

自媒体上的火灾视频是AI合成的

人工智能技术滥用将引发更多侵权纠纷、商业欺诈等

□潘自强

近期,公安机关破获多起涉人工智能案件。6月,浙江绍兴上虞区警方发现有网民发布关于上虞工业园区发生火灾的视频。民警核查发现,视频中的建筑、森林大火场景,并非该工业园真实场景,疑似源自其他视频。经分析,民警判断该视频是利用人工智能合成技术,将网络上多段不同视频剪辑拼接而成。

随着人工智能生成内容和深度伪造技术的日益成熟,虚假音、视频的伪造效果越来越逼真,技术使用也越来越便捷。本期“专家坐堂”梳理了上海法院近两年审结的涉新技术滥用违法犯罪案件,分析此类案件呈现出的新情况、新问题,研判风险,引导技术向善。



资料图片

“换脸”软件自娱自乐 侵犯了谁的权利?

彭某长相甜美,热爱古装,与独立摄影师程某合作拍摄、创作短视频和摄影作品,入驻抖音平台后发布的古风汉服短视频作品,备受粉丝的喜爱和关注,由此二人逐渐在圈内圈外形成较高的知名度和人气度。成为网络红人的彭某,不断接到展会、商演的机会,程某的商拍、寄拍也邀约不断,彭某本人及二人的作品具有较大的商业价值。

王某看到网红流量带来的巨大福利,遂注册成立了一家信息科技公司,开发、运营一款“秀颜”手机换脸软件,将程某拍摄制作的包含彭某以及其他网红肖像的短视频作品上传为模板,供用户“换脸”使用,用户付费成为会员后仅需上传自己的头像照片,即可通过 AI 技术与视频中的网红进行面部匹配、替换,然后导出高度近似的高清无水印视频作品,或用于自娱自乐或用于恶搞他人。彭某、程某获悉后,将王某及其经营的信息科技公司告上法庭。

上海市金山区人民法院经审理后认为,任何组织或者个人不得以

丑化、污损,或者利用信息技术手段伪造等方式侵害他人的肖像权。未经肖像权人同意,不得制作、使用、公开肖像权人的肖像。彭某具有一定的网络热度,其在抖音平台发布的视频资料中的肖像权应受到法律保护,王某未经彭某授权同意,以营利为目的使用含有彭某肖像的视频,已经侵害其肖像权。程某是涉案作品著作权人,王某未经许可,通过网络擅自使用和传播程某享有著作权的作品,且未支付报酬,侵犯程某对涉案作品享有的著作权,应承担停止侵权、赔礼道歉、赔偿损失等民事责任。

该法院遂判令王某在其运营的“秀颜”软件首页显著位置,对使用彭某肖像一事赔礼道歉,连续保留七日;王某赔偿彭某经济损失5600元。判令该信息科技公司立即停止侵权,删除涉案短视频;信息科技公司在其运营的“秀颜”软件首页显著位置发表声明,向程某公开赔礼道歉,30日内不得删除或撤销;信息科技公司赔偿程某经济损失2000元。

利用图片合成技术 伪造双车事故骗保

张某与荆某共同经营一家名叫强盛的汽修店,除日常车辆维修、保养,还代为拖车、代办事故理赔等,生意红火时店里曾停满待修车辆。一次偶然的机会,张某发现其维修的大部分发生单车小事故的车主,并不会选择向保险公司理赔,而是自掏腰包支付维修费用。张某遂利用代办事故理赔的便利,将放弃理赔的车辆开到定损点定损,私吞车主的理赔款。

尝到甜头的张某便与荆某合谋,将单车小事故伪造成双车事故,向保险公司骗取更高额的理赔款。二人一拍即合,半年内,伙同员工孙某等人(另案处理),利用图像合成技术,先后20余次将他人送修的单车事故车辆伪造成系与自己所有的车辆发生双车事故,用此“移花接木”手法向中国人寿、中国平安、太平洋保险等多家保险

公司骗取保险理赔款共计16万余元。

此后,保险公司在联运调查平台上发现张某、荆某投保的车辆存在大数据异常,经稽查部门调查发现,张某、荆某等人冒用多人身份证,伪造事故现场照片、人车合影,存在骗保可能,遂向公安机关报案。

上海市宝山区人民法院经审理后认为,张某、荆某单独或伙同他人,以非法占有为目的,故意伪造事故现场、办理保险手续骗取保险金,数额较大,其行为均已构成保险诈骗罪。该法院综合考虑二人的地位、作用、认罪认罚态度、部分退赃等情节,对张某判处有期徒刑八个月,并处罚金5000元;对荆某判处有期徒刑六个月,并处罚金5000元;责令张某、荆某继续退赔违法所得。

颜值检测是假 盗取信息是真

吕某是一名在校大学生,在网上冲浪时意外发现一款免费“颜值检测”软件,该软件声称只要上传一张正面照即可通过AI自动分析你的颜值,对皮肤状态、肤色、五官等进行分析并给出一定的分数。出于好奇,吕某当即下载了该软件,并授权软件使用时可访问手机相册,很快该软件给吕某的颜值进行智能评分,吕某又将该软件分享给身边的好友使用。殊不知,颜值检测是假,盗取信息是真。原来所谓的“颜值检测”软件是李某制作的一款具有非法窃取安装者相册照片功能的手机“黑客软件”,该软件以“颜值检测”为噱头,可以更加高效、便捷地采集使用者的人脸信息以及相册里的其他个人信息,压根不具备评分功能。李某到案后,公安机关在其服务器和网盘里查获含人脸信息、自然人姓名、身份证号码、家庭住址等公民个人信息8100多万条。上

海市奉贤区人民检察院在提起公诉的同时,还提起附带民事公益诉讼。

上海市奉贤区人民法院经审理后认为,“人脸信息”属于刑法规定的公民个人信息,利用“颜值检测”黑客软件窃取使用者“人脸信息”等公民个人信息的行为,属于刑法中“窃取或者以其他方法非法获取公民个人信息”的行为,依法应予惩处;李某非法获取并向他人提供公民个人信息的侵权行为,侵害了众多公民个人信息安全,损害社会公共利益,还应承担相应的民事责任。该法院遂以侵犯公民个人信息罪判处李某有期徒刑三年,缓刑三年,并处罚金1万元;扣押在案的犯罪工具予以没收;李某在国家级新闻媒体上对其侵犯个人信息的行为公开赔礼道歉,永久删除“颜值检测”软件及相关代码,并删除服务器和网盘里的涉案照片。

(以上人名及公司名均为化名)

观察思考 >>>

人工智能技术滥用引发更多侵权纠纷

数字化智能时代已经来临,技术创新红利与技术滥用风险并存。搭上技术快车的网络违法犯罪罪将驶向何方?

一是在纠纷类型上,人工智能技术滥用将引发更多侵权纠纷、商业欺诈。在互联网上换脸恶搞存在明显的法律风险,如果没有明确的授权或同意,将他人的脸部特征用于生成换脸视频或照片,可能构成对他人肖像权、名誉权的侵犯。不少主播在电商平台换脸直播带货,不仅侵犯他人肖像权,同时还可能被认定为虚假宣传,构成欺诈。

二是在应用场景上,深度伪造技术滥用将延伸至司法干扰、虚假新闻等领域。深度伪造技术门槛越来越低,不法分子利用该技术合成电子化证据材料,将加大司法机关对证据的审查难度;不法分子利用该技术合成虚假图文及音视频信息,造谣传谣、侮辱诽谤屡见不鲜,视觉失真造成新闻失实的影响将更深远,打击网络谣言的难度也将大大增加。

三是在次生犯罪上, AI 诈骗将催生侵犯公民个人生物识别信息的黑灰产业。AI 诈骗能够得逞,除了新兴技术的支持,往往还需要足够多的公民个人

生物识别信息作为基础素材,而随着强制要求采集人脸信息的场景不断出现,人脸、声音等生物识别信息泄露的风险也不断增加,极易滋生非法采集、售卖公民生物识别信息的灰色产业。

四是在社会治理上,一定程度威胁到信息安全和社会秩序。当前,人脸识别技术被广泛应用于刷脸支付、门禁管理、快递物流、住宿登记等金融、安防、交通领域,“人工智能+深度伪造”技术的滥用很可能导致人脸识别技术失效或者被欺骗。

技术本无罪,善恶在人心。防范化解技术滥用风险,应当坚持系统思维,需要在技术、法律和社会三个层面进行综合施策。在技术层面,需要进一步研究基于深度合成技术生成内容的鉴伪技术,创造更加安全可靠的技术解决方案。在法律层面,需要加快系统性立法和行业性规范制定,尽快构建起技术开发者、网络服务提供者、用户三个层面的监管体系。在社会层面,需要通过科普教育增强公众的防范意识和能力,司法机关亦可通过典型案件的审理及宣传,树立裁判规则和正确的价值导向。(作者为上海市第一中级人民法院刑事审判庭二级法官助理)