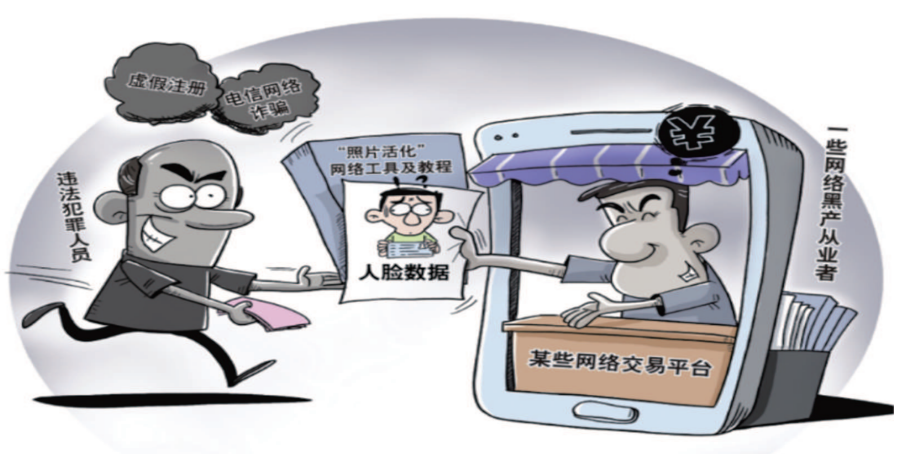
上海法治報
www.shfzb.com.cn
2022年4月19日 星期二

“变脸”诈骗防不胜防

合成技术滥用对个人敏感信息保护形成挑战

一段视频、一段语音未必是真人拍摄或者录制。在你不知道的手机App后台、支付界面、门禁闸机，或许有人正在盗刷你的脸……去年以来，多地发生“变脸”诈骗案。

记者调查发现，随着深度合成技术迅猛发展、落地场景激增，一些不法分子趁机牟利。音频、视频等合成技术滥用，对人脸、声纹、指纹等个人敏感信息保护形成挑战。



资料照片

截取面部视频画面“换脸”

近日，陈先生来到浙江省温州市公安局瓯海分局仙岩派出所报案，称自己被“好友”骗了近五万元。经过警方核实，骗子用了AI换脸技术，利用陈先生好友阿诚社交平台上先前发布的视频，截取了面部视频画面并进行了“换脸”，从而对陈先生进行了诈骗。

2021年4月，安徽省合肥市警方在公安部“净网2021”专项行动中打掉一个犯罪团伙，该团伙利用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手机卡等技术支撑。

在警方抓捕现场，几名犯罪嫌疑人正用电脑将一张张静态照片制作为人脸动态视频。模拟制作出来的动态人物不仅能做点头、摇头等动作，还可完成眨眼、张嘴、皱眉等丰富表情，效果极为逼真。

在嫌疑人的电脑里，警方发现了十几个G的公民人脸数据，人脸照片和身份证照片分门别类存放在一个个文件夹里。“身份证正反面照片、手持身份证照片、自拍照等，被称为一套。”民警介绍，成套照片被称为“料”，出售照片的人被称为“料商”，这些“料”在网上已转手多次，而“料”的主人却毫不知情。

犯罪嫌疑人马某交代，由于制作简单，一个视频价格仅为2至10元，“客户”往往是成百上千购买，牟利空间巨大。

近年来，类似案件在浙江、江苏、河南等多地发生。浙江衢州中级人民法院的一份刑事裁定书披露：张某、余某等人运用技术手段骗过支付宝人脸识别认证，并使用公民个人信息注册支付宝账户，非法获利数万元。

这些案件的作案流程颇为雷同：不法分子非法获取他人照片或有偿收购他人声音等“物料”，仅需少量音视频样本数据，便可合成媲美真人的伪造音视频，用来实施精准诈骗，侵害他人人身和财产安全，或销售、恶意传播技术换脸不雅视频等，造成肖像权人名誉受损。

网络“叫卖”合成软件教程

据合肥市公安局包河分局网安大队民警王祥瑞介绍，前述案件中8名犯罪嫌疑人多为社会闲散人员，有的连高中都没有读完。他们按照网购教程下载软件，花几个月便“自学成才”。

记者在网上联系到一位售卖相关教程的卖家。卖家介绍，全套软件及教程售价有400元、800元两档，800元的为高阶版本，“过人脸成功率超高”。记者在演示视频中看到，照片上传至软件后，标注出五官位置，调整脚本参数，一张脸便动了起来。“五官参数随教程送上，照抄即可。”据介绍，这些伪造视频不仅通过率高，人工审核都难辨真假。

“目前公众对照片等静态信息易被篡改已有所警惕，但对视频、声音等动态信息内容仍持有较高信任度。”清华大学人工智能研究院基础理论研究中心主任朱军说，深度合成技术飞速演进，让“眼见不再为实”，破解身份核验的难度会越来越低、耗时将越来越短。

专家担心，尽管针对深度合成技术的识别技术不断迭代、检测手段持续增强，但依然没能跑赢“伪造”技术升级的速度。浙江大学网络空间安全学院院长任奎说，随着合成技术应用门槛的进一步降低，合成内容已模糊真实与伪造的边界。

北京智源人工智能研究院安全创新中心执行主任田天认为，新型伪造方法层出不穷，网络传播环境日趋复杂，检测算法存在漏洞缺陷等，反深伪检测难度越来越大。

法律规定相对滞后，也给不法分子留下可乘之机。中伦律师事务所合伙人陈际红说，目前法律规定，禁止利用信息技术手段伪造等方式侵害他人的肖像权，但技术如何使用算合理使用，哪些情形下应禁止使用等，没有具体规定；收集或收购个人声纹、照片，使用人脸、指纹、DNA、虹膜等个人生物信息等行为，在哪些范围内构成犯罪、将面临怎样的惩罚，需要司法裁判进一步给出明确指引。

提高技术滥用的违法成本

保护人脸、指纹、声纹等敏感信息，不再担忧信息“裸奔”损害个人隐私、财产、名誉等，是公众的共同期待。

我国首个国家层面的科技伦理治理指导性文件《关于加强科技伦理治理的意见》近日印发，凸显技术伦理治理的重要性紧迫性。在今年的最高法工作报告中，包括人脸安全在内的个人信息安全等多次被提及。

陈际红表示，打击“变脸”诈骗犯罪，应从技术的合法使用边界、技术的安全评估程序、滥用技术的法律规制等方面予以规范，提高技术滥用的违法成本。

中国工程院院士、信息技术专家邬贺铨提出，针对深度合成技术滥用现象，应以技术规制技术，利用技术创新、技术对抗等方式，提升和迭代检测技术的能力。

技术规制之外，针对技术滥用暴露的风险治理应当体系化、完善化。“要构建数据集质量规范、根据应用场景对相关技术进行风险分级分类管理，明确设计开发单位、运维单位、数据提供方的责任。”国家工业信息安全发展研究中心副总工程师邱惠君说。

专家提醒，针对花样翻新的“变脸”诈骗，公众要提高防范意识，不轻易提供人脸、指纹等个人生物信息给他人，不过度公开或分享动图、视频等；网络转账前要通过电话、视频等多种沟通渠道核验对方身份。一旦发现风险，及时报警求助。

对电信网络诈骗保持严打高压

近日，国新办举办新闻发布会，邀请公安部、最高法、最高检、工信部、人民银行相关负责人介绍打击治理电信网络诈骗犯罪工作进展情况。

合力挤压犯罪空间

据介绍，全国公安机关深入开展“云剑”“长城”“断卡”“断流”等专项行动，先后组织开展150次全国集群战役。一年来，共破获电信网络诈骗案件39.4万起，抓获犯罪嫌疑人63.4万名，同比分别上升28.5%和76.6%。根据最新统计，电信网络诈骗立案数连续9个月同比下降，打击治理工作取得显著成效。

各部门充分发挥职能作用，合力挤压犯罪空间。“公安部会同国家移民管理局组织开展‘断流’专案行动，打掉非法出境团伙1.2万个，抓获偷渡犯罪嫌疑人5.1万名；会同最高法、最高检、工信部、人民银行和三大运营商持续推进‘断卡’行动，打掉‘两卡’违法犯罪团伙4.2万个，查处犯罪嫌疑人44万名，惩戒失信人员20万名，惩处营业网点、机构4.1万个。”公安部副部长杜航伟说。

“工信部升级启动‘断卡行动2.0’，组织集中排查处置涉诈高风险电话卡9700多万张，清理关联互联网账号5700万余个，对全国物联网卡开展拉网式排查，一大批存量高危号卡得到全面清理。”工信部网络安全管理局局长隋静介绍，2021年，工信部依法处置涉诈码号4.5万个、域名网址104万个，拦截涉诈电话19.5亿次、涉诈短信21.4亿条，部署推进“打猫（池）行动”，大力清理诈骗作案工具。

去年，人民法院、人民检察院加大力度，依法惩处电信网络诈骗犯罪。据了解，全国法院一审审结电信网络诈骗犯罪案件2.5万余件，6.1万余名被告人被判处刑罚；全国检察机关共起诉近4万人，依法惩治为诈骗犯罪“输血供粮”的各类网络黑产犯罪和掩饰、隐瞒犯罪所得、犯罪所得收益罪。

循法而行，依法而治，为打击治理电信网络诈骗犯罪提供有力法律武器。“最高法会同最高检、公安部先后制定出台了《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》和《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》，去年至今又两次下发关于‘断卡’行动会议纪要等规范性法律文件。”最高人民法院刑三庭负责人李睿懿介绍，人民法院将不断完善和明确法律适用标准，抓紧研究制定适应电信网络诈骗特点和规律的证据规范，进一步解决此类案件侦查取证难、认定难的问题。

全力追缴被骗资金

紧急止付群众被骗款3291亿元，累计拦截102万个资金账户148亿元，追缴返还人民群众被骗资金120亿元……“全国公安机关始终把追赃挽损作为反诈工作的重中之重。”公安部刑事侦查局局长刘忠义介绍，近年来，公安机关会同人民银行、银保监会等部门建立快速止付冻结、涉诈银行账户风险监测拦截等机制，出台相关规定细则，依法追缴返还电信网络诈骗受害人被骗资金。

李睿懿介绍，人民法院把挽回被骗群众财产损失与案件审理同步推进，会同相关部门依法彻查、追缴涉案资金，探索建立涉诈冻结资金依法及时返还机制，最大限度减轻和弥补被骗群众的财产损失。

金融行业“资金链”治理是打击电信网络诈骗犯罪的重要一环。2021年，金融系统识别拦截资金能力明显上升，月均涉诈单位银行账户数量降幅92%，个人银行账户户均涉诈金额下降21.7%。

“人民银行建成了电信网络诈骗资金查控平台，2021年商业银行、支付机构根据公安部门指令，处理涉诈资金1.5亿笔，紧急拦截涉诈资金3291亿元。商业银行向公安机关推送涉诈受骗资金交易预警信息242.8万条。”人民银行支付结算司司长温信祥介绍，在诈骗犯罪多发的中缅边境地区，人民银行会同公安部门探索运用新技术协助锁定1768名跨境资金转移“背包客”，不断织密金融行业风险防控网。

不断提升治理效能

电信网络诈骗犯罪多发高发，其背后折射出网络治理、社会治理等方面还需不断完善。“电信网络诈骗犯罪是复杂的社会治理问题，并不是简单的社会治安问题。”杜航伟表示，下一步，公安机关要在继续严打高压、严密防范前提下，一方面不断深化治理，依法加强对涉诈人员管理，全面落实出境管控措施，严格落实实名制和失信人员金融通信惩戒措施；另一方面继续加大宣传力度，将广泛宣传与精准宣传相结合，加强对易受骗群体、案件高发行业和重点地区的精准宣传，建立全方位、广覆盖的反诈宣传体系，切实增强人民群众防骗意识和反诈能力。

最高人民检察院第四检察厅负责人程雷表示，检察机关将更加重视数据赋能，强化大数据思维，推动建立数据互通共享，加强数据集成分析研判，及时发现打击治理的“死角”和“盲点”。

去年以来，工信部推出“一证通查”、12381劝阻短信，开发“老年人亲情号码预警”“闪信霸屏预警”等新功能，大幅提升了预警劝阻效果。“我们将继续加强反诈技术手段，建设国际出入口短信预警系统，实现对国际来话和短信实时主动提醒，提升群众防范跨境诈骗意识。通过‘反诈名片’，实现对主叫号码的权威标记，有效甄别号码真伪，多措并举，不断提升电信网络诈骗治理效能。”隋静说。

（来源：新华社、人民日报）

社址：上海市小木桥路268弄1号（200032） 电话总机：34160933 订阅热线：33675000 广告热线：64177374 交通安全周刊电话：28953353 零售价：1.50元 上报印刷