“AI换脸”居然有一条龙服务

专家:治理技术滥用应引入多方力量

“AI换脸”技术被滥用的新闻近日登上热搜。除了被应用于电信诈骗，“AI换脸”还常被用于影视剧二次创作、趣味恶搞小视频，甚至淫秽色情影像的合成中，而在网络上有商家提供各类“换脸服务”。律师指出，从娱乐“玩梗”到违法犯罪，藏在“面具”背后的用户若对该技术不当使用，会承担多项法律责任。

随着AI技术的迅速发展，“AI换脸”正进入越来越多的生活场景中。记者在网络上搜索发现，AI换脸软件的获取非常容易，有商家提供各类“换脸服务”。律师表示，若对该技术使用不当，可能会涉嫌行政违法、民事侵权甚至刑事犯罪。

资料图片

“朋友”视频借钱骗走430万元

朋友打来视频电话借钱，你还会怀疑对方身份的真实性吗？据媒体报道，今年4月，福州市郭先生的好友突然通过视频电话联系他，想通过郭先生公司账户走账430万元。由于通过视频聊天已“确认”了朋友身份，郭先生便放心转账。事后，郭先生通过和好友沟通才得知自己被骗，原来对方竟通过AI换脸和拟声技术，佯装好友对其实施了诈骗。

事实上，除了被应用于电信诈骗外，“AI换脸”还常被用于影视剧的二次创作、趣味恶搞小视频，甚至淫秽色情影像的合成生产中。比如，多名演员就遭遇过“AI换脸”，被人制作私人视频并对外传播。某网红博主也曾发文称，有人盗用她的“脸”制作了色情视频。

AI换脸容易操作吗？在某手机应用商城，记者以“换脸”作为关键词搜索到多款“AI换脸”的App，在其他网络平台上，用户也能搜索到部分“AI换脸”的小程序。

记者下载了某款App使用，其中有多款“换脸”模板可以选择，包括型男、古风视频、美女视频等。如果想“解锁”更多模版，则需要额外付费。以记者试用的这款App为例，其月会员29元、季会员59元，终身会员98元。根据提示，用户充值后只需一键上传照片，便可在15秒内生成对应模版的“换脸”视频。

网上各类“换脸服务”涌出

记者通过调查发现，除了直接提供“AI换脸”服务，还有不少卖家会提供“换脸”技术教程。

记者在网上联系到一名卖家，他向记者展示了一段利用AI换脸软件实现主播换脸的样本视频。视频中主播的人脸已被替换成一位金发碧眼的外国女性，而且表情自然，几乎看不出破绽。

“只需要提供一段人脸视频，3到5天就可以训练出一套高清定制模型，以后直播可以随便用。如果需要明星换脸的素材，我们这里都有，在软件使用上我们包教包会。”这名卖家说，这样一套模型收费3500元。

卖家还提醒记者，如果要进行直播换脸，最好配备配置较高的电脑系统，“这样我们完全可以做到防遮挡，观众基本分不出来真假，‘换脸’会更加灵动。”他说。而当记者询问能否直接帮忙做“换脸”视频时，对方则显得很谨慎，“现在查得严，用途不当的不做，其他的时长半小时内收费1500元。”

“正是由于相关技术门槛的降低，才使得如今‘AI换脸’技术被滥用。”对于如今涌出的各类“换脸”服务，北方工业大学信息学院副教授张远说。

张远分析认为，“一方面，随着AI技术代码的开源，很多人可以直接拿到成熟模型的源代码，有编程基础的人在此基础上稍加修改，便可以制作成一款AI换脸软件。另一方面，由于算力的进步，软件实时换脸能力相较于之前也大幅提升，这就令AI换脸更容易实施。”

治理技术滥用应引入多方力量

“这种换脸视频是否涉嫌侵权?”在换脸相关短视频的评论区里，有不少人提出这样的疑问。

对此，北京市京都律师事务所律师张雁峰指出，从娱乐“玩梗”到违法犯罪，藏在“面具”背后的用户若对该技术不当使用，会涉嫌行政违法、民事侵权甚至刑事犯罪，面临多项法律风险。

“从行政违法的角度来说，虽然现行法律没有明确‘AI换脸’必然会受到行政处罚，但如果使用场景涉及到寻衅滋事、捏造诽谤、不正当竞争等，则可能因此而受到警告、罚款、拘留等行政处罚；从民事侵权的角度来说，未经他人允许便擅自使用AI换脸技术可能侵犯如肖像权、隐私权、名誉权和知识产权等一系列权利。”张雁峰说。

对此，互联网分析师张孝容则认为，伴随着AI大模型的发展，声音合成、人脸交换越发逼真，AI换脸技术的不当应用，不仅涉及法律问题，还可能造成新型社会危害。

“因此，AI作品制作需要强制实施主动识别原则，令软件生成的所有作品加上AI水印。”张孝荣说，“另外，传播平台也需提供相应的说明字样。”

张远还提出，网络服务平台作为大数据采集端，可以提高识别能力，主动通过技术方法分析、研判、定位存在有法律风险的合成视频，严控问题视频的传播，完善事前处理机制。

人工智能使用边界在哪儿

对于滥用生成式人工智能技术的担忧在世界范围内都存在。不仅因为其超越一般技术的“创造能力”和“破坏性”，更因为人们发现，生成式人工智能技术发展的速度极快。目前，世界各国对其风险的预判与防范均处于探索阶段，有赖于法律体系的进一步完善。

警惕滥用人工智能技术

模仿一个人的声音乃至外貌，对AI来说并不是新鲜事。此前，“AI孙燕姿”就曾在B站等网络平台走红，视频上传者通过使用AI音色替换技术，生成了高度还原孙燕姿音色的翻唱歌曲。近期也有媒体报道了一款网络上的付费AI换脸软件，其套餐价格从499元到2888元不等，肉眼来看，换脸之后的“数字人”口型、表情、微小的动作几乎毫无破绽。

生成式人工智能的大量出现很大程度上得益于深度合成和机器学习的快速发展。而AI诈骗者正是通过这些先进的技术，训练出能够模拟人类语言和神态的AI。

苏州大学竞争政策与反垄断研究中心研究员方翔指出，近期的AI诈骗案件主要是人工智能技术在图像领域的应用，这种模式可以将不同人脸图像中的面部特征相互进行替换。“拟声”则是借助深度学习模型，根据已有的语音样本(如通话录音、网络视频等)生成与其近似的声音，进而做到与人交谈。

前段时间，中国互联网协会发文提醒，伴随着深度合成技术的开放开源，深度合成产品和服务逐渐增多，利用“AI换脸”“AI换声”等虚假音视频，进行诈骗、诽谤的违法行为屡见不鲜。面对利用AI技术的新型骗局，广大公众需提高警惕，加强防范。业内人士普遍认为，“AI换脸”技术的滥用给人们敲响了警钟，其复杂性、隐蔽性也给科技识别及运用提出了更高的要求。

“对于生成式人工智能，正当适度使用，可以倍增工作效率，有力推动创意产业发展，促进消费者福祉增长。但同时，虚假使用可引发谣言泛滥、侵害权利、压榨利益，而过度使用可引发践踏人性、减少就业、贫富悬殊，而恶意滥用甚至成为歪曲真相、撕裂社会、政策干扰、祸乱宇内的罪恶之源。”中国互联网协会法工委副秘书长胡钢认为，要坚持依法崇德治理，使全社会形成法网大于互联网、国法高于算法、人工智能不能成为“人工制人”的共识。

探索构建人工智能法律体系

“我国针对人工智能及数据安全、个人信息保护的立法虽然起步较晚，但日臻成熟。”方翔指出，2017年7月，国务院印发《新一代人工智能发展规划》，其作为我国AI发展的纲领性文件，提出了面向2030年我国新一代人工智能发展的指导思想、战略目标、重点任务和保障措施，其中特别提到“到2025年初步建立人工智能法律法规、伦理规范和政策体系，形成人工智能安全评估和管控能力”。

2022年12月，国家网信办、工信部、公安部联合发布《互联网信息服务深度合成管理规定》，强调不得利用深度合成服务从事法律、行政法规禁止的活动，要求深度合成服务提供者对使用其服务生成或编辑的信息内容，应当添加不影响使用的标识。提供智能对话、合成人声、人脸生成、沉浸式拟真场景等生成或者显著改变信息内容功能服务的，可能导致公众混淆或者误认的，应当进行显著标识。

2023年4月，国家网信办起草《生成式人工智能服务管理办法(征求意见稿)》并向社会公开征求意见，提出AI内容必须真实准确，禁止非法获取、披露、利用个人信息和隐私、商业秘密。

“总的来看，构建完善的人工智能法律体系，我国目前仍在探索阶段。”方翔说。

中国信息通信研究院云计算与大数据研究所所长何宝宏则指出，2022年12月发布的《互联网信息服务深度合成管理规定》明确针对在中国境内应用深度合成技术提供的互联网信息服务进行规制，其中，深度合成技术是指利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术。“在上述法律法规的具体落实过程中，存在两方面的挑战。”

“防范深度合成技术应用生成错误价值导向、虚假信息的能力需要进一步提升。《互联网信息服务深度合成管理规定》要求深度合成服务提供者对输入数据和合成结果进行审核、建立健全识别违法和不良信息的特征库、依法处置违法和不良信息的生成合成信息内容。但是，对于深度合成服务提供者如何落实内容管理需要进一步细化，提供者需要不断提升技管结合的能力；对于内容管理落实的具体效果，也有待进行持续性的跟踪检验。”何宝宏指出，对深度合成信息内容增加标识的具体规范也需要进一步细化，文件中明确深度合成服务提供者提供深度合成服务，可能导致公众混淆或者误认的，应当在生成或者编辑的信息内容的合理位置、区域进行显著标识。“但对于如何增加显著标识以及增加标识的具体方式需要尽快出台细化的要求规范。”

(来源：工人日报、中国青年报)