宇宙境杯 · 🅰

2024年3月12日 星期二 广告

责编/朱忠诚 胡晓新 审读/刘云祥 美编/雷林燕

"秒变"小丑!



"AI 换 脸 " 火 了! 最近,中国香 港警方破获一起诈 骗案一 -某公司职 员在参加一场"多 人视频会议"后被 骗走2亿港元。在 这场会议中,只有 受害者是"真人", 其他"参会同事"都 是诈骗分子用"AI 换脸"冒充的。网 友们纷纷感慨:"这 下,眼见也不一定 为实了"。

"AI换脸"的门 槛高不高,涉及哪 些"黑科技"?它可 能会导致哪些法律 风险,受害者又该 如何维权?除了 "换脸", AI 还有哪 些妙用? 3月11 日,记者来到宁波 头部IT企业-研软件股份有限公 司(以下简称国研 软件),探秘"AI换 脸"背后的技术原 理。

记者"秒变"小丑

"AI 换脸"有多神奇? 国研软件行 业应用研发部高级工程师孙一帆向记者 演示这项应用。只见摄像头"捕捉"记者 的面部神态后,把记者的脸"秒变"为小 丑的脸。由记者"换脸"而成的小丑,还 会跟随记者的表情"开口大笑"。它也能 把记者"换脸"成孙一帆本人,出现两位 "孙一帆"同框的画面。

"这款'AI换脸'应用来自Github 代码开源平台,通过深度学习算法,精准 识别视频中的人脸图像,并提取出眼睛、 鼻子、嘴巴等关键特征,再将其与素材库 里的图像进行匹配、替换、融合。只需上 传你的一张照片,就能快速换脸,但效果 不够逼真。要想提升效果,至少需输入 4000-6000张照片。"孙一帆介绍。

这样看来,通过"AI换脸"进行视频 会议诈骗,要么是"吃准"了视频会议的 参与者无需频繁变换表情,只需一张照 片"换脸"就能"糊弄"过去;要么就是骗 子已"潜伏"多日,收集大量当事人同事 的面部照片,以做到以假乱真。可见,保 护个人信息安全迫在眉睫。

那么,我们该如何分辨"AI换脸"和 真人? 网传的"捏鼻子"等方法靠谱吗?

孙一帆告诉记者,这种做法可以参 考,但并不绝对奏效。"目前的AI算法, 都是基于完整的面部照片,'捏鼻子'意 味着面部有遮挡,如果AI训练时遮挡的 数据不够,就可能'露马脚'。但如果训 练的数据充分,或采用更健全的算法,也 可能破解这一痛点。这种情况下,最好 询问对方彼此都知道的问题,以确认身 份。"孙一帆说。

至于网友们关心的"是否会被'AI 换脸'拿来做刷脸支付?"孙一帆认为,目 前还无需担心,因为现有的"刷脸支付" "刷脸门禁",并不支持"AI换脸"所需的 虚拟摄像头采集功能。但保护人脸数据 等个人信息安全,仍需技术开发方、APP 运营方、监管方等相关机构建立更严格 的标准和规范。

记者体验"AI换脸"秒变"小丑"。 记者 苗雪未 通讯员

"AI换脸"有哪些法律风险?

如今,"AI换脸"的应用层出不穷, 有人用它"复活"已去世的亲人,以寄托 思念;有人将它用于电商直播,以"提升 主播颜值";更有人拿明星照片"换脸"剪 辑视频……然而,企业或个人在使用 "AI换脸"时,稍有不慎就可能在违法的

浙江素豪律师事务所律师孙央指 出,"AI换脸"可能涉及的法律风险有以 下几种-

一是,著作权侵权风险。企业可能 在已有的视频或图片中,将人脸进行替 换。而其使用的视频或图片等素材,他 人可能享有著作权,如果未经著作权人 同意擅自使用这些素材,将侵犯著作权。

二是,肖像权侵权风险。《民法典》第 1019条规定,未经肖像权人同意,不得 制作、使用、公开肖像权人的肖像。如果 没有经过他人同意,将他人的人脸用来 制作短视频或其他作品,可能会侵犯肖 像权,

此前,杭州物联网法院曾审理过一 起因"AI换脸"APP利用深度合成算法 侵犯他人肖像权的案件。原告楼某某是 一位古风汉服模特,发现被告运营的 "AI换脸"APP,使用了其拍摄的古风造 型视频模板,供其他用户"换脸"生成新 视频。最后,法院判决被告向楼某某赔 礼道歉,并赔偿损失5000元。

三是,名誉权侵权风险。《民法典》第 1024条规定,民事主体享有名誉权,任何 组织或者个人不得以侮辱、诽谤等方式 侵害他人的名誉权。如果在AI换脸视频 中,将他人人脸替换的行为构成对他人 名誉的贬损,可能构成对名誉权的侵犯。

同时,针对人脸信息被"盗用"至 "AI换脸"应用等问题,《中华人民共和 国个人信息保护法》为侵害人脸识别信 息的行为,规定了罚款、吊销营业执照、 损害赔偿等行政、民事乃至刑事责任,以 增强对违规使用人脸识别技术、侵害人 脸识别信息的行为的威慑力。

如果发现"AI换脸"侵犯了自己的 权益,该如何维权?

孙央律师建议,受害人首先要保留 证据,通过截图、证据保全等方式保存侵 权视频或图片;如果是在某个平台上发 现被侵权,可以向平台运营者投诉,要求 删除侵权视频或图片;最后,可以向人民 法院提起诉讼,维护自己的合法权益。

如何让AI"为我所用"?

技术的进步绝非"洪水猛 兽"。要想让AI作为一种生产力 工具,既需要完善的监管体系,也 有赖于千行百业的从业者,加强 合理使用AI的能力。

以国研软件为例,该公司 将AI技术用于农贸市场的数 字化改造,研发出能自动"识 别"蔬果的智慧溯源秤,从而追 溯每一件菜品的"前世今生", 助力宁波保障"菜篮子"安全。 为提升工作效率,该公司IT技术 人员还用上了一款"小研机器 人",既能辅助写代码,又能方便 新员工快速入职。

"我们的'小研机器人'对接 阿里的'通义千问'大语言模型, 能运用 Python、Java 等多种语 言帮忙生成代码,解放IT人士的 生产力;我们还将企业的规章制 度导入系统,如出差流程、报销 流程等,方便大家一键查询,省去 人力沟通成本。"国研软件政务应 用研发部高级工程师毛校军告诉

在宁波,"AI+行业"的案例 层出不穷。比如,浙江九为健康 联合华为打造九为盘古中医药 大模型,借AI提升中医药研发 效率;宁波薄言信息打造"垂直 行业版 ChatGPT",为得力等本 土企业提供"智慧升级版 AI 电 商客服";多家外贸企业运用AI 跨语言和外商交流,增加接订单 的效率。

毛校军表示,灵活使用AI的 能力,或将成为未来人才的核心 竞争力。

记者 严瑾 通讯员 李栋



央视报道"AI换脸"应用。 视频截图

· 訓酒银行 宁波分行

全国性股份制商业银行

邳理财 到渤海 产品多 体验好

~~ ~		1417	7 1-41	12 17 32 73	
产品类型	期限(天)	业绩基准(年)	认购起点	募集时间	到期日
结构性存款2024年144号	50	1.10%-2.60%	10万元	2024/3/14-2024/3/18	2024/5/8
财收有略理财2024年31号	390	3.15%-3.95%	1元	2024/3/11–2024/3/13	2025/4/8
财收有略理财2024年14号	189	2.85%-3.35%	1元	2024/3/11–2024/3/18	2024/9/24
财收有略理财2024年22号	100	2.70%-3.30%	1元	2024/3/11–2024/3/18	2024/6/27

注:以上产品要素和交易规则均以产品说明书等法律文书为准,理财产品过往业绩不代表其未来表现,不等于理财产品实际收益。理财非存款,产品有风险,投资需谨慎。产品要素以说明书发行条款为准,大额存单其他期限及收益可详询渤海银行宁波分行或拨打客服热线95541。本资料仅 条款为准,大额存单其他期限及收益可详到别度取引了"62777年)" 作为我行宣传资料,并不构成对潜在投资者的邀约行为。 **宁波分行营业部:**宁波市江北区大闸路188号

一年期大额存单,年利率2.1%,起存金额20万元,额度有限

0574-87966315 0574-83862818

慈溪支行:慈溪市新城大道北路 483号 鄞州支行:宁波市鄞州区天童北路 899号 和邦大厦C幢一楼118室