

AI换脸拟声的发展与安全博弈

“妈，八千块钱不够，给我转一万五吧。”一位母亲正和女儿视频聊天，听着在外地上学的女儿在视频里撒娇抱怨“生活费不够用了”，她打算按下转账键。就在这时，家门打开了，她“真女儿”走了进来。而另一头，视频里的“假女儿”还在央求着妈妈“给生活费”。

这不是恐怖片，而是一则AI反诈视频，这样的场景也真实地发生在当下。在这条反诈视频评论区中，不少网友反映自己也有过类似的被编经历。

近日，国家金融监督管理总局发布新型电信网络诈骗，将“AI拟声换脸”纳入其中，作为专门类诈骗。

记者近日调查发现，AI拟声换脸技术已成为简单易操作的低门槛技术，只需拥有声音与照片等“素材”，借助软件即可瞬间实现“AI克隆”。

受访专家指出，擅自使用他人信息制作“拟声换脸”视频涉及多重法律风险。目前，我国有些立法及执法尚未能跟上科技发展的脚步，要进一步完善相关领域的立法、加大执法力度，秉持包容审慎的态度平衡技术的安全与发展。同时，专家亦提醒公众不要轻信“有图有真相”，要加强个人信息保护意识。

AI技术不再高门槛

随着AI技术的发展，AI拟声换脸技术变得唾手可得。记者浏览社交网络平台发现，不少网友即使是“技术小白”，也能够自主利用市面上的AI智能工具完成拟声换脸。

“只需要准备一段25秒的声音，构建声音进行训练，训练完毕后就可以输入想要的文本进行语音合成。”在某社交媒体平台上，一名科技博主发布了一段教学视频，向网友介绍如何用AI精准克隆人声。教学视频中，这名博主仅用时不到1分钟，就把AI拟声的原理讲解得清清楚楚，与此同时，一段“孙悟空”的拟声就这样诞生了。他输入了一段文本，AI便能用与“孙悟空”近乎一模一样的声色语气念出来。

据这名科技博主介绍，这个AI拟声工具无须下载，也不收费，是可以免费使用的网页，而如此制作出来的音频可以公开供他人使用，也可以导出使用。同时，AI可以变换多语种，“你要用什么语言，就用什么语言训练即可”。

记者按照视频中的指示打开对应网页，在网页中分别上传了5种不同声音，经过训练，这5种声音被近乎无差别地克隆，能够用来读出任意文案。除此之外，用户还能够在输入文案时加入情绪的描述，使得AI拟声如同能够“谈笑风生”的真人。

除了AI拟声，AI换脸也成了“热门”技术。在一些图片处理软件中，“一键AI换脸”能够瞬间将图片中的脸毫无痕迹地置换成另一张脸。而除了图片换脸，视频换脸也成了低门槛、易操作的技术。

“一天能做100个原创作品，这个工具太强了。”在社交媒体平台某



图片来源于网络

AI科技博主短视频里，他向粉丝们介绍起一款视频换脸软件。屏幕中，博主所展示的两个视频中的女生除了五官不同，其余的外貌、穿着及动作完全一致。“一键就能给她们高清换脸，变成另外一个人。”视频中，女孩不论如何转身，抑或做出任何表情，面部都没有产生畸变。

换脸拟声技术被倒买倒卖

AI拟声换脸不再是高门槛技术，而在社交媒体平台上隐蔽的“有偿技术传授”“技术买卖”则进一步降低了这种门槛，甚至使得AI拟声换脸成了不法分子“有手就会”的诈骗犯罪工具。

记者在某社交平台检索“AI换脸”时，有不少“卖家”混杂其中寻找其“客户”。“需要自定义AI换脸软件吗？”其中，一名卖家通过私信联系到了记者，推销其软件。记者询问该软件是否能够实时视频换脸拟声，卖家称“任何社交媒体都能够支持实时”。

随即，该卖家向记者展示了其在社交媒体平台上发布的换脸演示。在换脸演示中，该名男子以“英俊的脸庞”出现在社交媒体视频页面中，而这张“英俊的脸庞”是换脸后的“假面”。该卖家配文道：“网恋神器，直接变小哥哥，换个面貌可以去找小姐姐网恋了。”

为了让记者更“真切”体会到换脸技术的高超，该名卖家提出可以“打个视频看效果”。打开某社交软件视频通话，出现在记者面前的又是与“换脸演示”中面貌不一样的另一男子。该卖家表示，二者都是其通过换脸软件制作的。在视频中，他展示了喝水、捂嘴、捏脸、捂脸等多个动作，“做动作是没问题的，只要打开视频前把这个软件打开就可以了”。

在交流时，卖家不断向记者强调其所售卖的技术操作难度不大，且在视频时“看不出破绽”，而对于买家购买此项技术的目的，卖家则没有问及。“299元就给你装好软件，操作一遍演示。如果支付599元，则可以一对一教学，教会为止，软件可以永久不限次数使用。”该名卖家说。

记者调查发现，大多卖家通过私

信、评论等方式，用较为隐蔽的语言引导买家进行购买，对于购买目的并不予查明，便随意地将相关软件及操作方式变卖他人。除此之外，在某二手交易平台上，也有卖家出售相关技术。比如有卖家在产品描述中这样写道：“有手就可以，拍下就发完整视频资料 and 制作方法，可批量搞，虚拟资源能够变现。”

“有些人会利用技术去做违法犯罪的事情，尤其是在近几年，这种技术更容易使用了。”一名业内人士向记者透露，他就曾接到过一些“出格”的客户需求：“比如说有人联系我们，希望我们能用AI克隆技术去突破银行和一些支付软件的刷脸功能。还有人打离婚官司，要我们去拟声作伪证。如果没有问清楚，拟声换脸很容易就沦为不法分子诈骗、犯罪的工具。”

加强立法监督

张泽伟的AI工作室主要经营“AI数字生命”业务，他向记者介绍，在涉及个人的声音及形象时，工作室会综合多个方面避免信息落入非法用途：“首先我们会征得本人授权，如果是逝者，我们也会要求出示直系亲属证明。另外我们会签订协议，明确规定产品不能用于任何违法违规用途。”

北京大成（深圳）律师事务所律师陈翠也认为，擅自使用他人肖像制作“换脸”视频可能侵犯他人肖像权、隐私权：“根据《中华人民共和国民法典》第一千零一十九条，未经本人同意，不得以营利为目的使用他人肖像。换脸视频即便不以营利为目的，也可能因未获授权而侵犯肖像权。同时，未经许可传播涉及含有个人隐私的视频也会侵犯个人隐私权。”

陈翠表示，若拟声换脸视频内容不当或引发公众误解，可能会构成名誉权侵权，如果视频中包含他人享有著作权的内容（如影视片段），则可能构成著作权侵权。同时，未经授权制作和传播换脸视频还可能违反《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规规定，面临行政处罚或刑事责任。

“根据我国刑法、民法典、治安管理处罚法以及《互联网信息服务深度

合成管理规定》等，AI的换脸变声涉及多种法律风险，但现在仍然没有一部正式的关于人工智能的法律。”中国传媒大学文化产业管理学院法律系主任郑宁指出，现有法律其实对于这类现象是有相关惩治手段的。但之所以屡禁不止，是因为这种AI拟声换脸造假成本低，收益率高，“而法律制裁的脚步还跟不上”。

值得注意的是，国家金融监督管理总局将“AI拟声换脸”纳入新型电信网络诈骗类别。据金融监管总局金融消费者权益保护局介绍，“AI拟声换脸”类金融诈骗，从手法上看，多为不法分子以“网店客服”“营销推广”“招聘兼职”“婚恋交友”等为借口，通过微信、电话等方式联系消费者，采集发音、语句或面部信息。利用“换脸”“拟声”等技术合成消费者虚假音频、视频或图像，模拟他人声音或形象骗取信任，再以借钱、投资、紧急救助等借口诱导其亲友转账汇款，或提供银行账户密码等敏感信息，随后立即转移资金。

“这表明此类技术的滥用已引起法律和监管机构的高度关注。”陈翠指出，“目前，我国在相关领域仍缺乏系统性立法，涉及人工智能的法律规范较为分散，同时，人工智能伦理规范尚未形成统一标准，为有效遏制此类技术作为犯罪工具，须进一步明确其法律界定和应用边界。”

郑宁认为，目前，我国《互联网信息服务深度合成管理规定》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，这在一定程度上为深度合成服务的技术应用划定了底线。

“要正面划定AI拟声换脸的使用范围是有一定难度的，可以规定一些使用的原则，比如合法、必要条件等。”郑宁指出，当前我国有《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》，如果人工智能应用符合该规定应用条件，也可以遵循其要求进行安全评估。

在郑宁看来，对于AI拟声换脸的治理除了完善立法，加大执法司法力度之外，还应当“多管齐下”：“行业要积极自律，同时也要加强对公众的教育，一方面提升大家的守法意识，让大家知道这种行为是违法犯罪，另一方面教育公众善于防范和识别，不轻易相信有图有真相。”

“AI产业是需要规制的，但在安全与发展的平衡之间，涉及价值的选择判断问题。”郑宁指出，“我国目前的AI产业还处在发展阶段，因此发展和安全要并重。我们不能纵容违法犯罪，要保持审慎监管的态度，在分级分类的基础上进行预防式治理，同时也要持有包容的态度，促进产业发展，鼓励创新。”“AI技术的发展是不可逆的。”张泽伟亦直言，技术本身并无善恶，重要的是如何管理与规制技术的使用场景以及使用技术的人，以保证AI技术在我国的安全健康发展。

文章来源：《法制与新闻》杂志