

明星带货、熟人借钱？小心是 AI 换脸

通过人工智能（AI）手段为视频中的人物“换脸”，这种技术已经从编辑录制好的视频，发展到可以实时动态修改直播画面。最近，网上还出现一些“换脸直播”的教程，声称通过相关软件换上一张明星艺人的脸，用于直播带货等场景，能取得更好的效果。但法律专家提醒，这种做法可能涉嫌侵犯艺人的肖像权和名誉权，用于商业行为还可能涉嫌虚假宣传等。

而 AI 技术更被不法分子盯上，用于行骗……

“AI 换脸明星直播带货”教程热传

某主播：“AI 变脸直播，实时变脸软件分享。今天老张给大家带来一款‘神级’的 AI 工具，可以让你轻松实现实时变脸，打造特效直播间，无论是引流卖货还是卖专门的技术都是非常强大的。”

这样的“换脸直播”工具，最近在网上通过视频、文章等形式传播，并提供下载渠道。有的需要付费，有的声称点赞、关注、评论就能获取。

这些“模型”用中外明星艺人、影视角色、政商名人的名字命名。在另一个展示“换脸直播”效果的视频中，使用者把“成龙”的模型载入相关软件，摄像头前的人在直播画面中就有了与影星成龙相似的五官，但脸型、发型还保持原样。使用者歪头、变换表情，换上的五官动效自然顺滑，只在手掌从脸前划过时，出现了比较明显的破绽。

北京岳成律师事务所高级合伙人岳岫山律师表示，这样的换脸直播用于公开传播，可能涉嫌侵犯相关明星艺人的肖像权，如果涉及直播带货等商业行为，会成为加重情节。

建议平台主动识别相关内容

记者注意到，一些使用换脸技术的直播并不会直接提到相关明星艺人的名字，但也不会主动声明或者否认。

岳岫山律师表示：“如果用明星的脸去带货，然后还没有声明，这其实是涉嫌欺诈行为，或者说是虚假宣传行为，让公众误以为这就是明星在带货。如果说货品本身不好，或者带货中说的一些话或是一些行为导致公众对明星产生一些负面评价的时候，还可以主张名誉权的侵权责任。这种肖像侵权，是属于肖像权人向司法机关去主张民事责任。但是如果涉嫌到了虚假宣传，涉及了不正当竞争行为的话，市场监督管理部门是要给予行政处罚的。”

从事艺人宣传工作的袁女士认为，针对相关行为搜集证据和维权的成本比较高。而只要冒用了明星艺人的面部特征，不管是否提及姓名，侵权影响都类似。对于部分用户来说，即便有一行小字标识，也不一定能起到提醒作用。

“说实话是没有差别的，因为他本质上还是用这个明星的脸去做文章。如果我负责的明

岳岫山律师说：“只要是没有经过肖像权人的同意，在直播当中通过技术手段把自己的脸换成了明星的脸，这其实就是对明星的肖像的一种侵权。接下来根据不同的情况，承担的后果可能会不同。如果只是在娱乐，不涉及盈利行为，也是属于一种侵权，在赔偿的时候可能会考虑这个情节。但如果把明星的肖像用于带货直播，那么属于是一种商业行为，在赔偿数额上一定会给予一些考虑的。包括主观恶性、过错程度比较大，因此获利了，赔偿的损失数额可能就会更高一些。”

在知名艺人工作室从事宣传工作的袁女士表示，担心相关技术被用于推销假冒伪劣产品，损害消费者权益，也影响艺人的形象。

袁女士表示：“我经常刷一些平台都会看到。还是有一定的欺骗性的，如果不仔细辨别的话，就会认为是明星艺人本人，这一点我觉得还挺可怕的，万一卖的东西拿回去了以后货不对板，或者有一些更严重的问题，消费者就会觉得‘这个东西我是看着谁谁谁的脸去买的’，或者说‘我是进了谁的直播间去买的’。”

星艺人摊上了这个事儿，其实维权成本特别大，并且效果可能没那么好。我们也不可能每天都去发律师函，发也发不过来，甚至有的时候可能要找到侵权人都很费劲。”袁女士说。

近期，已经有平台企业发布了“关于人工智能生成内容的平台规范暨行业倡议”，其中明确禁止利用生成式人工智能技术创作、发布侵权内容，包括但不限于肖像权、知识产权等。一经发现，平台将严格处罚。还提出“发布者应对人工智能生成内容进行显著标识，帮助其他用户区分虚拟与现实”“发布者需对人工智能生成内容产生的相应后果负责”，等等。

岳岫山律师建议，平台还可以更主动地识别相关内容，限制侵权行为。

岳岫山律师建议：“平台应该对这种使用技术手段改变面部特征的，或者说进行了换脸的，应该能够监测出来，建议做标签化的处理。如果说是涉及到明星的面部特征，是不是可以给出一些限制，因为这涉嫌到一种侵权行为了，应该有义务制止。”



资料图片

“好友”视频通话 公司老板被骗 430 万元

除了部分主播为吸引眼球、博流量滥用 AI 技术，一些不法分子也盯上了 AI 技术。近日“AI 换脸”诈骗的相关话题冲上热搜，引发网友热议——骗子通过 AI 技术，在视频中“换脸”成受害者熟悉的朋友或领导，骗取钱款。

5 月初，内蒙古包头市公安局电信网络犯罪侦查局发布一起使用智能 AI 技术进行电信诈骗的案件。

4 月 20 日 11 时 40 分左右，福建福州市某科技公司法人代表郭先生的好友突然通过微信视频联系到他，两人经过短暂聊天后，好友告诉郭先生，自己的朋友在外地投标，需要 430 万元保证金，且需要公对公账户过账，所以想要借用郭先生公司的账户走一下账。

好友向郭先生要了银行卡号，声称已经把钱打到郭先生的账户上，还把银行转账底单的截图通过微信发给了郭先生。基于视频聊天信任的前提下，郭先生没有核实钱是否到账，于 11 时 49 分先后分两笔

把 430 万元给对方打了过去。

钱款转账后，郭先生给好友微信发了一条消息，称事情已经办妥。但让他没想到的是，好友回过来的消息竟然是一个问号。

郭先生拨打好友电话，对方说没有这回事，他这才意识到竟然遇上了“高端”骗局，对方通过智能 AI 换脸技术，伪装成好友对他实施了诈骗。

4 月 20 日 12 时 21 分，包头市电信网络犯罪侦查局接到福建省福州市公安局刑侦支队的外协请求，称福建省一知名民营企业负责人被骗走 430 万元，而涉案的银行卡为包头市蒙商银行对公账户，希望包头警方能够帮忙进行紧急止付。

据了解，在银行全力协助下，该诈骗账户内的 336.84 万元被骗资金已被成功拦截。同时，福州市公安局警方已接到剩余款项 93.16 万元资金流出信息。目前，福建警方与包头警方对此资金正在全力追缴当中。

仅需一张照片 骗子就能“换脸”行骗

据福建厦门市反诈中心工作人员介绍，郭先生遭遇的就是 AI 换脸骗术。骗子只需要一张照片，就能给视频中的人“换脸”。最新的 AI 技术还可以实时捕捉，让你在和别人视频通话的时候，把对方替换成任何一个人物，效果几乎到了以假乱真的程度。

同时，微信号、QQ 号被盗的情况时有发生，即使是你社交平台中现有的“好友”也存在被盗号的风险。据介绍，近期有些市民在点开“顾客”等陌生好友发来的压缩文件后，电脑中了病毒被远程操控，微信号和 QQ 号被盗，大量拉好友进诈骗群和发营销广告，有人微信因此被永久封

号。

厦门反诈中心提醒，在遇到类似的好友通过音频或视频借钱时，最好拨通对方的电话号码核实。特别是大额借款，最好当面进行确认。另外，微信好友的头像也很容易被复制。

警方同时提醒市民群众不要贪小便宜，在街头不要随意用手机扫码广告领取礼品等，容易导致信息泄露。

此外，当得知自己的微信号或 QQ 号被盗，或是有人以自己的名义进行借款诈骗时，当事人应尽快积极通过多途径提醒自己的好友，避免更多人受骗。

相关提醒>>>			
AI 技术如何介入新骗局？			
第一种是声音合成。			
骗子通过骚扰电话录音等来提取某人声音，获取素材后进行声音合成，从而可以用伪造的声音骗过对方。			
例如，某公司财务接到领导电话，要求立刻给供应商转款 2 万元，并将转账信息以邮件形式发送，转款理由是避			
免缴纳滞纳金。由于老板的口音十分逼真，该财务信以为真，在 1 小时内转款完成，后发现被骗。			
第二种是 AI 换脸。			
因为人脸效果更易取得对方信任，骗子用 AI 技术换脸，可以伪装成任何人，再通过视频方式进行信息确认。			
第三种是转发微信语音。			
除了 AI 换脸、合成语音外，还有一些诈骗手段也可谓防不胜防。前不久，有骗子通过转发微信语音的方式进行骗。			
在盗取微信号后，骗子便向其好友“借钱”，为取得对方的信任，他们会转发之前的语音，进而骗取钱款。尽管微信没有语音转发功能，但他们通过提取			
语音文件或安装非官方版本（插件），可实现语音转发。			
第四种是 AI 筛选受骗人群。			
值得一提的是，这些骗局中，骗子不是漫无目的地全面撒网，而是根据所要实施的骗术，通过 AI 技术筛选受骗人群，别有用心地锁定特定对象。例如，当进行金融诈骗时，经常搜集投资信息的用户就会成为他们潜在的目标。			