



AI换脸技术应用边界在哪里

专家：给AI换脸视频预留“技术水印”

调查动机

浙江杭州检察机关曝光了一个“女神群”，群里发送的淫秽视频有不少是犯罪嫌疑人使用“AI换脸”技术合成的，还可以根据顾客需要“私人定制”；河北高阳警方破获了一起制作、贩卖、传播淫秽物品牟利案，犯罪嫌疑人通过社交群自学“AI换脸”技术，用明星形象制作淫秽视频在网上以每10分钟300元的价格售卖……近期，有关“AI换脸”的案件和新闻引发社会关注和担忧。

随着人工智能的发展，“AI换脸”技术门槛逐渐降低，应用场景越来越多，在满足人们猎奇、美颜、社交等需求的同时，因“AI换脸”引发的争议乃至违法犯罪行为屡见不鲜，其背后隐藏的黑灰产业链也逐渐浮出水面。

“AI换脸”存在哪些乱象？用明星形象“AI换脸”是否合法？技术应用的边界在哪里？围绕这些问题，记者进行了调查采访。



□ 本报记者 赵丽
□ 本报实习生 胡森

“能教我这个怎么拍吗？”
“视频左下角点击进入有全套教程。”
“岂不是想亲谁就亲谁？”
“学会我的教程就可以。”

这是一名短视频平台博主与粉丝的对话。这位号称特效师的博主，发布了多个影视剧热画面的短视频，并把男主角“换”成了自己，引来不少流量。面对粉丝的讨教，博主称提供“手机版影视合拍教程”，售价99.99元。

类似出售“AI换脸”技术的博主，以及提供“AI换脸”技术的App和小程序不在少数。《法治日报》记者近日调查发现，目前在网络平台上，教授“AI换脸”技术、提供视频定制“换脸”服务乃至售卖明星“换脸”的淫秽视频等已经成为一门生意。

受访专家认为，技术发展是不可阻挡的趋势，技术应用也往往超前于风险应对手段的产生。要遏制“AI换脸”等人工智能领域的深度合成技术应用乱象，还得监管部门、平台、网民多方形成合力，多管齐下。此外，针对技术研究与应用的法律法规和执行效能还需进一步完善。

相关应用下载便捷 提供肖像即可定制

在电商平台，记者以“人脸替换”“deepfake”“专业定制换脸”等作为关键词搜索看到，不少商家宣称可以提供影视“换脸”，“AI换脸”等服务，售价基本在10元至200元之间。

关于“AI换脸”的用途，电商平台上某商家这样表述：“您可以成为《倚天屠龙记》中的张无忌，也可以成为《陈情令》中的蓝忘机，抑或是成为《红楼梦》中的林黛玉……您只需录制一个短视频发给客服，这边就可以为您合成同款视频，为您的青春，增添一份风采。”此项服务，领券购买只需238元起。

在手机应用商城，记者以“AI换脸”作为关键词搜索看到，多款“AI换脸”App映入眼帘。在某社交平台上，记者搜索“换脸”，也看到了不少关于“AI换脸”的小程序。

记者下载了热度最高的一款App，该App有多款“换脸”模板可供选择，包括AI绘画、影视剧、气质美女、男士专属等，一键上传照片便可生成“换脸”视频。

如果想在这些App和小程序上使用“AI换脸”功能，则需要付费。以记者试用的这款App为例，周会员17元，年会员398元。记者购买了17元的周会员，在登记手机号码并同意遵守相关合成规定后，导入视频素材，按“点击制作”和“开始制作”键，就可以将视频素材中的人脸进行互换。

一些卖家不仅提供“AI换脸”服务，还提供“换脸”技术教学服务，进一步降低这类技术的应用门槛。

在某电商平台，记者联系了一个经营“AI换脸”业务的商家，在其“智能换脸”的商品详情页面有这样一段描述：“你可以花费最低的成本，来优化工作简历的展示……让你初出江湖就有大佬一般丰厚的资历，在就业的竞争对手中一骑绝尘。”

据该商家客服介绍，想要“换脸”，只需准备

两部分素材，即包含面部信息的人脸素材以及提供身体、背景的内容素材，商家操作后，最终“两者结合形成成品”。至于价格，商家将根据工作量和难度进行最终定价，参考价格是1分钟以内60元，超过1分钟则根据时长按秒计算，如3分钟以上每秒0.9元，10分钟以上每秒0.7元。

同时，该商家还为“有心”学习的客户提供“AI换脸”教学套餐：一份自学套餐180元，辅导套餐360元，教学套餐则需720元。根据消费者的需求，商家提供相应等级和价格的教学服务。

教学内容百元到手 技术传播或涉侵权

“AI换脸”技术教学服务具体包括哪些？记者花99.99元在那名号称特效师的博主处购买了相关套餐，共7节课，每节课时长在1分9秒至3分45秒，课程总时长在20分钟以内，核心课程包括“擦除视频中的人物、如何运用蒙版、如何抠出人物合成”，这些课程均为手机屏录制。

据授课者介绍，制作一条“换脸”视频，需要用到多个手机端应用，但并不复杂——从影视剧片段中截取一帧人物画面，用消除笔把想要替换的人物涂抹掉，将照片保存后即可进行剪辑。不过，在正式剪辑前还需要再准备一段素材，那就是本人在绿幕中录制好相关片段中人物的动作、台词。

经过这一系列操作，特效师可以代替周星驰与《赌侠》中的女主角张敏对话；成为《狂飙》中的徐江与高启强在公路飙车；取代周润发成为《英雄本色》中的小马哥；在一条19秒的影视剧片段中，甚至取代郭京飞被迪丽热巴亲了一口。

购买完课程，特效师邀请记者加入课程群聊，与其宣称的上万人参与学习的盛况不同，群里加上群主只有18人。群内无人发言，只显示一位普通群友被管理员“禁言30天”。

特效师告诉记者，课程学习完就可以去制作了。电脑端可以制作更加丰富的“换脸”视频，不过价格比手机端贵4倍。

记者注意到，评论区有用户提出疑问：“换脸”技术教学服务是否涉嫌侵权？博主不置可否。对此，武汉大学法学院副教授申晨说：“通过网络平台卖课、社交平台教学等形式传播‘AI换脸’技术，如果技术传播者明显知道这个技术很可能被用于制作淫秽物品，这样的情境是可以判断其构成帮助侵权的。”

申晨进一步分析，民法典第1169条规定了教唆、帮助他人实施侵权行为，承担连带侵权责任。相较于帮助侵权，教唆侵权的主观恶性更严重，如果一些人利用网络平台主动诱导他人学习“AI换脸”技术去实施侵权，可以认定为教唆侵权行为。

换脸背后暗藏风险 应用边界亟待厘清

还有一个问题是：擅自使用他人肖像制作“换脸”视频，背后暗藏什么法律风险和侵权纠纷？

记者就此咨询前述特效师博主，对方回复称“视频‘换脸’不涉及侵权，因为影视剧都是公开的，如果侵权，那么那些影视剪辑和影视解说都侵权了”，并称自己从业以来没有遇到过相关纠纷。

然而，受访专家给出的法律分析正好相反。

中国传媒大学文化产业管理学院法律系主任郑宁告诉记者，擅自使用他人肖像制作“换脸”视频，可能会涉嫌构成侵犯他人肖像权、名誉权等。无论是“换脸”App的经营者还是普通网友，凡未经影视剧著作权人的授权和许可，擅自将“换脸”后的影视片段通过网络提供给公众，使公众可以在其个人选定的时间和地点进行在线观看甚至下载等，都可能涉嫌侵害影视剧著作权人的信息网络传播权。同时，如果“换脸”后对原影视剧片段的主旨进行歪曲篡改，最常见的形式就是恶搞，还有可能侵害影视剧著作权人的保护作品完整权等。

郑宁认为，如果“AI换脸”技术被不法分子利用，被用于诈骗、色情、盗窃、恶搞、非法逐利等，则会产生极大危害，不仅侵害他人合法权益，还可能危害社会公共安全。

郑宁介绍，目前没有相关行业规范明确“AI换脸”的特定应用场合，但规定了“AI换脸”行为应当遵守的边界。《互联网信息服务深度合成管理规定》（以下简称《规定》）明确，任何组织和个人不得利用深度合成服务制作、复制、发布、传播法律、行政法规禁止的信息，并要求深度合成服务提供者应当建立健全辟谣机制。这为深度合成服务的技术应用划定了“底线”和“红线”。

“《规定》出台，表明有关部门已经在有意识地规划包括‘AI换脸’在内的人工智能深度合成技术，但该技术并未针对人脸更换技术的应用范围、目的进行限制。”在申晨看来，“AI换脸”涉及人的肖像，其相对于其他个人信息更具特殊性，也更为敏感。“AI换脸”技术会导致对个人身份识别的混淆，继而导致信息传播秩序混乱。所以，需要对这种潜在的危害进行使用范围的限制。

那么，“AI换脸”技术的应用边界在哪里？申晨认为，可以从两个应用场景考虑：专业的影视制作，在获得演员授权的前提下，可以合法应用该技术；网民娱乐性的使用，例如熟人之间做一些“换脸”视频进行娱乐等。

“这就涉及如何理解其中的授权问题，根据相关规定，‘AI换脸’需要获得对方的肖像权授权。肖像权授权形式可以有两种理解：第一种，只要不反对你使用我的肖像，就完成了知情同意的过程；第二种，必须由肖像本人实施明示的意思表示，才能得到制作‘AI换脸’视频的授权。”申晨说，对授权形式的两种理解可能要做价值判断，通过主动同意的方式获得“AI换脸”的权限，虽然有利于保护肖像权，但不符合社会交往中的观念，但若采用第一种理解，可能会带来事后规制的成本，因此“AI换脸”的应用边界还需要通过社会实践进一步摸索。

建立安全评估系统 完善监管防范体系

针对“AI换脸”乱象，近年来，国家网信办、各地网警、检察机关等协调配合，加大整治打击力度，办理了不少民事和刑事案件，出台了多项政策法规加强治理。

我国刑法、民法典以及国家有关部门出台的《网络音视频信息服务管理规定》《网络信息内容生态治理规定》等多部法律法规及政策规定，均涉及深度合成应用的规范、侵权责任等内容。

4月11日，国家网信办发布《生成式人工智能服务管理办法（征求意见稿）》，对生成式人工智

能产业给出较为详尽的规定，其中包括定义、准入资格、责任义务和处罚措施等。

“尤其是《规定》对防范深度合成技术所带来的社会危害和法律风险，迈出了非常重要的一步，实现了从无到有，让深度合成技术的应用有了专门的监督体系。”申晨说，不过一些具体措施还有待细化，比如《规定》要求的安全评估体系怎么做，谁来评估，评估的标准是什么？这些需要结合产业发展、技术背景和专业知识进行细化。

在郑宁看来，我国缺乏对人工智能的总体立法以及人工智能伦理的行业规范，虽然目前的相关法律对于“AI换脸”可能侵犯隐私权、名誉权、肖像权、个人信息、著作权，以及对网络安全、数据安全也有相应规定，网信办的相关规定对于算法、深度合成技术、安全评估也有规范，但是在AI产业创新以及国家安全、个人权益保护之间实现平衡，如何划定各主体的权利义务责任边界，仍有一些模糊不清的地方。

“AI换脸”技术侵犯的权益十分敏感，经由网络传播速度快，范围广，让人防不胜防，仅通过事后的责任追究很难达到理想的规制效果。因此，应该从技术开发者、网络服务提供者、用户三个层面，设计一套独特的监管体系。”申晨说。

申晨建议，对“AI换脸”技术的开发者以及相应的科技公司建立严格的备案手续和安全评估系统。目前“AI换脸”技术还比较粗糙，但通过优化迭代，未来肯定会高效且逼真，因此一定要合理限制传播范围。未来的监管体系要控制住技术源头，可以尝试要求技术开发者在技术中预留一个“技术水印”，即用户如果使用该技术制作视频，视频文件中会留下痕迹，那么网络平台可以迅速识别出该视频是使用“AI换脸”技术进行制作的。

对于网络服务平台，申晨建议对使用上传视频服务的用户信息进行审核，即要把AI合成视频制作者的身份，以便在后期产生法律风险时确定责任人。平台还要通过技术手段审核视频内容，识别其中是否有人工合成的要素，并进行标注。同时，平台在接到人工合成视频存在法律风险的告知时，需根据民法典规定的网络服务提供者义务，建立一套完善的应对机制。此外，用户在使用网络平台服务的过程中，如果发现有人“AI换脸”视频涉嫌存在法律风险，一定要有举报意识。

“当上述三个环节都建立起监管机制，再结合对违法者法律责任的追究，将会形成一个较为有效的、应对‘AI换脸’技术法律风险的防范体系。”申晨说。

曾参与电子商务法立法工作的浙江垦丁律师事务所律师张延来提出，治理“AI换脸”技术滥用现象，除了法律途径，还需引入社会力量尤其是商业力量，就像计算机病毒需要引入杀毒软件来遏制一样。不过，更应该关注技术本身所带来的有利效果，对于滥用行为可以依法打击，不必过于恐惧技术本身，而是应该学习和拥抱新技术。

“任何技术都是双刃剑，还是取决于谁来用，怎么用，用了违法怎么追责。”AI换脸在一些场景具有积极意义，比如影视制作、广告等，不应全盘否定，但是也要对其风险有充分认识。”郑宁总结说。

漫画/高岳

算法实现「传统人防」变「数算预警」

惠州仲恺区构建一体化智慧体系破解市域治理难题

□ 本报记者 邓君
□ 本报通讯员 颜险峰 刘琪

作为国家级电子信息产业基地，广东省惠州市仲恺高新区工业园区林立，产业项目聚集，流动人口占比近八成，基层治理呈现案件多、隐患多、防控难“两多一难”问题。为此，仲恺高新区坚持问题导向，建立综治中心，彻底打通全区数据壁垒，整合综治中心、流动人口管理系统、消防网格系统、国土三维地图等平台数据，共享仲恺“慧瞳”视频汇聚平台等视频资源，高效打造仲恺智治市域社会治理平台，积极探索城市公共安全治理新模式。

《法治日报》记者近日采访发现，在数字赋能“平安仲恺”的架构下，仲恺高新区充分发挥党建工作组织优势，依托智治市域社会治理平台，针对社会治理的堵点、痛点、焦点问题，构建“1123N”（1个综治中心，1个仲恺智治市域社会治理平台，综治视联网和电子政务外网2张信息主网，高空鹰眼市场瞭望设备、联动调度系统、流动人口信息采集系统3个支撑，“码上办”“粤心安”心理服务等N个治理专题）全域一体化智慧治理体系，以“绣花”功夫精细基层治理，变“被动管理”为“主动治理”，全面提升社会治理社会化、法治化、智能化、专业化水平。

风险早预警 平安不出事

2022年1月，仲恺高新区美某光学公司因经营问题拖欠工资，近百名职工聚集讨薪。平台常态化监测与分析全区企业各类数据，系统自主分析研判风险，向产业园及网格员下发异常预警信息，但公司迟迟未能解决存在的问题。

事件发生时，根据平台搭载的鹰眼和视频实时场景监控，指挥中心立即调拨周边警力和区直相关部门赶赴一线及时处置，掌控现场事态，经多方调解，问题被妥善化解。

在拥有强大的数据来源之后，仲恺高新区加强“AI算法”与“闭环管理机制”深度融合，聚合20000路视频，28套高空鹰眼瞭望设备，以人群非法聚集、占道经营、重点人员布控、垃圾违规倾倒等28个算法为基础支撑，增强全域态势感知，实现以“传统人防”转为“数算预警”。

目前，该区已组建538组“最小应急单元”，100%覆盖全区重点区域与单位。根据平台预警，采用常态排查+重点巡查结合，基本实现应急处突“1分钟启动、3分钟互动、5分钟增援到位”目标，有力确保社会面平安稳定。2023年2月16日，仲恺公安分局网警大队根据智治市域社会治理平台信息，数小时内就抓获了盗窃电动车的主要犯罪嫌疑人丁某。

管好出租屋 治理无盲区

“我们党员房东或者租客遇到解决不了的难题，都会寻求出租屋党支部的帮助。”仲恺高新区陈江街道御湖社区五一花园的房东花姐介绍。

近年来，仲恺高新区创新特色治理模式，制定出台《仲恺高新区关于成立出租屋管理党组织实施方案（试行）》，实践以出租屋管理党支部为轴心，抓住“党员房东”作用支点，因地制宜创建“红色出租屋”基层治理新模式，全面推行“党小组建在网格上”的做法，消除治理盲区。

仲恺高新区党群办公室负责人说，该区从纵向和横向两个维度构建出租屋管理党组织体系。纵向构建“区级出租屋管理联席会—镇街出租屋管理联合党委—村（社区）出租屋管理党支部—网格（村小组）出租屋管理党小组”的四级组织网络；横向整合政法、公安、消防、城管执法等十个部门资源，通过小程序收集问题诉求，定期召开联席会议进行议事决策，营造共建共治的治理格局。潼侨镇新华社区出租屋管理党支部通过“红色出租屋”整合多方资源，帮助身患髓母细胞瘤、年仅9岁的女孩获得“关爱困境母亲儿童”救助基金3万元，并筹集慰问金、善款等数万元。

依托智治市域社会治理平台，仲恺网建建设出租屋、社区近10000台“智慧门禁”与11000个人脸识别摄像头，采用“3D视频图像”绘制“VR智慧社区”，实现“由像到人”“以房管人”，为网格员基层治理工作及社会治安防控提供坚实支撑。2022年底，演达派出所收到江苏警方的协查通报，称一名在逃17年的嫌犯用化名潜入惠南科技园，警方凭借一张犯罪嫌疑人老照片，利用“智慧门禁”和人脸识别技术进行比对，迅速锁定犯罪嫌疑人并将其一举抓获。

据悉，目前仲恺已建立1个出租屋管理区级党建联席会、5个镇街出租屋管理联合党委、49个出租屋管理党支部、9个出租屋管理党小组；共收集群众反映诉求275件，办结率达98%，助力全区基层治理提档升级；刑事治安、“两抢一盗”、消防火灾警情同比下降9.55%、6.22%和30%。

有事“码上办” 群众少跑腿

“动辄拳脚相加，我实在受不了了。”惠环街道居民王某称，去年结婚以来，因生活琐事频频遭受酗酒丈夫江某实施家庭暴力，碍于江某的威胁及面子问题一直不敢报警。一次偶然的机会，她了解到“仲恺码上办”小程序，并从中找到“矛盾化解”专题，抱着试一试的心态，她在小程序中讲述了自身遭遇，并寻求帮助。

仲恺高新区综治中心在收到事件提醒后，立刻安排有关部门人员上门调解。在工作人员的批评教育和法律知识普及下，江某深刻认识到自己的错误，诚恳道歉并表示坚决改正。夫妻俩最终冰释前嫌。“仲恺码上办”小程序的推出，高效实现了“服务进家门，有事码上办、群众少跑腿”。

聚焦百姓“最难事”，针对基层治理履责过程中科技助力低、数据采集多、上传不及时、管控难度大等问题，仲恺高新区紧扣“全地域、全要素、全过程、全时空”治理需求，系统创建“全城一张网”智治新格局。在智治市域社会治理平台上强化“码上办”“粤心安”“矛盾化解”等专题应用，实现不同需求模块设计、不同专题定制组合、不同内容精准分析，做实做细民生工作。

自开展市域社会治理现代化工作以来，仲恺高新区持续创建7个镇街、园区综治分中心，56个村（社区）已基本完成综治中心室（工作站）的规范化建设，并配齐配全社会治安形势研判室、矛盾纠纷调处室、“粤心安”社会心理工作室、法律咨询室、党建活动室、群众接待厅。全面下沉基层治理力量，社会矛盾化解能力进一步提升，一般性矛盾纠纷化解率达100%，重大矛盾纠纷化解率达85%，累计为群众办好事实事1458件，推动区域民众幸福感和满意度不断提升。