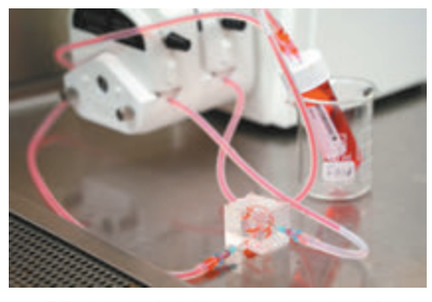
特區政府財政司副司長黃偉綸在頒獎禮致辭時表示，香港的傳統優勢在於國際金融中心和國際貿易中心，而創新和技術是香港創造新經濟增長的引擎，獎學金有助培育更多未來領袖才能，建設香港成為國際創新科技中心。

港大研「肝立方」個人化仿真肝代試藥

香港文匯報訊（記者 高鈺）癌症患者因腫瘤與免疫微環境的異質性，對藥效、副作用及耐藥性產生不同的影響，而肝癌病人缺少精準的藥物篩選方法，往往經歷多線治療失敗後，仍難以找到最適合的藥物，為患者帶來巨大的經濟負擔，更錯過最有效殺死腫瘤細胞的黃金時機。香港大學醫學院科研團隊成功研發出「仿生肝立方：肝癌和肝病的全面精準診療平台」，透過三維生物打印仿製病患肝臟，有助快速評估各種傳統藥物和新興療法的功效和副作用，讓醫生作出精準診療決策。

快速評估療效 膺日內瓦發明展金獎

該項新技術早前參展日內瓦國際發明展勇奪評審團金獎及「中國發明協會」特別獎。港大團隊昨日分享了項目中首創的三個核心技術：**第一**，細胞、基質蛋白分離技術，從肝癌患者的組織中提取肝細胞、腫瘤細胞、免疫細胞及基質蛋白，為病人訂製高度仿生化的體外肝癌模型「肝立方」，能精確模擬腫瘤特徵，如各類細胞的數目、組織硬度、免疫微環境等，成為個人化高標準的藥物篩選平台。



◆「肝立方」能夠精確模擬每個患者的腫瘤特徵。

第二，團隊運用先進的三維生物打印技術，製成具有正常組織、腫瘤組織、血管結構的體外模型，比傳統三維細胞培養和類器官等模型更仿生化、更能還原病人腫瘤內的實際情況。

第三，這個高度仿生腫瘤微環境體外模型內置創新的微血管系統，可在實驗室環境中持續進行藥物測試及評估各項療法的治療效果。

港大醫學院臨床醫學學院外科學系講座教授萬鈞指，「肝立方」精準模擬病人真實病況，可替代動物模型而廣泛應用於新藥研發，提供新藥臨床前有效性與安全性測試，為開展臨床試驗提供更真實準確的數據，從而縮短研發周期、降低成本、提升新藥成功率。在基礎研究方面，該項發明可多維度、立體化模擬肝癌與肝病微環境，推動科研人員深入發掘疾病免疫微環境的調控機制，有助加速發現新的免疫治療靶點和開發新的治療手段。現時「肝立方」正進行臨床前研究、臨床效能研究及安全性評估，團隊希望可盡快推出產品。