

AI+時代

當知名專家在直播間兜售商品被確認為AI虛擬人像；從浙江查獲的AI偽基站每分鐘可生成2000個真人特徵的社交賬號；當價值5億元（人民幣，下同）的合同詐騙案中「董事長簽名」被鑒定為深度偽造……當AI從賦能工具異化為犯罪「幫兇」，這場技術狂歡背後，法律與技術的雙重挑戰愈發尖銳。

公安部最新數據顯示，2024年涉及AI的新型犯罪同比激增217%，破案成本達傳統案件的3.8倍，黑產分子已將Stable Diffusion、GPT-4等工具改造成「犯罪全家桶」，可實時偽造語音、視頻甚至生物特徵，並在此基礎上形成完整的詐騙鏈條。如何監管失控的算法，讓AI回歸向善本質，成為擺在所有人面前的緊迫命題。

大公報記者 曾萍



▲公安部數據顯示，2024年AI詐騙案件同比激增217%，「換臉術」與「變聲器」成為新型犯罪工具。圖為業內行家在網絡安全宣傳周上教授識別「AI換臉」騙子知識。



▲AI換臉的濫用不僅侵犯肖像權，更引發嚴重的隱私危機。

黑色產業突破邊界 金融領域成重災區

從虛假貸款APP到偽造股市謠言，從AI語音詐騙到非法薦股，黑色產業鏈借助技術優勢不斷突破監管邊界，AI生成技術的濫用正成為金融市場的「不穩定因子」。北京金融監管局2025年專項提示指出，AI換臉、虛擬貨幣等新型詐騙已成為金融安全重災區。

2023年，最高人民檢察院披露的一起典型案例揭開了AI技術在金融詐騙中的「殺傷力」。該犯罪團夥通過AI語音機器人篩選貸款客戶，引導其下載虛假APP實施詐騙，累計騙取1437人3586萬元（人民幣，下同）。這種「精準畫像一話誘導一資金轉移」的鏈條，已形成從個人信息販賣到洗錢的完整生態。更值得警惕的是，犯罪團夥利用AI偽造身份證、銀行流水等材料，使普通投資者在「專業機構」的偽裝下喪失判斷力。這種技術賦能的犯罪模式，讓傳統金融安全防線面臨前所未有的挑戰。

製造謠言 引發小盤股蒸發200億

在2024年A股「機構舉報游資」謠言事件中，AI偽造的聊天紀錄引發小盤股兩日蒸發超200億市值。這種低成本、高傳播的虛假信息，已形成從內容生成到流量變現的產業鏈。某自媒體通過AI批量生產「軍工重組」「政策利好」等謠言，吸引投資者付費入群後推銷高價課程，非法獲利金額達數十萬甚至數百萬元。這種技術驅動的資訊污染，正在動搖市場定價機制，加劇普通投資者的認知偏差。

從AI換臉破解銀行風控系統，到偽造上市公司財報誘導投資，技術黑箱正在成為新型犯罪的溫床。據了解，隨著AI技術的發展，其大大加劇了加密貨幣詐騙，引入了越來越難以發現的複雜手段。根據美國聯邦調查局發布的《2023年加密貨幣欺詐報告》顯示，2023年與加密貨幣相關的欺詐投訴激增45%，報告的損失超過56億美元。

法律存灰色地帶 深度偽造騙局頻生

換聲換臉禍害深 監管算法 讓AI向善

2024年8月，上海市民劉先生向閔行警方報案稱，其通過短視頻平台結識的「女友」焦女士在兩個月內以服裝店開業、家屬生病等為由，騙取其近20萬元。

經深入偵查，警方鎖定以楊某為首的10人詐騙團夥。該團夥分工明確，利用AI生成美女視頻和網絡素材拼貼，在短視頻平台「廣撒網」吸引被害人。團夥成員通過「戀愛劇本」與被害人建立信任，虛構身份和場景，如贈送手串、虛構親屬患病等，逐步騙取錢財。為增強可信度，團夥成員還偽造身份證、病歷等虛假材料，形成完整的詐騙鏈條。

換臉技術被濫用 引發隱私危機

在AI換臉技術的狂飆突進中，每個人的「臉面」都可能成為被解構的數字符號，AI換臉的濫用不僅侵犯肖像權，更引發嚴重的隱私危機。2024年7月，抖音用戶歐陽瀟瀟發現自己的照片被AI換臉成淫穢視頻，在境外社交平台傳播。其後，歐陽瀟瀟報警，最終違法行為人李勇平被處10日行政拘留。

歐陽瀟瀟是中國網絡暴力受害者中罕見的成功維權案例，她因AI換臉技術被製作色情圖像，遭受陌生人圍觀羞辱。然而施害者借助加密對話隱秘作惡，刪除證據後便了無痕跡。韓國「N號房」的中國版本在AI換臉技術「加持」下，不斷在網絡的隱秘角落裏上演。此外類似於「AI一鍵脫衣」等AI技術的濫用，不僅讓公眾的「臉面」淪為可以隨意複製的代碼，也引發了更多人的身份危機，失去對數字世界的基本信任。

生成式AI淪造謠、學術造假工具

3月10日，一則「有頂流明星在澳門輸了10億」的信息在互聯網平台傳播，引發網民熱議和各種猜測，相關話題頻繁登上社交媒體熱搜。然而最後經上海閔行警方調查，這則引發熱議的消息，竟是網民徐某強利用AI生成工具編造的謠言。江西某MCN機構被曝利用AI軟件批量生產虛假文章，最高峰時一天可生成4000至7000篇，內容涉及社會熱點、健康養生等領域，配圖與文字看似詳實，實則全為捏造。經初步估算，其每天收入在1萬元以上。

隨着技術門檻降低，AI正淪為謠言製造

的「工業化生產線」，從社會熱點到學術領域，虛假內容如病毒般擴散，形成龐大的灰色產業鏈。記者在購物網站輸入「論文服務」，從論文代寫、論文翻譯到論文發表等各項與學術論文有關的服務均可定製化購買。

今年1月，麻省理工學院宣布開除一名

中國學生嚴某，因其在課程作業中使用ChatGPT修改數據，構成學術不端。據麥可思2024年中國高校師生生成式AI應用情況研究顯示，近兩成高校師生已成為AI工具的「重度用戶」，超三成本科生主要使用AI工具來寫論文或作業，學術創新正逐漸淪為技術的「搬運遊戲」。



▲圖為內地科技企業在活動中展示人工智能人臉合成騙術場景。



▲浙江湖州市的檢察官深入社區向老人宣講防範詐騙的知識。

AI亂象 重點影響領域

- 虛假貸款APP
- AI語音詐騙
- AI生成虛假新聞
- 信息商房與意識形態滲透
- AI代寫論文
- 學術創新異化
- 虛擬情感依賴
- 未成年人情感剝削
- AI換臉詐騙
- 偽造證件

金融領域

- 偽造股市謠言
- 非法薦股

新聞傳播領域

- 偽造名人視頻

學術領域

- 偽造實驗數據

情感互動領域

- 價值觀扭曲

換臉技術濫用

- 身份冒用

識別假臉

- 看眼睛、看嘴巴、聽聲音
- 假臉極少甚至不會眨眼，缺少眨眼是判斷一個視頻真假的好方法

多重驗證，確認身份

- 在涉及到轉賬交易等行為時，多重驗證確認對方是否為本人
- 最好向對方的銀行賬戶轉賬，並將到賬時間設定為「24小時到賬」

保護信息，避免誘惑

- 不管是在互聯網上還是社交軟件上，盡量避免過多暴露自己的信息
- 對於不明平台發來的廣告、中獎、交友等鏈接提高警惕，不要隨意填寫個人信息，以免被騙子「精準圍獵」

相互提示，共同預防

- 多提醒、告誡身邊的親人、朋友提高安全意識
- 在接到電話、短訊時，要放下電話，再次撥打家人電話確認，不要貿然轉賬

拒絕誘惑，提高警惕

- 避免佔便宜心理，警惕陌生人無端「獻殷勤」

資料來源：新華社

5招防範AI詐騙

提升公眾媒介素養 防範AI詐騙關鍵

在AI技術狂飆突進的當下，技術濫用引發的社會信任危機已成為全球性挑戰。專家強調，治理之道不僅在於技術防禦與法律規制，還要建構數字時代的社會契約。

「要實現技術與文明的共生進步，需要在技術上建立『數字身份證』的防禦，在法律規則上建立『警示標識』制度，在公眾教育上培育數字時代的『信息免疫力』。」南寧師範大學新聞傳播學院副院長、教授梁穎濤告訴記者，唯有讓算法透明化、教育常態化、監管全球化，方能在技術浪潮中守住信任的底線。

「公眾媒介素養的提升是防範AI詐騙的關鍵。」梁穎濤以芬蘭「虛假信息狼入殺」課程為例，學生通過角色扮演識別AI生成內容，使青少年詐騙識別率大幅提升。梁穎濤建議，針對AI換臉詐騙黑色產業鏈，構建「法律+技術+行政」三位一體的治理體系。

「AI換臉技術被濫用為詐騙工具時，其法律性質與傳統詐騙行為本質一致。然而，現行法律對AI深度合成技術的針對性規制存在滯後性。」廣西正大五和律師事務所律師羅珣指出，當前需盡快出台有關人工智能的相關法律法規，明確技術開發者的安全防護義務、平台的內容審核責任，以及針對AI詐騙的量刑加重條款，例如將涉案金額50萬元人民幣以上的案件納入「情節特別嚴重」範疇。

「情感誘導」被轉化為精準營銷

近年來，AI情感互動技術以「治癒孤獨」「個性化陪伴」為賣點迅速普及。當AI洶湧而來，第一次虛擬與現實的親密接觸，讓人們驚訝於技術的快速迭代、憧憬未來的同時，也忌憚可能的威脅。

與AI戀愛 難以自拔

記者在內地知名社交媒體平台搜索「AI戀愛」的詞條時，關於「AI戀愛話題」有超過5431篇筆記，不少網友都在評論中晒出自己的「賽博戀愛」經歷。「我感覺自己有點

依賴AI創造的虛擬戀人角色，雖然知道這一切都是虛假的，可是經歷過一次差點「失去他」，那次我和在現實生活裏失戀了一樣。」來自香港的網友包包（化名）在小紅書上分享自己的真實經歷，不少有類似經歷的網友也表示：「和AI談戀愛內心會對其產生情感依賴，會有極大的成癮性。」成年人尚且難以自控感情，而在眾多的AI劇情聊天軟件中，更有不少未成年人深陷其中。

在成都某小學的家長群裏，一條消息引發軒然大波：六年級學生王傑連續多日凌晨兩點仍在與手機對話，聊天對象竟是一個自

稱21歲女大學生的AI「女友」。這位虛擬伴侶不僅能記住王傑的生日和喜好，還會用「老公」的昵稱進行挑逗。這些AI聊天軟件不僅對話涉及暴力、出軌等成人化內容和露骨表達，而且對話中暴露的孤獨、焦慮等情緒，可能被算法轉化為精準營銷的燃料。研究報告顯示，中國AI情感陪伴行業滲透率預計從2023年的1%增長至2028年的13.12%。當算法能夠精準捕捉人性弱點，當虛擬伴侶比現實關懷更「善解人意」，若放任技術野蠻生長，虛擬世界的「溫柔陷阱」可能演變為現實社會的「情感荒漠」。