与朋友聊天视频秒变向父母要钱?

滥用AI换脸技术乱象调查

调查动机

知名医生张文宏带货蛋白棒?不久前,某视频博主发布的视频中,张文宏医生强烈推销一款蛋白棒,让不少网友信以为真,一时销量近1200件。

张文宏随后回应称,视频是AI合成的,"我在发现这事后立即投诉过那个AI合成的视频,但是它的账号一直在换,自己最后也没精力了。这些假的AI合成信息就像蝗灾一样,一次又一次发生,像漫天飞过来的蝗虫一样害人"。

目前,该涉事视频已从发布账号中移除,且该账号已被平台永久封禁。

AI换脸技术的应用边界何在?如何打击和治理网络中滥用AI换脸技术的不法行为?对此,记者进行了调查采访。

"爸妈,我现在在医院,着急用钱,麻烦再给我转两万吧……"视频中,女生神态焦急地倾诉着最近遇到的难事,向父母要钱,语气恳切,看上去几乎毫无破绽。

随后,该视频发布者发布了原视频,视频中,女生只是在和掌镜的朋友正常交流对话,所说的内容和神态与上一条视频中的完全不一样。

原来,女生向父母要钱的视频是利用AI合成技术生成的视频。

随着AI技术发展,AI换脸图片和视频成为热门现象,娱乐之余,让人真假莫辨,风险与困扰也不少。

记者近日调查发现,互联网上,不仅有人随意兜售AI合成软件,"手把手教学",使得制作生成AI"克隆人"视频的技术成了一门生意。还有人利用知名人士视频和声音AI合成新的视频,发在短视频平台上用来卖货。更有甚者,滥用AI换脸技术走上了违法犯罪的道路。

AI合成技术亟待加强监管。多位受访专家建议,完善立法,明确定义深度合成技术的应用范围和法律边界,细化平台、技术提供商、内容制作者及用户的法律责任。同时,构建多元主体协同治理的体系架构,全方位、全环节整治和打击涉AI犯罪活动和网络黑灰产业链。

"克隆人"成了生意 影音清晰真假难辨

在上述利用AI合成技术生成的视频介绍中,作者打出了"AI克隆人""AI数字人"等标签。据作者介绍,只需提供一段有清晰人脸和声音的视频,就可以在短时间内生成一个和原视频相似的新视频,说话的内容可以自行编辑文本。

生成的视频中人物形态之自然,语言之流畅,让评论区一些网友直呼"恐怖""真假难辨"。

记者查看视频评论区发现,该视频作者打起了"暗号"——在一些感慨技术逼真的网友评论下方留言"+薇4聊……教学,懂得来"(汉字与数字交替出现,用来代替聊天账号,暗示添加好友私聊)。

记者按照提示,添加其好友询问相关视频及制作方法。昵称"AI小米××"立刻回复道:"想自用还是直接代理赚钱?"

据其介绍,如果是自用,可以充值199元成为"AI幻影××"(某AI"克隆人"生成平台)的2年会员,可以立即生成AI合成视频共计38分钟,不限使用次数。而交纳499元则可以成为代理,号称"享受60%的首次分佣,躺赚20%的复购充值分佣,享受80%的招代理分佣"。

几天后,当记者再次试图打开上述视频时,显示"视频因违规无法播放",违规原因"疑似为高风险的项目/引流行为"。

"视频里在海边游玩的不是我,而是我的数字人分身。你跟着我操作,就能定制自己的数字人,轻松实现视频流量起号……"在社交平台、短视频平台上,类似以AI数字人、"克隆人"视频引流的帖子有很多。

记者就制作AI数字人的流程咨询一博主。该博主在之前发帖中明确表明"不收费""不用花钱",但提出要加入群聊成为会员,他会在群内发布相关操作指南和课程。

此外,在多个网购平台、二手交易平台,AI"克隆人"商品也可以随意买到。记者在某网购平台检索"AI换脸",显示搜索结果不存在,但更换关键词为"AI换人脸视频软件"后,立刻出现多款此类商品,价格从几元到上百元不等。

记者点进一款名为"AI数字人生成软件短视频制作对口型形象声音克隆定制AI分身"的商品,咨询店主后对方回复称:"使用软件时,您可以上传30秒以上的自己形象视频,然后输入文字,我们××数字人系统就可以给您生成对应口型和克隆您声音的视频了,2分钟左右就可以生成好。您下单后客服会一对一服务到您学会使用为止。"

随即,对方发来一个标价为98元的下单链接,称这是购买该软件的月卡,可以制作约30秒以内的视频32个,"短视频养号一个月足以快速起号"。

瞄准AI不法"商机" 利用技术违法犯罪

除了直接售卖AI换脸技术外,还有人瞄准了AI"克隆人"的不法"商机"。

据办案民警介绍,一些不法分子利用AI技术,将他人的脸换成熟人或亲人的脸,冒充诈骗对象的重要关系人,通过合成视频或照片来"以假乱真",扰乱被诈骗对象的视线进而实施诈骗。

滥用AI换脸技术行不法之实的事件屡有发生。

对此,北京航空航天大学法学院副教授赵精武分析说,利用AI换脸技术进行带货等行为,如果仿冒他人,除了构成民法上对肖像权等人格权的侵害之外,根据情节轻重,还可能构成刑法上的虚假宣传、网络诈骗等犯罪行为。"而随意售卖AI合成软件的行为,倘若存在主动为犯罪行为人提供相关软件服务等情形,则可能与犯罪行为人构成共同犯罪。"赵精武说。

"如果通过AI换脸技术编造险情、灾情等,还有可能构成编造、故意传播虚假信息罪。"北京盈科(上海)律师事务所数智化建设委员会副主任李悦举例说,前一阵子的"西藏小男孩被埋图",虽然使用的AIGC技术不是深度合成AI换脸,但也是使用AI技术。据了解,该行为人已被追究行政责任。如果其情节更严重的话,或构成编造、故意传播虚假信息罪。

李悦强调,首先必须明确,技术本身是中立的。AI换脸作为深度合成技术的一种具体应用,虽然存在被滥用的风险,但其本身并无"原罪"。目前,一些平台上的个人"售卖技术"行为,教他人使用开源项目或某些应用,本质上是在利用信息差。然而,如果课程内容专门教授如何突破深度合成应用的内容审核机制,则应当被否定。平台可以通过限流、警告、冻结账号等方式对这些视频内容进行规制。

"虽然AI技术在不断进步,但目前而言,仔细看的话还是能识别AI合成的视频。"李悦说,AI合成视频往往在面部细节上存在较为显著缺陷:微表情缺失(如眼角细纹、嘴角抽动难以捕捉)、光影不匹配(轮廓和阴影过渡不符合光线反射规律)以及皮肤过于光滑(缺乏毛孔、纹理和瑕疵)。在眼神与表情方面,眼球运动机械化(转动不连贯、眨眼频率异常),面部表情僵硬(转换生硬、笑容缺乏真实感)。"在运动过程中也会出现明显的问题,比如脸部变形等。观看手部动作也是一个比较快速识别的技巧,曾经很长一段时间,AI在处理人手的时候会出现非常多的问题,比如关节畸形等。"李悦说。

"据我观察,AI生成的语音通常更加流畅,语速更快,且较少出现'额''嗯''也就是说'等语气词或停顿。"李悦说,虽然声音克隆技术近年来取得了显著进步,几乎能够达到以假乱真的程度。但如果仔细辨别,仍然可以识别出AI生成的声音。毕竟截至目前,尚无任何一款AI能够通过图灵测试。

完善立法强化执法

AI合成技术的广泛应用,需要法治的护航。

李悦介绍说,我国于2023年颁布《互联网信息服务深度合成管理规定》,针对该技术的规范管理迈出了重要一步。在人工智能整体领域,我国也持续推出了一系列相关规定,包括目前正在研讨的人工智能法。

李悦建议,立法方面,需明确定义深度合成技术的应用范围和法律边界,细化平台、技术提供商、内容制作者及用户的法律责任。同时,加大对利用AI技术实施犯罪行为的刑事处罚力度,并完善针对AI合成视频的证据规则,明确其法律效力。

"技术方面,推广AI合成视频的检测工具和溯源技术,研发高效、低成本的检测服务,并向公众开放。利用水印技术对AI生成内容进行标识,便于追踪和识别。"李悦说,此外,可以建立AI企业备案制度,加强对企业资质、数据安全和算法透明度的监管。

李悦提出,进一步强化平台责任,要求平台对用户发布的内容进行审核,及时处理违法信息。

来源:新华网