拍案惊奇

利用“AI换脸”技术破解登录验证;利用职务之便盗用源代码转卖获利;利用平台漏洞购买万支胰岛素注射器。本期案例关注信息网络中的恶意行为,法官提醒广大看官,在信息爆炸、技术日新月异的今天,务必增强自我保护意识,妥善保管个人信息,警惕网络诈骗与非法入侵;同时,坚守职业道德与法律法规,不为一己私利触碰法律红线。

滥用“AI换脸”、盗用源代码、利用漏洞“薅羊毛”

网络有“脚印” 恶意行为难逃法网

以假乱真

●利用“AI换脸”破解认证
●五人篡改数据牟利被判刑

2022年4月,李某某通过网络购买培训教程及相关软件程序,掌握了利用他人个人肖像照片实现“AI换脸”伪造“眨眼”“摇头”等活体视频通过人脸实名认证、登录某服务平台系统个人账户的技术。

6月至次年2月,李某某先后招募孔某某及周某等人传授技术,随后又从符某某、陈某等中介处承揽非法人脸识别业务,同时采用“AI换脸”技术破解系统登录验证,由上家对系统内相应人员信息进行修改、增减,为多家公司非法牟利。

在此期间,孔某某加入李某某技术团伙开展非法人脸识别业务,8月又脱离团伙,先后招募王某等人另组团伙,从陈某、“坤哥”(在逃)等中介处承揽非法人脸识别业务继续作案。而陈某、符某某、陈某某作为中介,为两团伙提供客户资料。

经鉴定,缴获的各团伙成员手机、电脑中分别有公民个人信息七千至六万余条不等,非法获利从40万元至120万余元人民币不等。

■陈凤翔绘图

地点:广州市南沙区人民法院

结果:南沙法院一审判决被告人李某某、孔某某、符某某、陈某、陈某某犯非法获取计算机信息系统数据罪,判处有期徒刑三年八个月至三年三个月不等,并处罚金人民币十八万元至人民币四万元不等。宣判后,被告人李某某、孔某某不服,提起上诉。广州市中级人民法院二审裁定驳回上诉,维持原判。

法官说法:案件涉及非法侵入并篡改计算机信息系统数据,为非法公司牟利,触犯非法获取计算机信息系统数据罪。个人肖像照片属于个人信息保护法规定的生物识别类敏感个人信息,一旦泄露或者非法使用,易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。本案中,行为人通过“AI换脸”技术实现非法突破人脸识别认证目的,侵害了网络和个人信息安全。法官提醒,应强化个人信息权益保护,推进网络空间治理法治化。

贪小失大

●利用平台漏洞“薅羊毛” ●判决赔付差价30余万元

2021年6月,王某在网购平台上发现某药房胰岛素注射器标价0.01元漏洞,于是利用网络购物平台下单100份,工作人员发现该订单后,紧急电话联系王某告知价格标错,并将该订单取消。

同年12月,王某又利用平台可以通过“历史订单”页面以原价格重新购买订单的漏洞,分101次重复大量下单该产品,用101元的价格购得相应的注射器10100支。

药房诉至法院,认为买卖合同显失公平,要求撤销双方合同,王某返还相应的产品或折价补偿。王某则辩称双方的买卖合同已履行完毕,其不存在恶意刷单谋取非法利益的行为,故不同意赔偿。而且王某自己是药店经营者,产品已无偿送给众多顾客,无法返还。

地点:广州市越秀区人民法院

结果:案件审理过程中,越秀法院依法委托鉴定机构对涉案产品进行价格鉴定,鉴定机构出具的鉴定报告显示,王某购买的注射器总价为30万余元。法院认为,购物平台系统曾误将涉案产品标价为0.01元,王某在以该价格购买涉案产品后订单已被取消,王某已知该价格是标错的,但在半年后利用平台复购漏洞多次订立买卖合同,严重违背诚实信用原则并已构成显失公平,法院认定涉案合同属可撤销合同。最终,法院判决撤销双方买卖合同,并由王某向原告支付产品差价。

法官说法:本案涉及网络交易过程中“薅羊毛”行为引发的纠纷,争议焦点在于买卖合同是否构成显失公平。

王某明知系统标价错误,仍利用平台漏洞,批量购买上万支胰岛素注射器,远超正常需求,主观上显属恶意。另外,王某自称药店经营者,对相关产品的正常售价应有所了解,其购买价格与产品市场价相较甚远,客观上构成利益显著失衡。因此,王某的行为已构成显失公平,涉案合同应依法予以撤销。根据民法典规定,故王某则应当补回差价。

法官提醒,网络交易中,出卖人“刷单”、买受人“薅羊毛”等行为大量存在,对于违反诚信原则、扰乱交易秩序的行为应予以严格规制。就买受人而言,明知或应知对方系统漏洞的情形下仍坚持订约,将影响合同是否成立的认定,也应尽合理注意义务,以免得不偿失。

监守自盗

●利用职务盗用源代码获利
●六人构成侵犯商业秘密罪

2014年起,段某某、杨某某、李某甲、李某乙、李某丙、梁某某先后入职某物流有限公司,从事该公司物流系统的开发等工作,掌握了系统软件源代码等不为公众所知悉的信息技术,六人与公司签订了保密协议,约定了保密义务。

2019年4月,段某某、杨某某等人成立某科技有限公司,私下承接了一家供应链有限公司物流系统的开发项目,试图牟利。六人利用原物流公司的职务便利,盗用保密物流系统源代码等信息技术,通过复制、修改、添加、编写源代码的方式转卖获利,开发承接项目的物流系统。

其间,李某甲负责开发物流系统渠道对接模块;李某乙开发财务模块;李某丙开发客户订单管理系统;梁某某负责对物流系统进行测试,随后将开发完成的物流系统交付给这家供应链有限公司使用,收取费用共计659884.50元。

经鉴定,这套物流系统的源代码等技术信息与几人所在的物流有限公司的系统源代码构成实质性相似。

案发后,段某某等人主动向所在的物流有限公司进行赔偿,取得谅解,后向司法机关退缴违法所得共10万元。

地点:广州市黄埔区人民法院

结果:黄埔法院认为,被告人段某某、杨某某、李某甲、李某乙、李某丙、梁某某违反权利人有关保守商业秘密的要求,使用其所掌握的商业秘密,情节严重,其行为均构成侵犯商业秘密罪。

根据各被告人的犯罪事实、性质、情节及对社会的危害程度,法院依法对几人分别判处有期徒刑一年六个月至一年二个月不等的刑期,均宣告缓刑,并处罚金。同时判处没收违法所得及作案工具。该判决现已生效。

法官说法:商业秘密是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。作为企业生存与发展的无形资产,权利人依法对商业秘密享有专有权。根据法律规定,违反保密义务或者违反权利人有关保守商业秘密的要求,披露、使用或者允许他人使用其所掌握的商业秘密,系侵犯商业秘密行为,情节严重,构成犯罪。

■采写:新快报记者 高克 毛毛雨 通讯员 王君 郭馨 朱姝 梁艳华