



洩密漏洞 企業員工擅用未授權 AI

專家倡政府提供安防工具 補貼培訓網安人才

1 1 0 1 0 1 0 0 0 1 1 0 1 0



正視 AI 風險②

AI 於本港企業辦公、商業運營、金融審批、人力招聘等領域日漸普及，多數機構只看重生產力提升，卻忽視背後隱藏的雙重風險：一是中小企普遍存在的數據外洩漏洞，二是無透明機制的算法黑箱，默默影響全港市民的求職、貸款、保險、租住權益。

生產力局首席數碼總監黎少斌引述生產力局最新調查指出，本港絕大部分中小企未設立專職或兼職網絡安全人員，系統更新、權限管理、數據保護、員工培訓等基礎安防工作長期真空。企業推行 AI 數碼化後，最大的安全隱患並非外部駭客攻擊，而是內部員工私自使用未經公司授權的免費 AI 工具，這將導致智能危機更加嚴重。

大公報記者 苑向芹、蘇榮

黎少斌
(生產力局首席數碼總監)：



專家之言

香港中小企最大的 AI 安全漏洞，並非高端技術缺陷，而是無人負責、無規範、無培訓，員工隨意用免費 AI 外洩公司核心數據。

邱達根
(立法會科技創新界議員)：



本港大量中小企掌握海量市民數據，卻缺乏安防資源，是全港網絡安全最薄弱的環節，需要政府平台兜底支援。

關韜睿
(香港大學法律學院助理教授)：



AI 輔助決策若缺乏適當的解釋、人工覆核及操作紀錄，可能增加市民提出異議和舉證的困難。

風險正隨中小企 AI 普及日趨氾濫。

現時 AI 已廣泛應用於本港中小企辦公營運、人力招聘、信貸參考、保險定價及租務審批等場景。根據生產力局與私隱專員公署 2024 至 2025 年度聯合 AI 安全調查，本港超半數中小企已日常使用 AI 工具提升效率，但多數企業只看重生產力提升，完全忽略數據安全與算法透明的雙重風險，形成「技術走得快、規範跟不上」的失衡局面。相比大型企業完備的防禦體系，中小企已成為本港 AI 風險的重災區，既存在高頻內部數據洩露風險，亦充斥不透明的算法隱性歧視，直接影響普羅市民的日常生活。

立法會科技創新界議員邱達根直指，本港中小企是 AI 風險管控的薄弱環節。不少服務普羅大眾的中小企業，手握大量市民個人資料，卻受限於資金、技術、人才短板，無法像大型企業一樣搭建 AI 防禦體系、開展高頻安全演練。一旦中小企數據洩露，受影響的是全港廣大市民。他建議，數字政策辦公室應優化公共服務平台，向中小企免費提供基礎安防工具、漏洞檢測服務，同時透過政府補貼開辦行業培訓，緩解網安人才短缺問題。

數據外洩的顯性風險，亦加劇了 AI 算法黑箱帶來的隱性不公，而且長期被社會忽視。現時本港銀行信貸、保險定價、企業招聘、租務審批，普遍引入 AI 自動評分與篩選機制。算法依託歷史數據運行，會複製甚至放大社會固有偏見，對特定年齡、居住地、消費習慣的市民形成隱性歧視。

AI 輔助決策若缺乏適當解釋及可追溯紀錄，可能增加市民了解決策依據及提出異議的困難。香港

大學法律學院助理教授關韜睿建議，企業使用 AI 時，應按用途和風險設置適當的人工覆核安排，並保存必要的操作紀錄，這有助發現問題，亦可為日後釐清責任提供重要依據。

建立「與風險共存」防禦體系

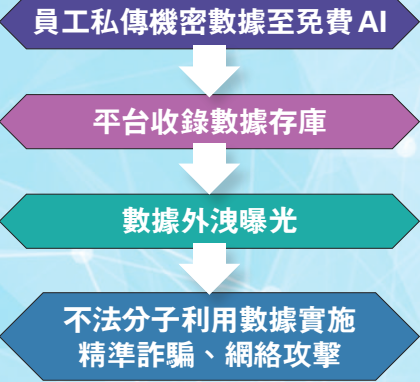
黎少斌建議，中小企需徹底轉變安防思維，拋棄「絕對防禦」的傳統觀念，建立「與風險共存」的新型防禦體系。在無法徹底杜絕入侵的前提下，做好數據加密、定時備份、權限分級，最大程度降低數據外洩與系統被攻破的損失。而成本最低、最有效的第一步，即是指派專人統籌企業網絡安全與 AI 使用規範。

上述專家不約而同指出，對於普羅市民而言，面對算法無形的「人生審判」，被 AI 系統作出不利決定時，不應默默接受。市民可主動向企業、金融機構查詢決策依據，保留溝通紀錄，若懷疑個人資料被不當利用、遭遇算法歧視，可向個人資料私隱專員公署求助投訴，維護自身權益。



▲ 越來越多企業員工使用 AI 提升工作效率，但背後的安

中小企數據外洩連鎖風險鏈



中小企 AI 安全漏洞與對策

漏洞	解決方法
無專人負責安防	指派專人統籌
員工私用未授權 AI	制訂 AI 使用守則
數據無加密備份	開展員工安防培訓

資料來源：生產力局調查、黎少斌專訪

「內部人為疏忽，遠比外部技術攻擊更致命，也是本港企業最普遍的 AI 安全死穴。」生產力局首席數碼總監黎少斌對《大公報》表示，在全民 AI 的大潮下，愈來愈多的員工為提升工作效率，將客戶資料、商業機密、項目文件、個人敏感數據直接上傳至公開 AI 平台。專家指出，此類操作極易導致數據被 AI 平台收錄訓練，最終造成大規模資料外洩，成為不法分子實施精準詐騙、網絡入侵的素材。

近年香港發生多宗真實私隱外洩個案，暴露本地中小企 AI 應用的嚴重漏洞。一間負責民生服務的本地中小企員工，為節省工時、快速整理客戶檔案，未經公司批准，擅自將數百名市民的住址、聯絡方式、收入紀錄及服務紀錄等敏感資料，批量上傳至免費生成式 AI 平台整理報告。相關數據被 AI 平台後台自動收錄訓練，其後資料外洩，被不法分子用於精準電話詐騙及個人資料盜用。多名市民長期受騷擾，投訴時卻發現企業沒有任何 AI 使用規範、操作紀錄與數據管控機制，無法溯源、無人問責。

手握大量市民個人資料

黎少斌指出，與數據外洩同樣普遍的，還有「無形的算法審判」：不少市民求職被篩走、貸款被拒、保費被調高，卻從未收到合理解釋，一切皆是 AI 黑箱自動決策所致。這類隱性

「黑箱審判」自助評分 AI 令求職者屢屢落選

隨着 AI 深度融入香港商業與民生場景，算法黑箱已成為繼數據外洩後，本港最隱蔽的數碼風險。不同於可溯源的網絡安全事件，AI 黑箱運作具備不透明、無解釋、難舉證的特質，讓市民時刻面臨系統自動做出的「隱性人生審判」，卻無從申訴維權。

現時本港招聘、信貸、保險、租務等領域，普遍採用 AI 自動評分與篩選機制。AI 依託歷史大數據運行，會不自覺複製社會固有偏見，將年齡、居住地、職業等標籤轉化為隱性歧視標準，造成部分群體求職落選、貸款被拒、保費偏高的不公結果。更關鍵的是，

多數中小企以商業機密為由，封鎖算法運算邏輯與評分規則，形成完全封閉的決策黑箱。

香港大學法律學院助理教授關韜睿指出，缺乏適當的人工覆核及操作紀錄，可能增加釐清決策依據和責任的困難。企業應按用途和風險落實相關保障。他亦建議為中小企提供實用指引和技術支援，協助做好風險管理。

專家呼籲，破解算法黑箱亂象，需建立透明化機制。政府應強化監管引導，要求民生領域 AI 決策保留覆核流程與完整紀錄；企業需主動公開基礎評分規則；市民亦應提升權益意識，主動查詢 AI 決策依據，打破算法壟斷，守護數碼時代的社會公平。

破除 AI「隱性審判」

生活場景	AI 運用方式	維權途徑	監管機構
求職招聘	AI 自動篩選履歷	查詢篩選標準、保留紀錄	勞工處
銀行貸款	AI 風險評分審批	索取書面審批理由	金管局
保險服務	AI 核定保費風險	申請覆核評估結果	保監局
個人私隱	AI 儲存分析個人數據	投訴、查閱個人數據	私隱專員公署

人工智能研發院今年將投入運作 推動 AI+ 發展

【大公報訊】記者李樂兒報道：香港五年規劃提出，構建「三大創科園區、五大研發機構」，打造具國際競爭力科技產業先進研發中心與中試轉化基地。創新科技及工業局副局長張曼莉接受專訪時指出，新格局下的「人工智能研發院」、「生命健康研發院」兩大重點機構正密鑼緊鼓推進。

張曼莉透露，人工智能研發院年內將投入運作。目前董事局已完成組建，行政總裁與營運總監招聘工作進入最後階段，目標如期啟動，以推動本港「AI+」發展。她指出，人工智能研發院將擔當領頭羊的角色，引導並助力香港 AI 創新發展及產業

應用，有組織地統籌協調，助力上游 AI 科研，並進一步推動中下游成果轉化，開拓更多應用場景，深化拓展「AI+」行動在香港的發展賦能，透過技術賦能經濟社會進一步發展。

人工智能研發院設有五大使命及工作方向，包括 AI 前沿領域的研發和突破，「AI+」賦能產業升級，完善 AI 治理體系，深化國際創科交流與高端人才匯聚，開展人才培訓並推動 AI 普及應用。至於生命健康研發院，主要聚焦「人工智能+生命科學」。

張曼莉表示，生命健康研發院目前已成立督導

委員會，制定研發院發展方向及提供指導意見，並即將委聘董事局，成員將包括具不同背景及經驗的專家學者及特區政府代表，同時行政總裁全球公開招聘工作正同步開展。研發院將以「1+3」（一總院+三分院）模式推進，即河套深港科技創新合作區香港園區（河套香港園區）的生命健康研發總院，加上三所由大學籌建的分院。據悉，總院預計今年內基本完成籌建，將用作實驗室及辦公室。三個分院將依託其負責大學的優勢資源，分別聚焦先進診斷技術、新一代預防技術、疾病治療及老年相關疾病研究等重點領域展開研究。目前各分院已提

交建議書，創新科技署正進行審批及研究，期望盡快開展有關工作。



▲ 生命健康研發院將設於河套香港園區，由大學籌建的分院，另有三所由大學籌建的分院。大公報記者林堅攝