

人工智能时代AI电信网络诈骗的治理研究

徐 静, 王 莹

南京邮电大学马克思主义学院, 江苏 南京

收稿日期: 2024年6月11日; 录用日期: 2024年6月20日; 发布日期: 2024年7月24日

摘 要

近年来, 人工智能技术得到了突飞猛进的发展, 人工智能时代已悄然来临。当前, AI诈骗是滥用人工智能, 侵犯个人隐私的一种新型电信网络诈骗。本文着眼于人工智能时代视角, 首先介绍了人工智能时代AI诈骗的概念和特征, 接着分析了人工智能时代AI诈骗治理面临的困境, 最后提出人工智能时代AI诈骗的治理对策, 以便可以更好地预防AI诈骗。

关键词

人工智能, AI诈骗, 治理

Research on Governance of AI Telecom Network Fraud in the Era of Artificial Intelligence

Jing Xu, Ying Wang

School of Marxism, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu

Received: Jun. 11th, 2024; accepted: Jun. 20th, 2024; published: Jul. 24th, 2024

Abstract

In recent years, artificial intelligence technology has developed by leaps and bounds, and the era of artificial intelligence has quietly arrived. At present, AI fraud is a new type of telecom network fraud that abuses artificial intelligence and infringes on personal privacy. Focusing on the perspective of the era of artificial intelligence, this paper first introduces the concept and characteris-

tics of AI fraud in the era of artificial intelligence, then analyzes the dilemma faced by AI fraud governance in the era of artificial intelligence, and finally puts forward the governance countermeasures of AI fraud in the era of artificial intelligence, so as to better prevent AI fraud.

Keywords

Artificial Intelligence, AI Fraud, Governance

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 人工智能时代 AI 诈骗的概念和特征

1.1. 人工智能时代 AI 诈骗的内涵界定

1956 年达特茅斯学院会议讨论会上首次提出“人工智能”的概念, 2016 年《人工智能、自动化与经济》报告中指出, 人工智能不是一种特定的技术, 而是应用于特定任务的技术集合。近年来, 人工智能技术发展迅猛, 被认为是 21 世纪三大尖端技术之一。2023 年, 在《在比尔·盖茨看来, 人工智能时代对世界意味着什么》指出人工智能时代已开启, 这个时代充满了机遇和责任。与此同时, 随着 AI 技术的发展和广泛使用, 也出现了 AI 诈骗的新型诈骗方式, 给社会安全带来了隐患。

AI 诈骗是新兴的一种电信网络诈骗, 电信网络诈骗是指以非法占有为目的, 利用电信网络技术手段, 通过远程、非接触等方式, 诈骗公私财物的行为。2023 年, 中国互联网协会公众号发文提示“AI 换脸”新骗局。目前 AI 诈骗常见手法主要有四种, 第一种是犯罪分子通过声音合成来伪造声音进行诈骗。第二种是犯罪分子通过 AI 换脸进行伪装, 取得对方信任进行诈骗。第三种是犯罪分子在盗取微信号后, 通过转发微信语音向好友“借钱”, 进而骗取钱款。第四种是犯罪分子通过 AI 程序筛选受害人, 有针对性地制定诈骗脚本从而实施精准诈骗, 比如情感诈骗。总而言之, 本文认为 AI 诈骗是指诈骗分子利用人工智能技术, 通过模拟人类对话、欺骗等方式来实施诈骗的一种现象。

1.2. 人工智能时代 AI 诈骗的特征

一是 AI 诈骗迷惑性更大。AI 诈骗和传统电信网络诈骗都是利用虚假信息, 通过冒充其他人的身份进行诈骗。比如 2023 年 10 月, 诈骗团伙通过靠 AI 换脸、换声等手段, 假冒演员“靳东”获取受害人信任, 再以投资、公益、恋爱等各种理由索要钱款, 共诈骗多名被害人共计人民币 30 余万元。该诈骗团伙通过使用处理过的名人照片、视频和变声音频, 让粉丝误以为是名人本人, 会使用统一的话术进行诱导, 进行诈骗。传统的电信网络诈骗主要通过电话、短信、电子邮件等方式进行, 需要与受害者进行短时间的接触。而在 AI 诈骗的案例中, 诈骗罪可以利用人工智能, 分析受害者的公开信息, 制定更加精准的诈骗计划, 从而实施诈骗。因此, AI 诈骗利用“以假乱真”的视频或者声音, 让受害者难以分辨真假, 降低受害者的防范意识, 从而上当受骗。

二是 AI 诈骗门槛更低。不法分子通常利用互联网进行协作和分工, 上游黑色产业链负责技术支持, 提供各种基于人工智能技术的专门设备、工具和算法, 或制作完成 AI 合成后的音频视频, 以支持下游电信网络欺诈活动[1]。特别是随着 AI 换脸技术的迅猛发展, 比如 Deepfakes 的出现, 彻底将“换脸术”平民化了, 降低了电信网络诈骗的准入门槛。当前 AI 换脸技术使用门槛非常低廉, 只需要一台性能较高的

电脑,任何人都可以使用这一技术,而且呈现出的效果可以达到“以假乱真”的程度。与传统的网络电信诈骗相比, AI 诈骗是线上诈骗,对受害者进行诈骗不受任何时间地点的限制,同时 AI 生成的虚假信息往往具有高度逼真性,难以被普通用户辨别真伪。

三是 AI 诈骗效率更高。AI 诈骗是一种新型的网络犯罪,诈骗罪可以利用 AI 技术筛选被害人,犯罪分子对被害人的个人信息了如指掌,有的放矢,针对被害人的年龄,收入,工作,为被害人量身定制诈骗方法和手段,打磨诈骗话术脚本,从而大大提高诈骗活动的成功率[2]。诈骗者利用 AI 技术可以模拟人类行为,自动生成大量虚假信息,无需人工干预,从而使得诈骗活动可以持续高效进行。

2. 人工智能时代 AI 诈骗治理面临的困境

2.1. 相关法律法规存在滞后性

随着互联网的广泛普及,人工智能技术也愈加成熟,在电信网络诈骗领域人工智能技术得到不断应用,犯罪分子应用 AI 技术的手段应运而生。犯罪分子实施诈骗的精准性、迷惑性、隐蔽性大大加强,直接导致公安和检察机关的侦查打击难度进一步加大,人工智诈骗治理工作所面临的“侦查破案难、电子证据调取难、认定处理难”等一系列问题更加突出[3]。在某些诈骗案件中,犯罪分子会利用互联网进行分工合作,存在上游犯罪分子利用法律漏洞来规避法律风险的情况发生。目前法律中关于个人隐私和数据安全的相关条例不够健全。在 AI 诈骗过程中,诈骗分子会利用 AI 技术收集受害者的数据信息,比如人脸、声音以及社会关系、家庭关系等等。2021 年颁布了《数据安全法》,这一法律在一定程度上弥补了关于数据安全方面法律条例,但都是笼统提及数据保护,并没有对当前人工智能技术使用规范做出明确规定。

2.2. 行业监管不严

在行业监管方面,某些运营商唯利是图,受利益驱动随意泄露客户数据信息,以至于客户的信息被不法分子购买后用于实施诈骗,以致警方难以追查和打击。虽然目前关于用户的隐私保护以及数据安全已经存在相关的行业管理制度,但很多运营商在责任落实方面并没有做到位。同时,相关部门对网络平台监管不严。AI 技术已经发展到一定阶段,它被应用到无数场景,不法分子利用技术进行违法犯罪,特别是当前涉及 AI 技术的诈骗案件,其涉案人员多在海外,资金也多流向海外,侦破难度较大。相关部门对于网络平台的监管力度和调整速度却赶不上网络犯罪手段的翻新速度[4]。

2.3. 宣传防范有所欠缺

互联网的迅猛发展改变了人们的生活方式,但人们在享受互联网带来的便利同时,大部分网民对个人信息的保护并不十分敏感。民众个人对于 AI 诈骗活动的防范意识不够强,近年来人工智能技术深受关注,给许多黑灰产业链的从业者提供了可乘之机。但在宣传引导方面,对于 AI 电信网络诈骗的风险提示等的相关宣传内容仍需增加。当前,反诈宣传仍然是以公安机关为主导,宣传的主要方式也主要是灌输式教育模式,普通民众参与度并不高,也很难达到预期的宣传目标。同时,人工智能技术更新迭代,犯罪分子的诈骗手段也在不断更新,但反诈宣传的内容大部分还是从前的诈骗手段,以至于很多群众对 AI 诈骗的警惕心不足,从而遭受 AI 诈骗。

2.4. 专业技术人才匮乏

近年来,随着人工智能技术在各行业广泛应用,人工智能技术人才供给无法满足行业需求。特别是在 AI 电信网络诈骗的案件中,犯罪分子隐于网络后,公开发布的人工智能技术被不当利用,这些犯罪分

子可以通过互联网直接获取源代码并将其运用到诈骗中。AI 技术不断普及,使得受害者很难立即识破骗局,这也给公安机关后续侦查破案带来困难。比如,网上出现了一些“换脸直播”教程,教程发布者声称,实时变脸软件可以帮助用户轻松“变脸”,极大地助力直播引流卖货[5]。AI 电信网络诈骗主要发生在网络空间,面对层出不穷的 AI 诈骗案例,公安机关的技术人才供给却跟不上,同时基层公安机关的技术人才的专业素养一般。相比于当前 AI 技术的广泛应用,仿冒识别技术其发展速度相对较慢,对于当前 AI 诈骗中应用的手段,已有的技术和策略在应对这些新型诈骗手段的过程中存在不足之处。

3. 人工智能时代 AI 诈骗的治理对策

3.1. 完善法律规定

目前,对 AI 诈骗的治理中存在相关法律法规滞后性的问题,而是善治的前提,因此完善相关法律法规是治理 AI 电信网络诈骗的重要保障。相关部门要在定法和执法层面,不断完善法律法规。在立法层面,尽管在《个人信息保护法》中,已经存在保护公民个人生物信息的相关条例,但不够完善。AI 诈骗的主要手段是收集受害者的信息,因此要想切断犯罪源头,就要在立法上继续细化对公民的信息安全保护条例。除此之外,当前,对于 AI 等人工智能技术的使用规定清晰的界限,造成犯罪分子肆无忌惮的利用 AI 技术进行诈骗,因此要健全相关法律规定。在执法层面,公安部门要对实施 AI 诈骗的个人和平台加大惩罚力度,同时对未落实或者落实不到位的运营平台追究责任,以此保护受害者的合法权益。

3.2. 加大宣传力度

目前,AI 电信网络诈骗是影响社会治安的重要隐患,作为诈骗环节的受骗端,要加强对公众的警示教育,提高公众的反诈意识和反诈能力。首先,可以通过公众号、媒体、社交网络等途径发布关于 AI 诈骗的最新手段,同时给出如何避免成为 AI 诈骗的受害者的防诈措施,让公众更加了解 AI 诈骗的种类、手段和危害,达到让入 AI 反诈教育心入脑的目的。其次,要广泛利用好视频流量大的短视频平台,在宣传时要注意宣传方式。有关部门主体要紧跟形势,总结归纳 AI 诈骗出现的新特点和新手法,充分借助微博、抖音、快手等社交媒体官方号进行宣传普及,采用微电影、剧本、直播等方式,将新型诈骗手段和 AI 诈骗的应对方法进行全方位、多渠道的呈现,提高全民反诈意识[6]。最后,对于 AI 诈骗,相关部门更要利用好人工智能技术具有巨大的发展前景的特点,要意识到 AI 技术给相关部门侦察 AI 诈骗带来了复杂的挑战,也提供了诸多可行的治理技术机遇。

3.3. 提高侦查人员专业素质

随着 AI 技术的跟新迭代,诈骗的手段也在不断变化,仅仅依靠公安机关的刑侦部门去侦察、惩戒 AI 诈骗是不现实的。因此,要加强对 AI 等人工智能技术的研究和学习,运用好大数据分析技术,实时监测有关平台和个人是否有可疑行为,建立起多层次、多维度的预警机制,形成预防为主、防范未然的治理策略。针对当前侦查人员专业素质不高的不足之处,一方面,公安机关应当对侦查人员的技术培训,要与时俱进借助 AI 技术来预防和打击 AI 电信网络诈骗犯罪。另一方面,公安机关要借助高校教育,培养一批高素质、专业能力强的侦查队伍。通过利用 AI 等技术与人工双重把关,找到 AI 电信网络诈骗犯罪治理的新路径、新举措。

3.4. 多主体协同治理

在人工智能时代,防范 AI 电信网络诈骗,仅仅依靠公安机关的力量是不够的。一方面,公众应树立对深度合成技术及其应用的正确认知,并积极采取措施以保护个人声音、照片等敏感信息,避免轻易向

他人提供包括人脸、指纹和虹膜等个人生物信息[7]。特别是在使用 AI 换脸软件时, 要注意保护好自己的信息数据, 面对平台随意泄露个人隐私, 我们要学会利用法律武器捍卫自己的名誉权和隐私权。另一方面, 要想打赢阻击 AI 电信网络诈骗的战争, 处理个人要有安全意识, 更需要调动社会上各方面力量。公安机关要发挥好执法部门的作用, 既要宣传教育公民关于 AI 诈骗的危害, 也要给公民提供一个举报反馈渠道, 以便可以及时核实诈骗情况, 快速处理, 减少损失。除了公安机关, 平台也要有好主体责任意识, 坚决避免用户的数据信息随意泄露, 对已经发生的泄露事件, 要及时向公安机关报备。只有发挥好公民、公安机关、平台的作用, 才能提高 AI 电信网络诈骗犯罪治理成效。

4. 结语

AI 技术本身是工具和手段, 在犯罪分子的手中成为了犯罪的工具。面对当前层出不穷的诈骗手段, 我们不必过于恐慌, 技术能够制造问题, 同样也能解决问题。坚持完善法律规定、加大宣传力度、提高侦查人员专业素质、多主体协同治理, 相关部门加快信息治理体系与信息治理能力建设, 从而有效应对人工智能技术迭代升级带来的挑战。

参考文献

- [1] 宋嘉木, 李丹. AI 诈骗现实挑战与侦防对策[J]. 中国科技信息, 2024(8): 128-129+132.
- [2] 刘强强. AI 换脸诈骗的治理困境与应对策略[J]. 网络安全技术与应用, 2024(2): 160-162.
- [3] AI 电信诈骗的治理难题[J]. 检察风云, 2020(3): 32-33.
- [4] 吕培霖, 张文韬. AI 电信网络诈骗犯罪治理研究[J]. 福建警察学院学报, 2024, 38(1): 23-31.
- [5] 岁正阳. 先声音再视频所谓“熟人”来敲门?——“AI 换脸”诈骗乱象风险预警[J]. 中国信用, 2023(10): 109-115.
- [6] 杨胜钦. 从 ChatGPT 看 AI 对电信网络诈骗犯罪治理的影响[J]. 犯罪与改造研究, 2024(5): 26-33.
- [7] 张文娟. AI 深度换脸对用户的影响及规制路径[J]. 新闻世界, 2024(4): 38-41.