

# 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,张文宏医生强烈推荐一款蛋白棒,让不少网友信以为真,一时销量近1200件。

张文宏随后作出回应称,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。

□ 本报记者 孙天驷

“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,女生只是在和挚友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。

《法治日报》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“+微(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××”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”。

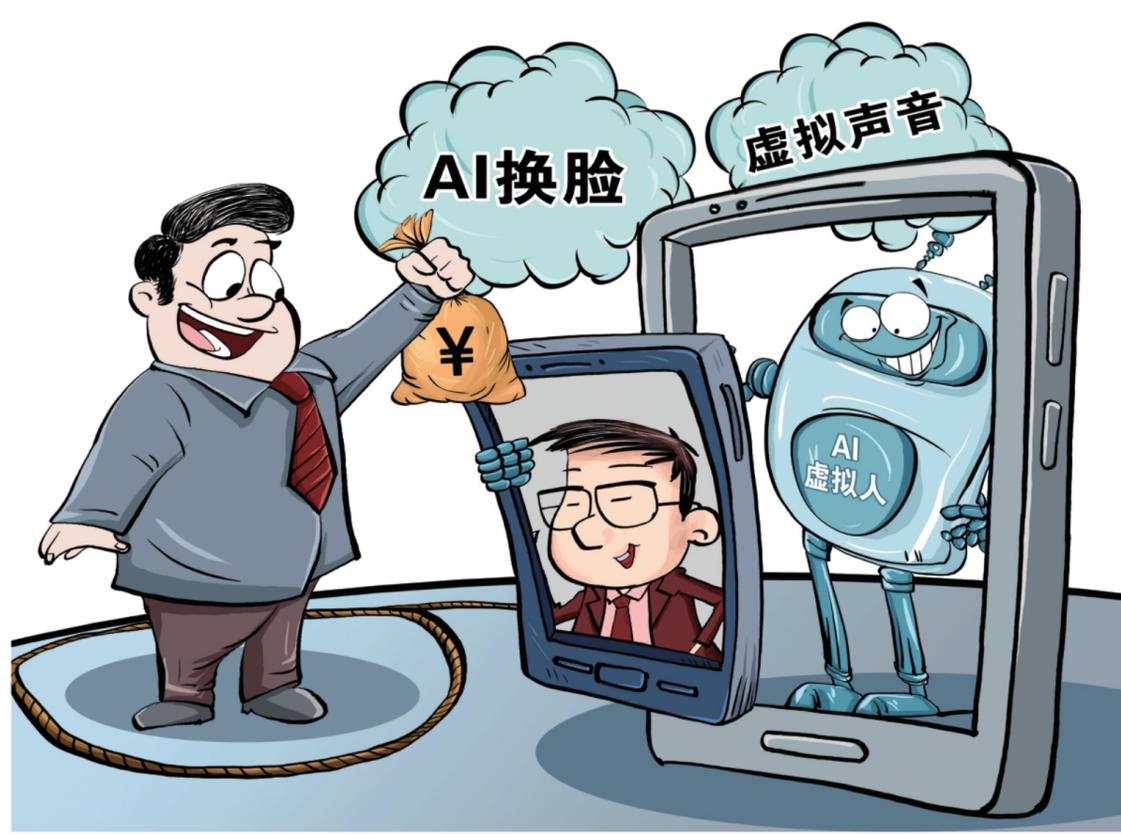
几天后,当记者再次试图打开上述视频时,显示“视频因违规无法播放”,违规原因“疑似为高风险的项目/引流行为”。

“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,记者在某网购平台搜索“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。

记者点击进入一款名为“AI数字人生成软件短视频制作”的店铺,软件测试工程师李某察觉到该店涉嫌侵权,向店主方回复称:“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”。

前不久,天津虹桥警方在一起AI诈骗案中,成功追回市民被骗的83万元。天津市民李先生此前收到了一条短信,对方自称是李先生单位的领导,要求其社交软件详聊。

加上加好友后,对方便以有急事需要资金周转为由,要求李先生向其转账,还保证事后钱款一定返还。对方还主动打来视频电话。看到视频那头出现的确实是“领导”,李先生瞬间放下戒备,分3笔向对方汇款95万元。当天下午,李先生与朋友聊天时提起这件事,越想越觉得不对劲,于是报警。

接到报警后,天津警方迅速与银行开启联动机制,及时对3张银行卡进行紧急止付操作。银行成功冻结了涉案资金83万元。

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。

据公开资料,此前,有人在社交平台用AI换脸成富商马云,视频连线获取网友信任,目标受众多为对AI缺乏认知的中老年人,之后再以“做扶贫项目”等为由骗取钱财。还有人在短视频平台上冒充演员靳东与中老年人接触,以需要钱拍戏为由诱使他人转账。

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分子提供相关软件服务等情形,则可能与犯罪分子构成共同犯罪。”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,仔细说的话还是能识别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(如眼角皱纹、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(切换生硬、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’‘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 企业备案内容标识

AI合成技术的广泛应用,需要法治的护航。

赵精武介绍,我国目前对于AI合成技术已经作出了较为充分的规定,例如《互联网信息服务深度合成管理规定》(生成式人工智能服务暂行管理办法)等,明确要求深度合成服务提供者落实信息安全主体责任,使用者不得滥用深度合成服务。

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,包括目前正在研订的人工智能法。

“当前全球范围内AI技术竞赛异常激烈,我国在这一领域仍处于‘追赶者’的位置。因此,我们应更深入地思考:究竟需要构建怎样的人工智能法律体系。

这一体系既要能够适应技术快速发展的需求,保障社会公共利益,促进人工智能产业的健康可持续发展,又要助力我国在AI竞赛中提升竞争力,实现从‘追逐者’向‘引领者’的转变,从而在全球AI发展格局中占据更有利的位置。”李悦说。

受访专家指出,目前精准打击利用AI合成技术违法犯罪行为还存在一些难点。

李悦说,技术难题主要体现在匿名性,犯罪分子使用匿名身份和虚拟货币;取证困难,需证明视频真实性、来源及目的,以及跨境性,一些犯罪工具或行为涉及境外。法律难题则包括责任链条长,涉及AI工具提供者、制作者和传播者;主观性认定困难,需证明行为人明知违法,且证据标准高。

“滥用AI技术实施犯罪行为往往与传统犯罪行为(如电信诈骗、传播网络谣言等)相结合,需要公安机关联合各大网络平台采取更为直接、有效的治理措施。”赵精武说。

为此,他建议构建多元主体协同治理的体系架构:公安机关与网信、工信等部门联动执法,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;执法部门同步更新监管技术,推动人工智能技术在刑事侦查等领域的应用,进而更高效、更精准地打击滥用AI犯罪行为;网络平台积极落实平台主体责任,积极配合执法活动,严格落实网络实名制和黑名单制度,严防各类行为人员通过更换账号登录方式躲避平台监管。

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合成视频的取证规则,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、数据安全及算法透明度的监管。

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,制定AI行业行为准则和道德规范,推动行业自律和技术应用的伦理合规性。建立跨部门执法合作机制,共同打击跨境AI犯罪,并共享AI犯罪案例和犯罪手法信息,提升全球范围内的防范和治理能力。

“AI技术的宣传教育也很重要。”李悦说,对执法人员、司法人员进行AI技术知识培训,提升其专业能力和执法效率。同时,通过媒体宣传提高公众对AI犯罪的防范意识,普及AI技术的基本知识和风险。

漫画/李晓军

# 乌市去年空气优良天数突破三百天

□ 本报记者 潘从武 □ 本报通讯员 王晨 李春蕾

近日,一场大雪如约而至,新疆维吾尔自治区乌鲁木齐市处处银装素裹。雪后天晴,市民王女士深吸一口气清冽的空气,望一眼透蓝的天空,心里无比畅快。

“以前乌鲁木齐的冬天,天几乎都是灰蒙蒙的,抓一把路边的雪,化在手中黑乎乎的。”王女士眼中的变化,是她对乌鲁木齐市大气污染防治工作最直观的感受。

对于乌鲁木齐市两级检察机关参与“乌—昌—石”区域大气污染防治公益诉讼专项监督活动的9个办案组,60余名检察官来说,点滴变化,都离不开专项监督活动的深入推进。

“乌—昌—石”区域包括乌鲁木齐市七区一县、昌吉市、阜康市、玛纳斯县、呼图壁县、沙湾市,以及新疆生产建设兵团第六师五家渠市、第八师石河子市、第十二师,是天山北坡经济带的重要组成部分。该区域大气污染防治形势严峻,煤炭消费量占新疆全区近一半,冬季空气质量频发。

新疆维吾尔自治区人民检察院于2023年3月启动“乌—昌—石”区域大气污染防治公益诉讼专项监督活动,很快发现某公司存在多个违法问题,可能损害公共利益。2023年4月,该公司被作为第一批重点监督的企业,交由乌鲁木齐专案组办理。

专案组调查发现,该公司擅自停运污染治理设施,可能污染环境;将无效数据用于在线监测设施验收,并委托环保公司出具多份检测报告,存在造假行为。

虽然该公司存在污染环境的事实,符合民事公益诉讼立案条件,但生态环境损害赔偿一般优于检察公益诉讼。2023年11月,乌鲁木齐市人民检察院将该公司污染环境的线索移送至市生态环境局,建议对该案启动生态环境损害赔偿程序。

针对其他问题,乌鲁木齐市人民检察院向多家行政单位制发磋商函,检察建议书,并将可能涉及犯罪的线索移交市公安局米东区分局。

2024年5月,乌鲁木齐市人民检察院牵头多家行政单位,就某化工公司整改情况举行听证会,对环境污染系列案件的履职情况进行综合评议。听证员充分认可本案整改成效,认为社会公共利益得到有效维护。

目前,该企业已缴纳生态环境损害赔偿费用,在相关行政单位的督促下,该公司开展自查,对存在的隐患问题全部完成整改。

“2024年,乌鲁木齐市空气质量优良天数突破300天,与各方努力分不开,我们以‘乌—昌—石’区域大气污染防治公益诉讼专项监督活动为契机,依法办理检察机关移送的生态环境损害赔偿案件,追究企业污染责任,使企业进一步树牢‘环境有价,损害担责’意识,落实环境保护责任,助力提升环境空气质量。”乌鲁木齐市生态环境局法规科工作人员李瑞莉表示。

生态环境保护非一日之功,要坚持精准治污、科学治污、依法治污。2023年5月,自治区(“乌—昌—石”区域大气污染防治2023年行动方案)中明确提出,推进清洁取暖改造和农业散煤治理,按照宜电则电、宜气则气、宜煤则煤的原则,因地制宜稳妥推进冬季清洁取暖。

在“乌—昌—石”区域大气污染防治公益诉讼专项监督活动中,专案组坚持把燃煤污染控制作为监督方向,督促推动行政机关对区域586万散煤用户完成清洁取暖改造,6087台农业上生产燃煤设施清洁能源完成改造,预计减少散煤消费约45万吨。

减少汽车排放污染物,是改善城市空气质量的一项重要举措。专案组督促行政机关对乌鲁木齐市38家机动车检测机构进行现场检查,发现问题109项,对违规情节较轻的12家检测机构采取立即整改、约谈、训诫等方式予以处理。

推进蓝天保卫战需要群策群力。专案组在专项监督活动中注重协同联动,通过与生态环境局、发改、工信、公安、住建等相关行政机关座谈,商议大气污染防治难点、痛点,促成治理共识,实现同向发力。

例如,与自治区环境保护科学研究院合作,通过对违法企业排污行为进行证据固定,由专家出具赔偿金额意见,办理生态环境损害赔偿案3件,涉及金额516.4万元。同时,聘请人大代表、政协委员、高校环保专业专家、第三方检测机构人员担任“益心为公”志愿者,在线索研判、调查取证、整改评估等方面提供专业支持,聚力解决办案难题。

专项监督活动中,专案组发现某企业存在污染防治措施未与主体工程同时建设、施工现场无任何扬尘污染防治措施,开工建设前未征求相邻社区意见,未取得污染物排放总量指标等问题。目前,在行政单位和检察机关的共同努力下,该企业对存在的环保问题全部完成整改。

2024年9月29日,在“乌—昌—石”区域大气污染防治公益诉讼现场交流会暨天山北坡城市群大气污染防治公益诉讼工作推进会上,乌鲁木齐市政协委员刘颖和其他参会代表听取了该企业环保问题整改情况,了解企业污染防治情况,并实地对企业生产车间整改效果“回头看”。人大代表、政协委员、人民监督员和“益心为公”志愿者对企业整改效果进行现场测评。

在“乌—昌—石”区域大气污染防治公益诉讼专项监督活动中,我真切感受到了涉案企业积极整改的态度和执行力,看到了检察机关充分发挥公益诉讼职能,全力推动区域大气污染防治的力度和决心!”刘颖说。

# 免“会员”阅读小程序竟是侵权“黑洞”

□ 本报记者 丁国锋 许瑞雷 □ 本报通讯员 吴玉洁

数字化时代,网络文学市场呈现出蓬勃发展的态势。由于网络文学作品具有极易被复制传播的特性,致使著作权人的利益频繁遭受侵害。近期,经江苏省太仓市人民检察院提起公诉,短篇网络文学界头部平台知乎被侵犯著作权案一审宣判,两名被告均获刑。

知乎盐选故事是指经知乎平台审核后,发布于知乎盐选专栏内的短篇小说,其阅读权限设定为只有开通知乎盐选会员的用户,才可阅读全文。

2023年2月,软件测试工程师李某察觉到该店涉嫌侵权,向店主方回复称:“使用软件时,您可以上传30秒以上

开通会员,这让“有技术”的他动起了歪心思。随后,李某着手在电脑上编写用于爬取知乎盐选故事的爬虫脚本,并成功钻研破解了知乎平台的爬虫技术措施。

2023年3月,在脚本测试成功后,李某将其上传至某云服务平台中执行,并开发了5个小程序。读者只需在小程序内输入想看的知乎盐选故事的链接,小程序就会自动调用脚本爬取网页链接中的盐选故事内容,成功后免费供读者阅读和下载。

读者若想免费阅读盐选故事,必须先看完小程序内的广告,李某便能获得相应的广告收益。

为获取更大利益,李某与兼职做小程序推荐的卢某达成合作,由卢某在网络平台上发布图文为李某引流,李某则向卢某提供2个类似的小程序供其运营,并

为其提供技术维护,同时约定抽取卢某30%的广告收益。

2023年7月,知乎发现部分小程序存在免费阅读盐选故事的情况,怀疑有人恶意爬取盐选故事非法牟利。该公司遂向公安机关报案。

2023年8月,李某、卢某先后被抓获归案。两人到案后如实供述相关犯罪事实,退出全部违法所得,并下架涉案小程序。

该案系太仓市首起网络环境下侵犯著作权案。在公安机关立案侦查后,太仓市检察院第一时间受邀提前介入,引导公安机关及时与涉案云服务平台取得联系,调取、存证相关电子数据,围绕小程序和脚本功能、涉案作品数量、涉案作品与著作权权利人作品的同一性比对等方面,全力夯实证据链条。经鉴定,涉案

作品与知乎盐选故事具有高度同一性,爬取小说共计32万余篇。

出于从快打击侵权行为的考虑,2024年5月,该案移送检察机关审查起诉后,在证据链完整、犯罪嫌疑人均认罪认罚的基础上,太仓市检察院依法建议法院适用简易程序。

此外,考虑到权利人若另行提起民事赔偿诉讼,将耗费大量时间和精力,太仓市检察院积极促成李某、卢某对知乎所遭受的损失进行赔偿。双方在太仓市检察院调解室内达成和解,知乎出具了《刑事谅解书》,并表示不再追究二人的民事责任。

近日,法院依法以侵犯著作权罪判处李某有期徒刑3年,缓刑4年,并处罚金10万元;判处卢某有期徒刑6个月,缓刑3年,并处罚金2万元。