



香港AI素養與治理研討會 2026 — 智引未來 治理有方

AI治理： 攜手構建具韌性的發展體系

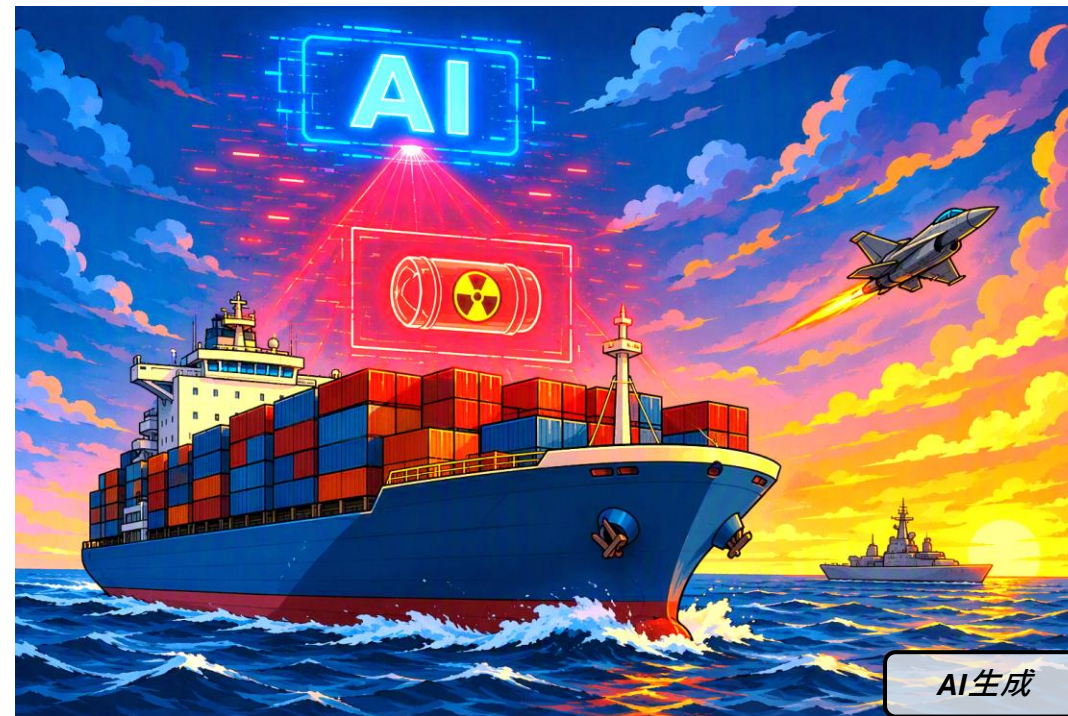
鍾麗玲女士
個人資料私隱專員

守護私隱 · 改革創新

Protecting Privacy · Embracing Innovation

2026年9月30日

AI安全治理與發展相輔相成



統籌發展和安全

國家「十五五」規劃

堅持統籌發展和安全

全面實施
「人工智能+」行動

加強AI治理

《香港第一個五年規劃》

以AI技術賦能千行百業

優化AI及數據治理

建立有利AI發展的
規範框架

《2026年施政報告》

加大推動各行各業應用AI

持續在鼓勵創新與
保障安全之間取得平衡

建立AI韌性需各方配合

私隱專員公署的「3C」策略

Ensuring
Compliance

促進合規

Communication

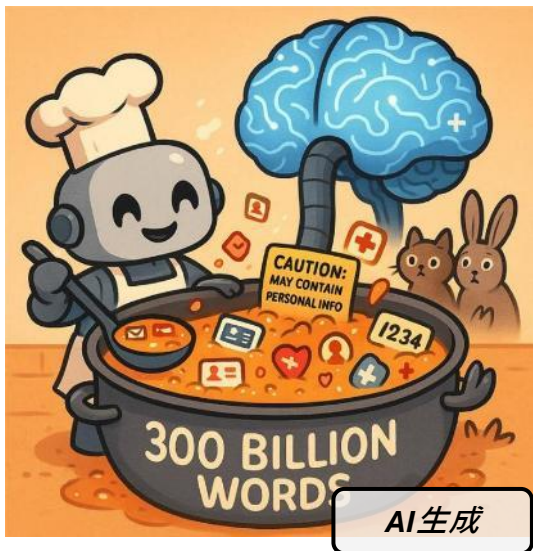
持續溝通推廣
提升業界意識

Collaboration

加強跨界、
跨地域協作

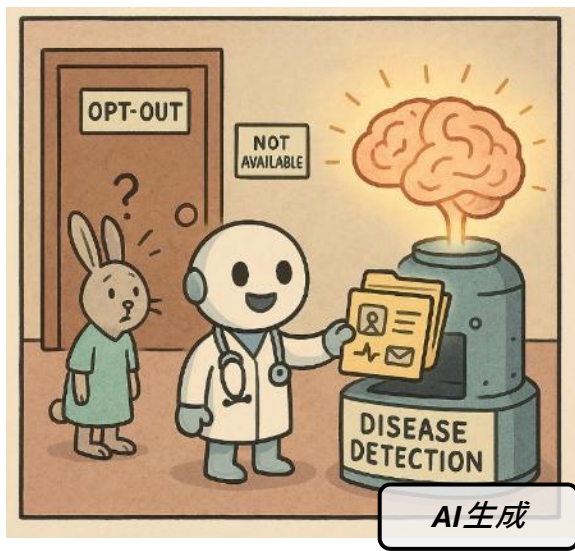
4

AI帶來的風險



資料收集過量

AI傾向於收集和保留盡可能多的數據，包括個人資料



資料的使用

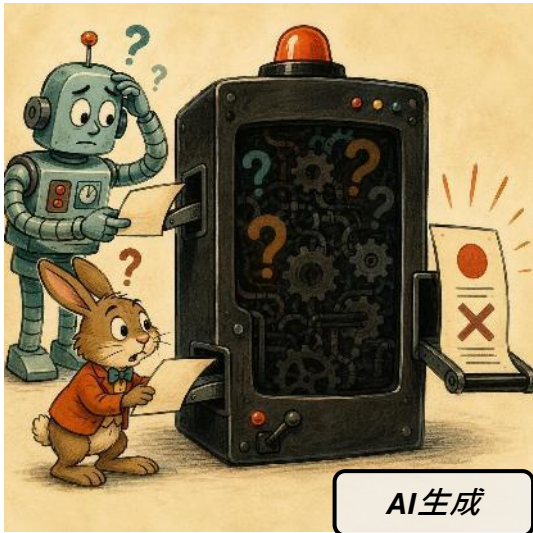
AI系統開發者在資料當事人不知情或未得到其同意的情況下，將其個人資料用於訓練AI



資料準確性

即使AI系統中儲存了過時或不準確的個人資料，開發者亦未必能夠更正或刪除這些資料

AI帶來的風險



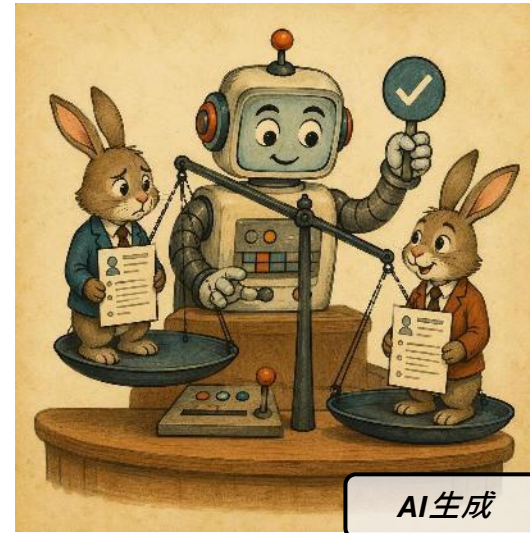
黑盒 (Black-box)

使用者未必能夠得知AI系統的內部運作邏輯，包括其數據處理及決策過程



幻覺 (Hallucination)

大型語言模型可能生成似是而非的內容



偏見

若訓練數據的質素及準確性欠佳，可能產生偏頗及帶有歧視的輸出結果

AI風險實例

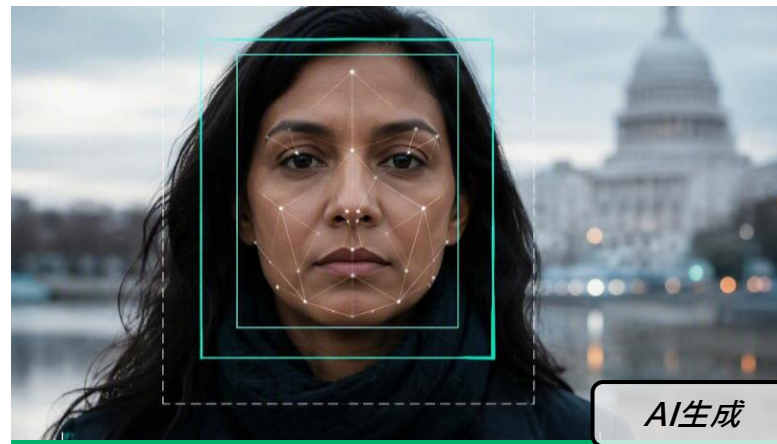


01 招聘

歷史數據導致性別偏見

亞馬遜曾開發AI招聘工具，但由於過往獲聘者大多為男性，系統因而傾向認為男性求職者較優秀，對女性求職者產生偏見

來源：[CNBC](#), [ABC News](#)



02 人臉識別

AI點錯相

AI人臉識別技術誤將一名女子識別為銀行盜竊案疑犯，導致她被拘留六個月，然而證據顯示她案發時與案發地點相距千里

發布AI指引

機構



2021年8月



2024年6月



2025年3月



2026年8月

公眾

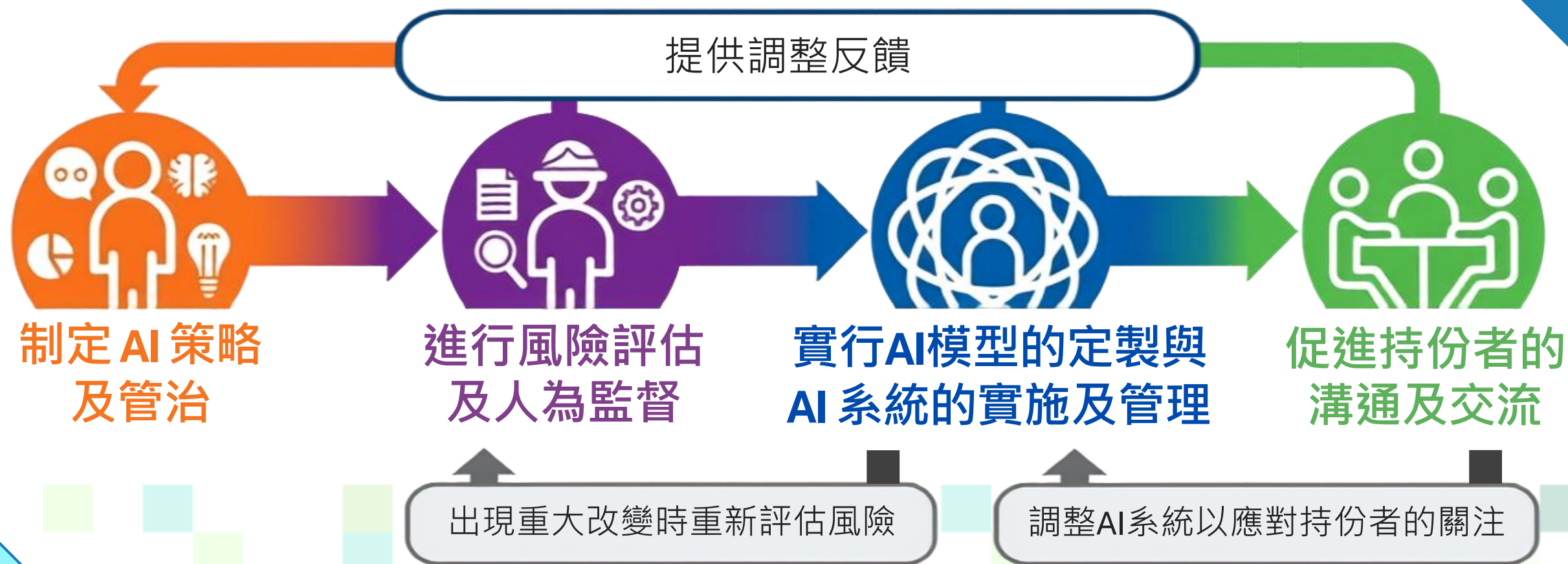


2023年9月



2025年12月

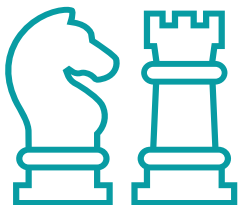
《人工智能 (AI): 個人資料保障模範框架》



9

制定 AI 策略及管治

1



AI 策略

3



採購AI方案的
管治考慮

2



管治架構

4



培訓及
加強認識

AI採購過程

1. 尋找AI方案

2. 選擇合適的AI方案

3. 收集及準備數據

4. 為特定目的定製AI模型

5. 測試、評估和驗證AI模型

6. 測試和審核系統和組件的安全性和私隱風險

7. 將AI方案納入機構的系統中

10

《僱員使用生成式AI的指引清單》



目的

協助機構制定僱員在工作時使用生成式AI的內部政策或指引，以及遵從《私隱條例》有關處理個人資料的相關規定

特色

以清單形式呈現

機構可以制定與其價值觀及使命一致的內部政策或指引

五個部分

01

範圍

02

保障個人資料私隱

03

合法及合乎道德的使用及預防偏見

04

數據安全

05

違反政策或指引的後果

《代理式人工智能篇：保障個人資料私隱》

協助機構了解使用代理式AI涉及的個人資料私隱風險

就如何負責任地使用代理式AI以及確保符合《私隱條例》的規定提出**九項建議**



01 避免過度或任意收集個人資料供代理式AI使用

02 就代理式AI處理個人資料保持透明度

03 確保代理式AI處理的個人資料的準確性

04 訂定適當的保留時限

05 確保未經同意不會將個人資料用於新目的

06 維護代理式AI系統中個人資料的安全

07 確保查閱及改正資料的權利

08 持續進行風險評估

09 分配明確責任及提供培訓

12

使用AI聊天機械人「自保」貼士

1



不要與AI聊天機械人分享自己及他人的個人資料

2



如有需要，提交改正或移除資料要求

3



對網絡安全威脅提高警覺

4



與AI聊天機械人對話時，不要分享機密資料和檔案

5



謹慎使用AI聊天機械人提供的資料

6



刪除聊天紀錄中不需要保留的對話

13

守護私隱·改革創新
Protecting Privacy · Embracing Innovation



聯絡我們



人工智能私隱保障熱線: 2110 1155



人工智能私隱保障專題網頁:
https://www.pcpd.org.hk/tc_chi/artificial_intelligence/index.html



Email: communications@pcpd.org.hk



地址: 香港皇后大道東248號大新金融中心13樓1303室

追蹤我們



私隱公署PCPD



香港个人资料私隐专员公署



Office of the Privacy Commissioner for
Personal Data, Hong Kong

