责任编辑 / 魏艳阳 E-mail:fzbfzsy@126.com

“谎颜”AI换脸 一键生成or直接“搬运”？

嘉定法院审结一起著作权侵权纠纷案

释法

□ 见习记者 王葳然 通讯员 张晓莉 叶莎

用户点开“谎颜”小程序，通过“AI换脸”便能一键生成自己的古风汉服形象，观看广告后还可免费保存到手机相册。但实际上部分模版素材却是侵权“搬运”的盗版？近日，嘉定区人民法院审结一起因提供“AI换脸”服务引发的著作权侵权纠纷案。

陈女士是一名古风人像摄影师，在某短视频平台上开设有实名认证账号，并发布其自行创作的短视频，有300余万次获赞、10余万粉丝。

一天，陈女士发现上海某科技公司运营的一款名为“谎颜”的小程序里设置有AI生成“一键换脸古风汉服”板块，其中展示的部分模版素材竟与自己平台账号中发布的短视频如出一辙。

不仅如此，陈女士还发现，用户仅需将自己的照片上传至“谎颜”小程序，在点击观看30秒广告后即可制作“AI换脸”后的古风汉服形象，并免费保存到手机相册中。

在意识到自己创作的短视频可能被他人擅自使用后，陈女士随即进行了证据保全。陈女士认为，上海某科技公司未经许可在“谎颜”小程序中使用自己创作的13条短视频，侵害其作品的信息网络传播权，因此向人民法院起诉，要求上海某科技公司立即下架侵权视频、赔礼道歉并赔偿经济损失及维权合理费用。

嘉定法院经审理认为，陈女士创作的原始视频体现了制作者独创性的选择安排，属于受著作权法保护的视听作品。“谎颜”小程序中的视频内容系通过对原始视频进行局部替换合成，二者构成实质性相似。上海某科技公司以“AI换脸”为卖点将原始视频用于牟取商业利益，既未经授权许可，又未支付报酬，其行为侵害了陈女士作品的信息网络传播权，应当依法承担相应的民事责任。

案件审理中，上海某科技公司表示认识到相关行为可能构成侵权，已经删除涉案视频、主动履行了相关人工智能算法备案。

在此基础上，法院就运用算法技术提供网络服务向上海某科技公司发送合规建议，该公司接受建议并承诺今后将加强算法安全评估及素材来源合规审查，注意对他人个人信息、隐私、肖像等人身权益及知识产权的保护。同时，被告获得了陈女士谅解，原告撤回要求下架侵权视频、赔礼道歉的诉讼请求。

法院经审理认为，上海某科技公司作为数字经济行业小微初创民营企业，应诉后能够主动响应人民法院的合规建议，积极整改并获得权利人谅解，其后续合规经营也有利于市场健康发展，这在其责任承担中也可作为考量因素。人民法院综合原始视频的类型、独创性程度、市场价值、上海某科技公司的使用方式、侵权行为影响等因素，判决上海某科技公司赔偿陈女士经济损失及合理维权费用共计7500元。

判决后，双方均未提出上诉，目前该案已生效。

【法官说法】

以算法为基础的人工智能技术对于推动新质生产力及数字经济发展具有重要意义，但其技术应用及生成内容不得侵害他人合法权益、妨害市场竞争秩序及整体利益。

涉案原始视频是古风人像写真类视频，由一系列有伴音的连续画面组成，在内容编排、景别选取、拍摄角度等方面体现了制作者独创性的选择安排，属于受著作权法保护的视听作品。

“AI换脸”是指利用合成算法进行素材加工、内容转化和合成输出，但相关过程触及知识产权或人格权等多种法益，如：破坏肖像与主体的同一性，侵害他人肖像权；对“人脸”等生物识别信息未尽到合理安全保障义务，侵害个人信息权益等。因此，利用算法等人工智能技术应当注重多重法益保护，注意行为边界，避免侵害他人合法权益，合理合法开展经营和服务活动。

算法等人工智能技术广泛应用于各领域，正处于不断发展过程中，需坚持促进创新和依法治理相结合，推进技术运用向上向善。实践中，算法服务引发多元主体利益冲突，各类新型纠纷不断涌现，司法既要通过个案确立裁判规则，应对算法纠纷对传统法律关系带来的挑战，又要积极发挥治理职能，合理运用司法建议等形式引导技术合规利用，弥补现有法律法规与当前算法治理需求之间的空白。

本案被告系数字经济行业小微初创民营企业，对算法等人工智能技术应用涉及的政策因素、法律因素及行业发展因素等缺乏全面了解。为帮助其合规经营和稳定发展，人民法院制发合规建议，提示其强化依法经营意识、积极完善行政手续、注重素材合法性审查、内容生成合成合法性审查、重视安全发展等，被告亦主动响应合规建议，积极作出整改且获得了权利人谅解，实现了一定的治理效果。

价值数百万元虚拟币不翼而飞

4名“内鬼”犯非法获取计算机信息系统数据罪获刑

□ 记者 季张颖

价值百万元的虚拟币不翼而飞，证据锁定了3名“内鬼”，然而一路追踪，竟然发现还有“案中案”，真正幕后大盗浮出水面……近日，经徐汇区人民检察院依法提起公诉，徐汇区人民法院依法以非法获取计算机信息系统数据罪，分别判处被告人刘某、张某甲、董某有期徒刑3年，并处罚金3万元；以非法获取计算机信息系统数据罪，判处张某乙有期徒刑3年，并处罚金5万元。

谁动了他价值百万的虚拟币

2023年5月，当市民欧某在咖啡店里打开某公司开发的虚拟币钱包软件，想查看一下自己时值数百万元的虚拟币是否增值时，发现账户中的虚拟币全都不见了。欧某自行排查后发现，竟是一个月前有人将自己的虚拟币一转而空。

通过对程序进行分析，欧某注意到虚拟币钱包软件中存在会自动获取虚拟币钱包地址、私钥的后门程序，并据此追踪到可疑的用户信息。2023年8月，欧某带着自己搜集到的证据前往徐汇公安分局报案。几天后，犯罪嫌疑人、均为该公司员工的张某甲、董某、刘某陆续到案。

三人到案后交代，2023年3月初，三人经商议，决定在某虚拟币钱包软件中加入后门程序以获取用户私钥。三人分工合作，由刘某负责编写后门程序，董某负责购买服务器和域名并对获取的私钥加密，张某甲负责搭建服务器和数据库。当用户首次安装带有后门程序的软件，后门程序就会在5天后自动运作，将私钥、助记词等信息上传至域名下的数据库内。运行一定时间后，后门程序就会自行停止窃取相关信息。

为逃避侦查，2023年5月底，三人在保存好窃得的私钥及解析出的对应数字钱包地址后，就把服务器和数据库销毁了，并约定两年后方可使用这些私钥来非法获取用户的虚拟币，结果三个月后就被公安机关抓获归案。但对于欧某的损失，三人均供述称并未打破“约定”，提前非法获取虚拟币。经鉴定，三人共计非法获取助记词27000余条、私钥10000余条，成功转换数字钱包地址19000余个。

在充分对现有的证据进行研判后，承办检察官认定，刘某、张某甲、董某并未转走欧某的虚拟币，但三人的行为已构成非法获取计算机信息系统数据罪。经徐汇检察院依法提起公诉，徐汇法院作出如上判决。

幕后大盗浮出水面

刘某、张某甲、董某因自己的行为受到了法律的制裁。那么，究竟是谁动了欧某的虚拟币呢？承办检察官在讯问过程中，从三人的供词中发现了端倪，引导公安机关收集证据，进一步分析研判案情，最终锁定了这个虚拟币大盗。

原来，在欧某使用的另一个平台上的虚拟钱包软件中，也被曾就职于该公司的张某乙植入了后门程序。张某乙到案后交代，2021年7月，他利用自己的专业知识以及对虚拟币的了解，在客户端代码中编写了一段收集用户私钥和助记词的代码。当用户交易虚拟币时，代码就会自动获取用户进行签名操作所使用的助记词或私钥，并通过邮件形式发送到张某乙的邮箱。

2023年4月，张某乙因个人经济压力，就通过自己非法获取的助记词和私钥得知了欧某的虚拟钱包地址，将其中的虚拟币尽数转到自己的钱包地址中，并立刻转换成其他数字财产或虚拟币。经鉴定，张某乙共计非法获取用户私钥及助记词6400余条。经过检察官的法治教育，张某乙自愿认罪认罚，并在家人的帮助下，向欧某赔偿部分损失，获得了谅解。张某乙因犯非法获取计算机信息系统数据罪，最终获刑。

检察官提示 >>>

企业经营者在产品正式发布前，应进行充分的安全检测，特别是数字产品，如被植入恶意程序，不仅隐蔽性高，且危害性大，更应仔细排查。

相关开发者们要恪守职业道德，把自己的专业知识、技术用于正途，切勿因一时贪念，在自己负责的产品中加入类似本案中后门程序这样的非法牟利的“私货”，否则将面临严厉的法律制裁。

使用者们也要定期检查自己的资产情况，注意留存相关凭证，以备必要时可以依法维护自身权益。