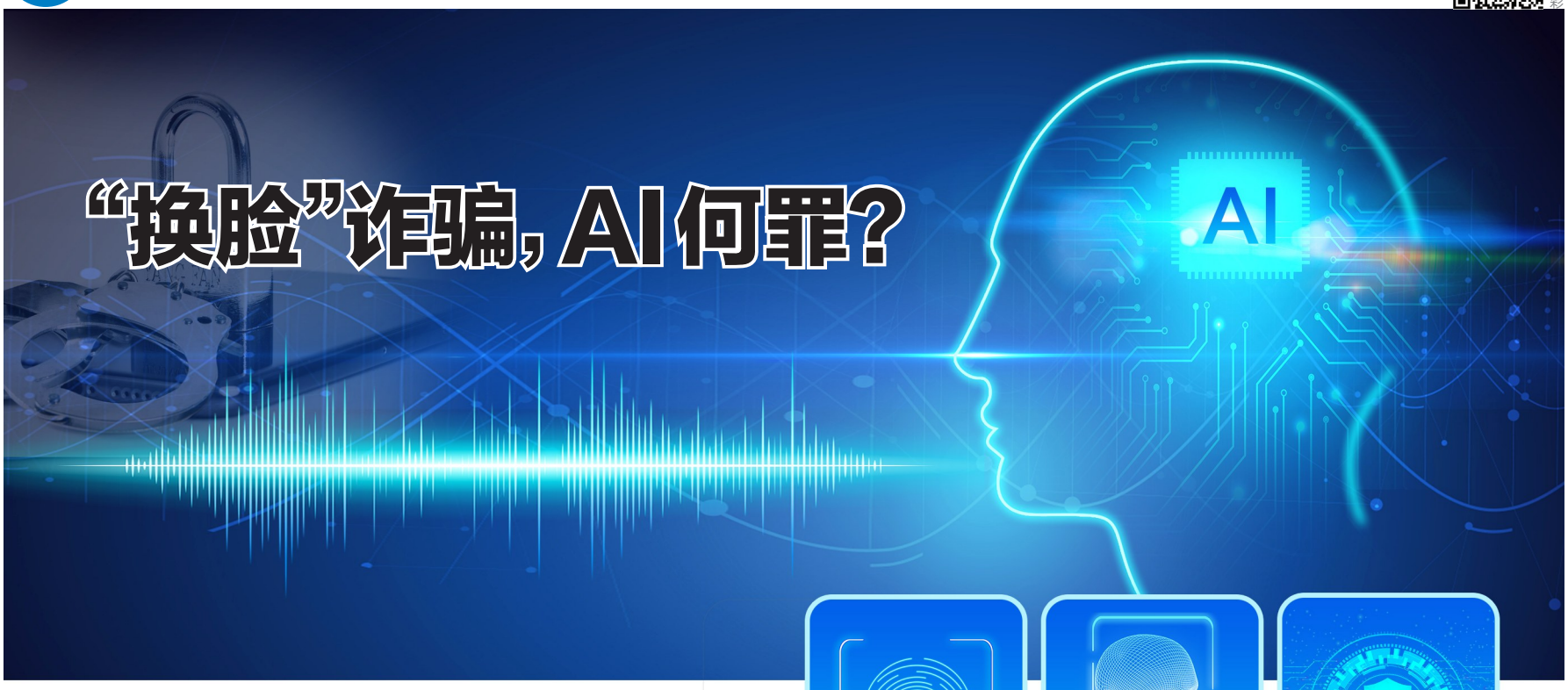
“换脸”诈骗，AI何罪？



记者 徐越蔷

骗子通过AI换脸和拟声技术，10分钟骗走福州某公司430万元；安徽一男子被9秒“AI换脸视频”骗百余万……近段时间，几起宣称利用AI技术实施诈骗的案件引发关注，“AI诈骗正在爆发”的话题一度冲上微博热搜。

通过与公安部门核实确认，记者了解到，“AI诈骗爆发”的传言不实，目前此类诈骗发案占比很低。此外，截至发稿，上述涉及安徽的案件，仍在进一步办理当中。

2023年显然是无可争议的AI大年。专家表示，利用新技术诈骗是电信诈骗的典型特点，应当在深入研判涉AI诈骗行为新规律的基础上，综合施策，从技术层面和监管层面“双管齐下”。

现象
两起案件涉嫌诈骗数百万元

据“安庆公安”官方微博5月25日消息，日前，安庆经开区发生一起冒充“熟人”诈骗案，诈骗分子使用了一段9秒钟的智能AI换脸视频，佯装“熟人”实施诈骗，金额高达132万元。但记者发现，目前该条微博已无法查看。

6月10日，记者联系到安庆警方。对方表示，“这个案子目前还在办理中，案件尚未定性”，具体情况仍有待调查。

此前，据“平安包头”微信公众号消息，内蒙古自治区包头市公安局电信网络犯罪侦查局发布一起使用智能AI技术进行电信诈骗的案件，福州市某科技公司法定代表人郭先生10分钟内被骗走430万元。该条消息推送于5月20日，目前公众依然可查看。

两起案件披露后，引起高度关注，“AI诈骗正在全国爆发”等相关词条占据微博热搜榜前列。6月10日，国家反诈中心辟谣：“AI诈骗正在全国爆发”传言不实。公安部刑侦局提醒大家，转账前请多方核实，切勿轻信网络信息。

不过，警钟已经敲响。记者留意到，利用AI技术进行诈骗的案例并非近期新发，早在2021年初，公安部网安局就曾发文提醒公众，注意防范合成声音和AI换脸等人工智能新型诈骗手段。

“AI换脸及拟声技术本质上是对人脸、声音等生物特征信息二次加工利用。”安徽一名人工智能行业资深从业者傅女士向记者分析，“AI换脸技术可以将一个人脸图像中的面部特征替换成另一个人脸图像中的面部特征，同时保持原图像中其他部分不变。”

关注
个人信息泄露是黑灰产源头

值得关注的是，除了生成式AI技术，被打包销售的个人信息则是“AI换脸”诈骗中所需投喂的“原料”。近年来，各地公安机关在严厉打击此类侵犯个人隐私及售卖信息的行为。

在公安部部署的净网2021专项行动中，合肥市公安局网安支队联手包河分局打掉一个在合肥、青岛等地非法利用AI人工智能技术，伪造他人人脸动态视频，为黑灰产业链提供注册的虚拟手机卡等技术支撑的犯罪团伙。

为了完成视频制作，嫌疑人就需要大量的公民个人信息照片。“身份证正反面照片、手持身份证照片、自拍照等，被称为一套。”民警表示，成套照片被称为“料”，出售照片的人则被称为“料商”，而这些“料”在网上往往已经转手了很多次，但很多受害人对此却是毫不知情。

在当前的大数据时代，更应保护公众隐私。“骗子分析公众发布在网上的各类信息，根据所要实施的骗术，通过AI技术筛选目标人群。”傅女士提醒道，从个人防范方面来说，大家在网络或社交平台上发布图片、视频、音频时，可以嵌入不可见的数字水印信息，这些信息在不影响视觉效果的情况下，能大大降低视频和照片被AI模型成功篡改的概率。

说法
用AI换明星脸带货或涉侵权

打开电商平台，涉及“AI换脸”销售比比皆是。记者咨询一家出售“AI换脸”教程的商家，对方称“帮你换成别人的模样还能直播变现”，该套资料包括视频换脸教程、直播换脸教程、遮罩模型训练、换脸模型参数讲解、在微信中的应用等。

随后，记者又以买家身份咨询了多家“制作换脸合成视频”的卖家，得知制作价格根据分辨率和时长来确定，一条30秒的视频，价格通常在几十元至几百元不等。客服声称，“如果用来审核，可以选贵的，合成度更好，一般查不出来。”

目前，AI换脸随处可见，在手机应用软件、短视频平台上，不少用户都“尝鲜”过。仅需上传一张照片，就可以变成视频中人，或视频换装，走进各种场景。

事实上，AI换脸并非法律监管空白地带。2023年1月10日起施行的《互联网信息服务深度合成管理规定》已提出，服务者若提供智能对话、合成人声、仿声、人脸生成、替换等深度合成服务时，应当进行显著标识，避免公众混淆或者误认。4月11日，国家互联网信息办公室发布的《生成式人工智能服务管理办法（征求意见稿）》，也对生成式人工智能产业做出了包括定义、提供者的合规义务在内等多方面的详尽规定。

安徽云旗律师事务所律师廖雪伶向记者表示，AI换脸自娱自乐无可厚非，但提供AI换脸技术的互联网公司若未经明星授权擅自使用，或某些单位或个人未经授权擅自使用AI换脸技术从事商业活动，则可能侵犯包括但不限于肖像权、姓名权、名誉权等民事权利，权利人可向侵权人主张停止侵害、消除影响、恢复原状、赔偿损失等权利。

观点
AI安全课题有待持续攻关

“AI换脸”诈骗，怎么防？“即时AI换脸视频有破绽，可以让对方用手放在面部前面晃动，AI技术会发现有障碍物则无法实时计算输入包含手部的画面。”傅女士还提到，判断一个视频是否经过AI换脸处理，可以观察其中的人物是否缺乏眨眼的动作，“因为多数假脸使用睁眼图片合成，极少数会眨眼。”

傅女士认为，从企业责任的角度看，公司和机构需要更加严格的信息安全管控，这样才能降低“AI换脸”技术滥用风险。“企业需要持续开发新的技术解决方案，如AI检测和预防系统，以检测和预防利用AI技术实施诈骗活动的发生。”

“对于深度合成服务与应用方面的规范，还需进一步细化。”安徽的柯少婷律师建议，对于提供“AI换脸”技术的互联网科技类企业加大监管力度，对公民的个人信息保护应加强普法宣传力度；建立健全警民互通渠道，增强公民的自我监管意识。

实际上，每一次新技术的迭代都有可能带来层出不穷的技术诈骗，也正所谓“科技是一把双刃剑”。多位业内人士向记者表示，当前，AI安全研究仍然落后于AI能力研究，这是技术厂商应持续攻关的方向。