肆意收集個人資料訓練演算法 用戶失對話數據付款信息

ChatGPT違私隱規定 意下禁令促解釋

◆意大利當局以AI技術透明度不足為由，暫禁止使用ChatGPT。圖為意大利個人數據保護局。網上圖片

意大利個人數據保護局稱，當局認為ChatGPT沒有提供足夠法律依據，合理解釋AI大量收集和儲存個人資料以「訓練」演算法的做法。平台沒有詳細告知用戶如何收集處理各項信息，也沒有設置符合當地法律規定的年齡驗證系統，確保用戶年滿13歲，且不會讓未成年人接觸非法材料。

母公司OpenAI或被罰2千萬歐元

意大利當局還指出，ChatGPT上月出現用戶對話數據和付款服務信息丟失問題，加劇當局的擔憂。意國據此要求母公司OpenAI必須在20天內通報採取哪些措施保障用戶私隱，否則可被處以最高2,000萬歐元，或相當於公司全球年營收4%的罰款。OpenAI回應稱願意與意國當局合作，並在意大利將ChatGPT下線。

澳洲悉尼大學商務信息系統教授蓋爾分析稱，ChatGPT以大型語言模型為基礎，OpenAI為此收集約3,000億個從全球互聯網系統性收集的詞彙，包括書籍、文章、網站和公開的社媒帖文等，當中或包括未經授權的個人信息，「嚴格來說，如果您曾經撰寫過社媒帖文或發表過評論，那麼它們都不排除已被ChatGPT使用。」

ChatGPT沒保障「被遺忘權」

蓋爾強調，依照全球私隱保障法律的一項基本原則，個人信息不應被外洩到「其最初產生的環境以外」。即使ChatGPT收集的是公開可用的數據，公司為訓練演算法將大量數據拆解重組，也會破壞一些詞句的上下文完整性。他也批評OpenAI未有解釋用戶能否要求公司刪除自己的個人信息，「在信息不準確或有誤導性時，這種被遺忘權非常重要，但ChatGPT沒有相應的保障。」

部分全球知名出版商據報已審查名下產品內容，確認有版權歸屬的資料多大程度上被用於訓練AI聊天機械人。不過蓋爾提醒，即使是一些沒有明確版權歸屬但較為敏感的信息，也可能在用戶給出指引時被外洩，「這可能是一段代碼、一份草案或是一段正在草擬的論文，但它們都或被收集並作公共用途。」

蓋爾最後提醒，OpenAI已提及公司不排除未有預先通知，就與第三方共享用戶個人信息，情況令人擔憂。「AI技術有許多潛在好處，但我們也要記住，OpenAI是一家私營的牟利機構，其利益和商業需要不一定符合更大的社會需求。」

透過對話推測用戶特徵 AI聊天收集「隱形數據」

香港文匯報訊 人工智能（AI）聊天機械人ChatGPT強調其沒有利用任何用戶的個人信息。不過美國網絡私隱專項律師傑薩尼解釋，互聯網時代個人信息的定義不斷更新。AI技術在收集大量數據基礎上滿足用戶需求，意味「用戶與AI聊得愈多，AI對用戶的了解愈多」，愈容易推測用戶的個人特徵，這些正是企業投放廣告或宣傳產品時所需的資料。如何監督AI收集或使用這些「隱形數據」，將是監管機構一大挑戰。

傑薩尼提到，AI聊天機械人理論上可結合數據庫的大量資料，從對話中推測用戶的年齡、性別、職業或興趣等。相關數據經收集整合，能夠更精確描述用戶群體特徵，這些資料不排除會被有償提供給廣告商，讓制訂廣告投放更精準。這也意味部分個人信息即使公開可用，也可能產生潛在私隱問題。

罪犯引導AI猜測賬號密碼

傑薩尼還設想稱，雖然AI聊天機械人不會主動提供其他用戶的非公開資料，但企業不排除要求AI機械人依照一些社媒用戶的公開信息，分析其是否為合適的廣告投放對象，更不排除有潛在犯罪分子引導AI技術解構公開資料，猜測特定用戶或會使用的賬號密碼，或竊取其他敏感數據。

傑薩尼認為，監管部門可以主動針對AI技術的特點，設立數據收集和使用相關規定，而非暴露出私隱外洩問題後再收緊監管要求，「就像全球各國立法限制企業收集個人資料作定向廣告投放一樣，類似方法或可避免濫用AI技術帶來意想不到的問題。」

◆意國個人數據保護局網站公布相關指令。網上圖片

◆用戶與AI聊得愈多，愈容易被收集「隱形數據」。網上圖片

◆披猜預期會有相應監管AI的方式產生。網上圖片

專家：AI長遠發展需符合人類利益

香港文匯報訊 歐洲初創企業資訊網站Sifted創辦人桑希爾認為，人們對AI技術的擔憂現時還不足以阻礙其發展，但其長遠發展方向需符合人類利益，否則勢必面臨更多質疑聲音。桑希爾分析稱，作為一項新興技術，AI技術遭到質疑甚至反對非常正常，就像火車、汽車、電腦和互聯網新興產品問世時，社會也需要一定時間才能適應。

政府頒令配合監管

桑希爾表示，在AI技術領域，許多科企都互為商業競爭對手，部分科企出於有意放緩對手發展速度、保障自身商業利益的批評聲音，也需要用戶詳細辨別。

桑希爾指出，關於AI技術涉嫌侵犯私隱等質疑聲音正在浮面，「或許設立獨立專家機構，審核科企的AI技術演算法並限制其適用範圍，應該是政府監管議程的下一個項目。」

ChatGPT掀辦公室風波 員工變依賴高層憂洩密

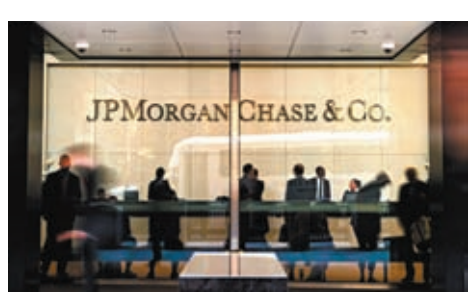
香港文匯報訊 自去年11月底問世以來，ChatGPT迅速被眾多職場人士所接受，除用它來編寫可以自動執行任務的代碼外，還利用該技術來生成充滿職業口吻的電子郵件，但不知不覺間，一場辦公室風波正在醞釀，管理者已開始對出自ChatGPT的工作予以反擊。

調查顯示，ChatGPT已為員工廣泛使用，部分更指工作效率大為提高。然而，許多領導者都對員工可能會分享的企業情報感到緊張，包括摩根大通在內的幾家大公司已屏蔽ChatGPT的訪問渠道，其他公司則鼓勵使用替代方案，例如亞馬遜等。

律師樓憂總結判例欠準確

法律及商業資訊服務商律商聯訊首席產品官巴克利談到，ChatGPT讓律師們興奮不已，因為它可以減少耗時的繁瑣工作，包括總結判例。但一些律師事務所已頒布新規，包括限制員工在ChatGPT平台上輸入專有信息、禁止律師將未經編輯的人工智能（AI）生成文本作為法律意見分享給客戶。巴克利說，其中一大擔憂在於準確性問題。

對於如何監控和管理生成式AI在職場上的應用，許多企業仍在努力尋找答案。根據工作聊天類應用程式Fishbowl在1月份的一項調查，在受訪的近1.2萬名上班族中，40%以上的人表示，他們會在工作中使用ChatGPT或其他AI工具，其中近七成的人說，他們沒有將此事告訴老闆。



◆摩根大通已屏蔽ChatGPT的訪問渠道。網上圖片

籲暫停高級AI訓練 科企公開信遭潑冷水

香港文匯報訊 逾千名科技界和人工智能（AI）領域的領袖早前聯署公開信，呼籲6個月內暫停高級AI的訓練及開發，當中包括Tesla行政總裁馬斯克、蘋果公司聯合創始人沃茲尼亞克及Stability AI總裁莫斯塔克等重量級人物。他們聯署公開信的理由是AI可能對社會和文明構成潛在風險，引發熱議。

《華爾街日報》援引該公開信背後的組織者之一泰格馬克的話表示，AI的進展已超過許多專家幾年前認為可能達到的程度。他說，「這就像是一場自殺式競賽，誰先到並不重要，重要的是整個人類有可能會失去對自己命運的控制。」泰格馬克表示，6個月的暫停開發將讓整個行業獲得「喘息機會」，那些選擇謹慎行動的公司並不會處於劣勢。

諸多業內人士對公開信提出不同意見。Meta副總裁兼首席AI科學家勒邱恩沒有在信上簽名；莫斯塔克則發推文稱，雖然自己已在信上簽名，但他不贊同暫停開發6個月的提議。同時，據美國CNBC網站上月29日報道，Google也並未受到這封公開信的影響，其正在重組虛擬助手部門，以更加專注於開發AI聊天技術Bard。科大訊飛股份有限公司高級副總裁杜蘭表示，暫停AI訓練是非常困難，「AI的快速發展的確會帶來失業、私隱被侵犯等問題，但它更多的是提升人們的效率、醫療、改善環境等。」

Google CEO 籲着眼有效管理AI應用

香港文匯報訊 Google正研發人工智能（AI）聊天機器人Bard，行政總裁披猜表示，將致力於讓Bard導入更複雜的語言模型，提供更自然的互動體驗，但也強調AI應用中的私隱安全問題非常重要，並認為現在很難停下AI的發展腳步。

現趨勢難停下發展AI腳步

披猜指目前並非只是專注讓Bard在AI技術競賽勝出，更強調重視AI技術應用過程中伴隨的隱私安全問題。披猜認為AI技術確實應該要有相應管理辦法，但以現行趨勢很難停下發展AI腳步。

披猜表示，除非政府機構強行介入限制AI技術發展，否則即便Google或OpenAI同意暫停發展AI技術，仍無法讓其他業者停下腳步，因為AI技術已經變得更加重要，甚至成為許多運算發展基礎。因此，披猜認為，重點不應該放在是否暫停AI技術發展，而應該着眼於如何有效管理AI應用。隨着更多AI應用發展普及，披猜預期會有相應監管方式產生，進而讓多數人對於AI技術發展的擔憂獲得改善。