(2025-08-01修改版R2)

書面質詢

馬耀鋒議員

關注人工智能深偽技術衍生的數據安全問題

人工智能（AI）的迅速發展，對社會及經濟發展帶來巨大機遇，同時亦帶來了全新形式和難以提防的犯罪挑戰，當中尤以深偽技術所涉生的詐騙、侵犯個人信息、製造虛假信息為主要方式，引起國際的共同關注。早前保安司公佈罪案統計數據時，經已指出4月接獲首宗AI深偽技術詐騙案，本澳如何有系統地預防和抵禦有關挑戰，值得政府及早研究和規劃。

事實上，社會已有不同意見，建議政府透過立法手段，以專門法律法規強化預防及打擊相關犯罪行為。除此之外，在相關工作有實質進展前，特區政府亦有必要盡早堵截可能出現的漏洞，特別現時本澳資訊科技普及，公營及私營線上系統已普遍採用多元的身份認證手段方便居民使用；以一戶通為例，就兼容人面識別的功能，但在AI深偽技術的挑戰下，有關系統的安全性受到明顯威脅。譬如國內就曾發生不法之徒利用AI換臉突破金融平台的人面驗證，盜刷受害者銀行卡的個案。澳門在一戶通已逐漸成為居民處理政務服務主要平台下，當中儲存的個人隱私和資料集中，當局如何提升其識別能力和安全性，值得重視。

此外，現時“網絡安全事故預警及應急中心”作為針對公共部門及關鍵基礎設施營運者的網絡安全事件進行監察、預警及緊急處置的主要實體，在統籌提升本澳應對人工智能犯罪的各項能力上具重要角色和功能；然而，早前保安司司長在口頭質詢時亦明確表示，保安部門在招聘網絡安全人才方面存在困難，難免令社會擔憂本澳預防相關網絡安全風險的能力不足，當局有必要對其部門設置和人力資源配置上，給予充分條件和保障，才可配合當前及未來工作需要。

最後，除公共部門外，私營企業亦多有使用人面識別的認證功能，相關企業部份透過於一戶通的人面識別系統連動進行身份認證，部份則

可能自行開發；一方面再次突出相關公共平台系統安全的重要性，另一方面亦有需要對系統的開發和使用作出適當規範。政府宜與本澳企業共同磋商和研究，針對有關系統的安全性，訂定具約束力的規範和監管指引，並協助其對數據管理的安全和影響進行評估，以及設置處理和應急預案，以整體提升和合理規範本澳在數據保護方面的軟、硬實力。

為此，本人提出以下質詢：

1. 請問當局現時一戶通等具人面識別系統的政務平台，是否有足夠能力預防和應對AI深偽技術帶來的防偽挑戰?在加强政務平台對於深度偽造檢測技術方面又有何實際行動方案?

2. 請問當局現時網絡安全事故預警及應急中心有否就AI相關犯罪設置專門的應對小組，在技術人手方面又是否足夠？如否，當局又有何完善計劃？

3.請問當局會否針對目前本澳私人市場上採用人面識別的系統（如銀行、電子支付等平台），與業界合作訂定具體和具約束力安全指引及規範，又有否計劃協助相關企業對數據保護的安全性和影響進行評估，以提升整體安全性？另外，目前企業與一戶通在人面識別上的掛鉤，有否存在風險識別及避險機制？

Io Fong MA
Assinatura digital
2025.08.06
11:25:12 +0800