書面質詢

黃潔貞議員

關於人工智能技術犯罪的監管

近日香港高校一名男學生涉嫌利用人工智能軟件，生成多名女性師生不雅照，事件引發社會對人工智能（AI）技術犯罪的關注。伴隨人工智能技術的快速發展，在推動社會創新發展的同時，亦衍生新型犯罪形態。今年4月下旬警方接報本澳首宗涉及AI深偽技術（Deepfake）的詐騙案件，雖然及時遏制有關犯罪並未造成市民損失，但可見此類犯罪手法極具隱蔽性與危害性。

縱觀全球及周邊地區案例，人工智能技術犯罪主要以技術濫用主導犯罪類型，通過偽冒名人、親友聲音及影像實施勒索或誘導轉賬，以及非法獲取他人生物特征數據，例如人臉、聲紋等，用於合成不雅內容或虛假信息，侵犯個人信息與名譽等方式，對社會治安造成影響。例如香港2024年錄得3宗AI深偽技術騙案，涉及款項就超過3.6億元。

由於人工智能技術使用門檻低、開源工具普及等，讓不法分子更容易掌握及運用有關手法進行犯罪行為。參考中國內地做法，今年3月相關單位印發了《人工智慧生成合成內容標識辦法》的通知，通過標識提醒用戶識別虛假信息，明確相關服務主體的標識責任義務，規範內容製作、傳播各環節標識行為，實現從生成到傳播的全鏈條治理。香港政府數字辦公室則在四月公布《香港生成式人工智能技術及應用指引》，為技術開發者、服務提供者及使用者，提供應用生成人工智能技術的實務操作指引。當前本澳面對人工智能技術犯罪儘管可使用《網絡安全法》、《打擊電腦犯罪法》、《個人資料保護法》等法律條文，但仍缺乏專門針對人工智能技術訓練、生成內容標識、刑事歸責等方面的專門立法及指引，難以應對人工智能技術更新迭代快速及其“黑箱特性”。

對此，本人提出以下質詢：

1. 現時本澳尚未有針對人工智能技術的專門立法，參考國內發布《人工

智能生成合成內容標識辦法》及香港發布《香港生成式人工智能技術及應用指引》的做法，相關部門會否從人工智能技術訓練、生成內容標識、刑事歸責等方面出發，研究相關的立法工作？

2. 保安司司長曾在口頭質詢大會時表示，保安部門在澳門招聘網絡安全人才存在困難，當局曾聘請4位來自內地的人員，但因薪金低、辛苦而工作時期不長。為此，請開當局在培養本地及引進外地“善偵查、專技術、懂法律”的網絡安全人才，以應對人工智能犯罪方面有何規劃？

3. 因應人工智能犯罪在不同地區的出現，有必要強化區域聯防機制。當局在粵港澳大灣區城市加強合作，研究構建人工智能犯罪數據庫，實現詐騙手法、犯罪手法等信息共享，推動跨域警務協作上有何工作部署？

Kit Cheng WONG
Assinatura digital
2025.07.18
14:56:12 +0800