网络创新:技术应用须划定合法边界

——上海法院解析新型网络犯罪相关案例

本报记者 郭 燕 本报通讯员 潘庸鲁

导读:

操纵虚假流量“刷量控评”、利用技术手段推送“流氓广告”、解析贩卖快递面单信息、发布伪原创“AI洗稿”内容牟利……技术的迭代与“流量经济”的兴起正催生出技术加持下的新型网络犯罪。近年来,依托数据要素和信息技术实施的此类犯罪手法不断翻新,呈现出犯罪手段技术化、对象数字化、场景生活化、形态产业化等新特点,对司法裁判提出全新挑战。为切实维护人民群众人身财产安全、规范网络空间秩序,上海法院梳理相关典型案例,聚焦技术创新与违法犯罪的界限、新型数据犯罪的司法认定、团伙犯罪量刑标准等关键问题,明确法律适用,着力提升网络犯罪打击与治理的整体实效。

案说·多元解纷

盗窃token等数据刷量控评

2022年9月起,李某通过网络先后招聘戎某微、姜某文、王某兵非法获取网站用户token、cookies数据。这些数据因具备身份认证功能、可用于登录用户网站账号,被李某等人用于给网站直播间刷人气以牟取非法利益。2023年5月,姜某文又招揽邹某能加入该团队。

其间,李某负责管理团队、对外招揽业务、联系兼职“地推”寻找用户下载重打包APP或者登录网站。戎某微负责编写脚本利用非法获取的网站用户token、cookies数据给直播间刷人气。姜某文负责对APP重打包,加入非法获取网站用户数据的代码,并设置将获取的数据自动上传至服务器。王某兵负责存储网站用户账号数据的服务器管理。邹某能负责新技术开发。经鉴定,涉案服务器中存储的token数据共计47219条、cookies数据共计1421条。公诉机关审查后,以非法获取计算机信息系统数据罪,对李某等五人提起公诉。

一审法院审理后认为,被告人李某等五人结伙,非法获取具有身份认证功能的计算机数据,情节特别严重,其行为均已构成非法获取计算机信息系统数据罪,且属共同犯罪。据此,法院以非法获取计算机信息系统数据罪分别判处被告人李某等五人有期徒刑三年二个月至一年,并处罚金人民币2万元至8000元。

宣判后,各被告人均未上诉,公诉机关亦未抗诉,判决现已生效。

法官提示

当前,“网络水军”操纵虚假流量、刷量控评等行为已形成庞大的黑灰产业链。本案中,犯罪分子通过重打包APP植入恶意代码,诱骗用户扫描二维码安装APP,在用户不知情的情况下窃取账号权限,用于为直播间刷人气牟利。此类行为损害了用户的账号安全,破坏了公平竞争的网络直播环境。本案判决明确非法获取token、cookies等数据的行为,构成非法获取计算机信息系统数据罪。

专家点评

李 翔

华东政法大学发展规划处处长、教授、博士生导师,上海市法学会案例法学研究会会长

token、cookies数据作为计算机信息系统运行过程中自动生成的身份认证凭证,不同于传统意义上的个人信息,通过唯一标识符与特定用户账号、自然人主体形成稳定关联,能够直接实现身份识别和账号登录,具备身份认证的核心特征,属于计算机信息系统数据范畴。本案裁判精准界分上述参数的法律属性,既避免将此类技术性数据排除在法律保护之外,也防止与个人信息不当混淆,彰显了刑法对计算机信息系统数据的专门保护。被告人重打包APP植入恶意代码、诱骗用户安装的行为,属于未经授权或超越授权获取数据的典型情形。本案判决为同类案件审理提供了明确的法律适用路径,也为网络黑灰产业的治理提供了司法参考,彰显了数字时代刑法对数据安全的独立保护价值,有助于构建多元数据治理体系,实现治罪与治理的统一。

劫持用户手机强推广告

A平台系某公司搭建的用于推广APP内商品、服务等项目的推广平台。平台用户在A平台注册后,可从平台获取推广链接并发布推广,当手机用户点击推广链接并成功购物后,推广者可获得推广佣金。推广佣金由商家支付。某公司基于商家授权负责提供技术服务,可从商家账户代划佣金给推广者。

2019年11月至2020年10月间,蔡某注册A平台推广账户后,与某视、某步等电商APP开发公司开展信息推广合作。蔡某在APP内配置SDK模块,手机用户安装运行上述APP时,会下载并运行蔡某编写的APK程序,实现手机用户在自行打开或者通过其他渠道唤起上述APP时,首先会被强制显示蔡某的A平台账户所关联的推广链接页面,用户购买商品后,蔡某即可获取佣金。蔡某以此方式获取推广佣金共计600余万元,提现200余万元。

2021年1月11日,蔡某被公安机关抓获,其到案后如实供述了主要犯罪事实。审理期间,蔡某在其家属帮助下,退出违法所得50万元。公诉机关审查后,以诈骗罪对蔡某提起公诉。

一审法院审理后认为,被告人蔡某利用计算机技术手段骗取他人财物,其行为已构成诈骗罪,且数额特别巨大。蔡某到案后如实供述了主要犯罪事实,依法予以从轻处罚。据此,一审法院以诈骗罪判处被告人蔡某有期徒刑十一年,剥夺政治权利一年,并处罚金人民币25万元。一审宣判后,蔡某提出上诉。

二审法院审理后认为,上诉人蔡某利用技术手段,非法控制用户手机完成相应指令,以牟取巨额推广佣金,其行为已构成非法控制计算机信息系统罪,且属情节特别严重。蔡某到案后能够如实供述自己的罪行,依法可以从轻处罚。据此,二审法院以非法控制计算机信息系统罪判处上诉人蔡某有期徒刑六年六个月,并处罚金人民币25万元。

批量解析贩卖快递面单信息

2024年8月至9月,彭某为非法牟利,伙同他人在未经某快递公司授权的情况下,非法侵入该公司计算机信息系统,批量解密快递单号,获取对应的明文数据后贩卖给他人。其间,彭某通过网络发布广告,招揽有解密需求的客户以及能够将单号解密为明文数据的上家,从中赚取差价,非法获利9000余元。

2024年8月,郭某烨为非法牟利,伙同他人通过网络发布信息招揽有解密需求的客户,在未经该快递公司授权的情况下,使用其在职公司IT部开发的自动化脚本及模拟器,非法侵入该快递公司后台服务器,批量解密快递单号,获取对应的明文数据后贩卖给他人,非法获利3万余元。经鉴定,郭某烨所使用的自动化脚本及模拟器,系专门用于查询和解密该快递公司系统内部收件人手机号、收件人姓名及收件地址。公诉机关审查后,以非法获取计算机信息系统数据罪,对彭某、郭某烨提起公诉。

一审法院审理后认为,被告人彭某、郭某烨违反国家规定,分别伙同他人采用非法技术手段获取计算机信息系统中处理的数据,其中,彭某情节严重,郭某烨情节特别严重,其行为均已构成非法获取计算机信息系统数据罪。据此,法院以非法获取计算机信息系统数据罪,分别判处被告人彭某有期徒刑一年,并处罚金人民币5000元;被告人郭某烨有期徒刑三年,并处罚金人民币2万元。

宣判后,两名被告人均未上诉,公诉机关亦未抗诉,判决现已生效。

法官提示

随着互联网的高速发展与数字经济领域竞争的日趋激烈,部分中小微企业将“流氓广告”等灰色业务作为获取经营收益的渠道之一,这不仅侵害了其他经济主体的合法权益,也推高了数字经济的信任成本,破坏了公平有序的市场经济秩序,理应受到法律的惩处。但此类案件又有一定的特殊性,即案件当事人通常还兼有中小微企业的技术人员、公司实控人等多重身份,基于成本控制及技术保护等因素,技术开发、应用、推广等工作“一肩挑”情况较为常见。在发展压力巨大的情况下,公司业务模式触犯刑法的现象时有发生,进而可能对公司发展造成毁灭性打击。因此,审理此类案件,首先需要精准剖析行为的本质,并在此基础上准确认定行为对计算机信息系统和网络竞争秩序的客观损害。其次要包容审慎,发挥司法的规范引导功能,推动数字经济平稳发展。

专家点评

李怀胜

中国政法大学刑事司法学院教授、博士生导师,网络法学研究所所长

组织利用AI洗稿

2023年11月至2024年5月,徐某、罗某雄、阚某奇结伙,合伙经营某信息科技有限公司。公司主要业务是从网上搜找、截取海量的热点文章、新闻,再通过AI软件下达“爆款标题”“重复率不得高于25%”等“洗稿”指令,将这些文章、新闻“洗稿”变成伪原创,然后将拥有网络自媒体平台账号的网民招募为学员,利用学员的账号发布伪原创的文章、新闻,赚取平台支付的流量提成后与学员五五分成。

其间,徐某作为公司实际控制人负责教授公司员工使用软件;罗某雄负责招募有自媒体平台账号的学员,指导学员发布“洗稿”后的热点文章、新闻;阚某奇负责公司员工的考勤、发工资、学员提成的分发,帮忙在网上搜找、截取热点文章、新闻并导入软件等。经审查,徐某、罗某雄、阚某奇等人通过上述行为,共计非法获利5万余元。公诉机关审查后,以非法经营罪对徐某等三人提起公诉。

一审法院审理后认为,被告人徐某、罗某雄、阚某奇结伙,违反国家规定,以营利为目的,编撰虚假信息并通过网络有偿提供发布,扰乱市场秩序,情节严重,其行为均已构成非法经营罪。据此,法院以非法经营罪分别判处被告人徐某、罗某雄、阚某奇有期徒刑一年十个月至一年六个月,均并处罚金人民币5万元。

宣判后,各被告人均未上诉,公诉机关亦未抗诉,判决现已生效。

法官提示

AI技术在提升社会生产力、提高人们生活工作便利性的同时,也被不法分子用于侵犯著作权,诈骗,编造、故意传播虚假信息,非法经营等违法犯罪活动。本案中犯罪分子先组织利用AI软件对热点文章、新闻进行搜找、截取并进行“洗稿”,后利用学员自媒体平台账号发布“洗稿”后的伪原创,获取平台流量提成。这种明知是虚假信息而提供有偿发布信息服务的行为,不仅严重扰乱信息网络服务市场秩序,也对社会秩序造成严重影响。

本案一方面明确组织利用AI“洗稿”并对“洗稿”后的虚假信息提供有偿发布的行为,应当认定为刑法第二百二十五条第四项其他严重扰乱市场秩序的非法经营行为,以非法经营罪定罪处罚;另一方面,也在AI技术快速发展的当下,明确技术的合理、合法使用边界。

人大代表点评

盛 弘

全国人大代表、上海市长宁区虹桥街道古北荣华第四居民区党总支书记

本案的被告人未经授权调用系统数据接口,使海量面单数据在极短时间内被批量窃取并贩卖,致使收寄件人的姓名、手机号、住址等信息外泄,不仅侵害众多消费者隐私与安宁,该信息还可能被用于诈骗等下游犯罪。一张小小的快递面单,承载的是个人信息的安全,更是千家万户的生活安宁。司法机关依法打击此类犯罪,捍卫了消费者数字生活中的隐私与安宁,对推动全链条信息保护治理格局构建具有重要示范引领作用。

专家点评

孙万怀

华东政法大学刑事法学院院长、教授、博士生导师

本案判决明确了利用人工智能技术进行“洗稿”所生成的“伪原创”信息的法律属性。此类信息虽经算法重组呈现原创表象,但其本质在于刻意隐匿或模糊信息来源,导致公众对信息真实性产生误解,具有扰乱信息网络服务市场秩序的实质危险性。行为人以营利为目的,规模化地通过信息网络向公众提供此类信息发布服务,直接侵害了国家对互联网信息服务依法实施的市场准入与内容管理秩序。“信息网络服务市场秩序”的保护对象,应当扩展至以信息真实性为基础的网络生态内容,这一新型市场法益值得刑法重点关注。技术工具的中立性并非刑事责任的当然阻却事由,刑法有必要也有能力穿透技术表象,依据行为的实质危害作出精准回应。这不仅有助于数据要素时代信息网络服务市场秩序的维护,也是人工智能产业规范、健康发展的司法保障。唯有在法律框架下明确非法与合法的界限,技术创新才能真正行稳致远。