

提供避开人脸识别认证功能程序行为的定性

文/施月玲 朱文菁

【裁判要旨】 认定提供侵入、非法控制计算机信息系统程序、工具罪时，应在承认计算机信息系统内涵扩展的基础上，对所提供程序、工具的标准从技术门槛和规范目的上予以限定。其中，认定“专门程序”应考察其技术手段与实施目的是否高度一致——即是否未经或超越授权，通过计算机技术突破或避开系统安全保护措施以实现侵入、控制计算机信息系统或非法获取数据的目的。人脸识别验证属于计算机信息系统的验证措施，用技术手段使其被规避应当被视为对系统安全的侵害。

□案号 一审：(2024)沪0109刑初714号

【案情】

公诉机关：上海市虹口区人民检察院。

被告人：苏某杰。

2022年，被告人苏某杰针对安卓手机操作系统研发“虚拟相机”软件，通过突破安卓系统的安全防护机制，对手机相机功能进行未经授权修改，干扰系统相机的正常运行，以实现绕过“某手”“某音”等软件人脸识别实名认证的目的，并通过网络销售上述软件获利。经查，2023年8月至2024年3月，苏某杰获利共计USDT16万余枚，相当于人民币114万元左右。

2024年4月8日，被告人苏某杰在

福建省厦门市被公安人员抓获，到案后如实供述了上述犯罪事实。

【审判】

虹口区人民法院经审理认为：被告人苏某杰提供专门用于侵入、非法控制计算机信息系统的程序，情节特别严重，其行为已构成提供侵入、非法控制计算机信息系统程序罪。公诉机关指控被告人苏某杰犯提供侵入、非法控制计算机信息系统程序罪罪名成立。关于被告人苏某杰的辩护人提出被告人苏某杰不属于情节特别严重的辩护意见，经查，被告人苏某杰因提供涉案“虚拟相机”获得共计逾百万元的违法所得，符合相关司法解释关于“情节特别严重”的规定，被

告人苏某杰到案后能如实供述自己的罪行，退缴全部违法所得，自愿认罪认罚，可以分别依法从轻、从宽处罚并适用缓刑。故判决：一、被告人苏某杰犯提供侵入、非法控制计算机信息系统程序罪，判处有期徒刑3年，缓刑4年，并处罚金8万元。二、退缴的违法所得连同缴获的被告人苏某杰的电脑一台、手机16部予以没收。

一审判决作出后，被告人苏某杰未上诉，检察院未抗诉，判决已发生法律效力。

【评析】

本案系提供侵入计算机信息系统程序的新型“黑客”案件，行为人并没有主动侵入计算机信息系统，而是

案例

设计出替换实时拍摄功能的软件进行售卖,该程序后被证实用于突破人脸识别规则进行新用户注册获得平台返佣。本案的争议焦点在于该行为的定性,对此,有三种不同的观点:

第一种意见认为,被告人不构成犯罪。软件作用于使用者的手机客户端,并不属于计算机信息系统。且其提供的是一种中性的技术工具,本身具备合法使用场景,比如直播时可以将实时拍摄的画面切换为相册里保存的视频从而节省人力资源,提供者无法预知或控制购买者的具体使用方式,并且软件不会对计算机信息系统造成损害,不具有危害性。

第二种意见认为,被告人构成非法控制计算机信息系统罪的共犯。其提供的软件对手机自带的相机功能进行屏蔽,避开了安卓系统的安全防护策略,如无其帮助,则仅掌握他人身份信息的罪犯无法绕过人脸识别验证进行虚假身份注册从而获得平台返佣,被告人属于非法控制计算机信息系统罪的共犯。

第三种意见认为,被告人构成提供侵入、非法控制计算机信息系统程序罪。其通过出售软件获利,而该软件可用于避开相关软件基于安卓系统安全防护策略设立的人脸识别规则,达到非法控制计算机信息系统的目的。

笔者赞同第三种意见,具体理由如下:

一、计算机信息系统的范围应涵盖联网状态下的移动终端及其应用程序

在非破坏性的针对计算机信息系统犯罪中,我国刑法主要针对行为人为人实施侵入、非法控制计算机信息系统或非法获取计算机信息系统数据的行为进行规制。除了国家事务、国防建设、尖端科学技术领域三个涉及国家安全的领域外,对于其余计算机信息系统,构成犯罪的还需符合情节严重的标准。

计算机信息系统的概念在实务中随着技术发展不断扩展,2011年9月1日起施行的最高人民法院、最高人民检察院《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(以下简称《司法解释》)采用了概括加列举的解释方法,将“计算机信息系统”“计算机系统”界定为“具备自动处理数据功能的系统,包括计算机、网络设备、通信设备、自动化控制设备等”。在联网环境下,手机软件或者小程序属于计算机信息系统的范畴,其在客户端、服务器端和通信传输端的协同架构下运行,三端间实时数据的交互、处理符合自动处理数据的逻辑,形成了一个完整的计算机信息系统运作闭环。

本案中,被告人研发的“虚拟相机”软件的主要功能在于以播放手机内已存储的视频文件的方式,对手机原生相机拍摄的视频进行替换。以创

建“某手”软件新账号为例,“某手”软件在发起人脸识别实名验证请求时,首先向手机操作系统(OS)请求相机使用权限,手机操作系统通过相机服务器分配手机的存储器用于存储相机所拍摄的视频,“虚拟相机”利用钩子函数(hook)劫持并替换存储器中的视频,通过将事先存储的他人身份信息回传给“某手”软件,再由“某手”软件传输至“某手”服务器,完成实名认证。在整个交互过程中,“某手”的后端服务器、前端软件、与手机通过网络形成了一个密不可分整体。因此,从犯罪对象上看,“虚拟相机”软件侵入的对象为联网状态下的手机软件,而其正被计算机信息系统的范畴所涵盖。

二、“专门程序”的认定应兼顾技术特征与行为目的的双重判断标准

根据刑法第二百八十五条第三款规定,提供者入罪途径有二:一是“提供专门用于侵入、非法控制计算机信息系统的程序、工具”;二是“明知他人实施侵入、非法控制计算机信息系统的违法犯罪而为其提供程序、工具”。为行文简洁,笔者以下将其简称为“专门程序”和“其他程序”。

虽然法条原文仅列举了侵入、非法控制的功能,但是通过体系解释,刑法第二百八十五条规制的内容应当覆盖非法获取计算机信息系统数据的行为。从规范目的看,提

① 喻海松:“《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》的理解与适用”,载《人民司法》2011第19期。

供的程序、工具的违法性在于其具有侵入、非法控制以及非法获取数据任一功能。^①无论是“专门程序”还是“其他程序”，其客观归责基础在于该程序在实际使用中实现了上述任一功能。

以“其他程序”入罪时，需结合程序的实际使用场景和提供者的明知程度。一般而言，“其他程序”原本的开发场景合法，比如搭建普通网站，但是在使用场景上具有明显不正当性，即该网站通过编辑可高度模仿某官网界面、较易使大部分用户产生误解。当开发者明知他人要利用该网页欺骗用户身份认证信息，使用目的上具有非法获取计算机信息系统数据的故意，便可通过提供“其他程序”追究开发者的刑事责任。

“专门程序”相较于“其他程序”，具有两方面的特征：一是在功能实现上体现出对计算机信息系统安全防护措施的突破性与针对性；二是使用目的与功能实现上高度统一。《司法解释》第2条对专门程序进行了分类，包括“（一）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能的；（二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；（三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具”。简言之，此类程序通过未经系统主体

授权，或超越既有授权范围的技术操作，绕过系统安全防护的核心机制，从而达到侵入、非法控制或非法获取数据的任一目的。从定义上看，“专门程序”在技术手段与行为目的之间呈现出紧密的连贯性与一致性，其技术特征本身即服务于违法目标的实现。

在计算机信息系统中，人脸识别实名认证应当被认定为安全保护的必要措施之一。在计算机信息系统认证端，用户真实身份的验证是防止未经授权访问的关键措施，构成访问控制机制的核心。该验证一是提升了系统准入环节的安全性，用以遏制身份盗用和账户共享的风险；二是增强了平台对用户管理的精确性，使得系统能够针对未成年用户实施使用时长限制，或是防止被封禁用户重新使用服务。

实时拍摄是人脸识别验证的必要环节，本案被告人所提供的“虚拟相机”程序，在技术上实现与绕过人脸识别实名认证规则高度关联。该程序未经计算机信息系统授权，非法控制视频流的传输过程，对输入平台的实时拍摄数据进行篡改，使用目的直接指向突破人脸识别实名认证机制。因此，该程序在技术特征和实施目的上违法性高度一致，应被认定为刑法意义上的“专门程序”。

三、缺乏意思联络的程序提供行为不构成非法控制计算机信息系统的共犯

根据我国刑法共同犯罪理论，构

成共犯需具备双重要件：一是客观上存在协同配合的实质性帮助行为；二是主观上具有明确的共同犯罪故意。在非法控制计算机信息系统罪中体现为主观上具有非法控制计算机信息系统的犯罪故意，同时存在意思联络，对各自实施的行为以及其余行为人的犯罪行为相互期待。^①如提供者仅为他人利用信息网络实施犯罪提供技术支持，并未与实行者之间就具体犯罪事项的合意，则不宜被认定为非法控制计算机信息系统的共犯。网络空间中的信息技术支持行为相较传统犯罪的帮助行为更具独立性，法律选择将提供者入罪正是帮助行为正犯化的典型。在缺少事前通谋的情况下，对提供功能违法性明确的程序以提供程序罪入罪，应当为立法选择的应有之义。

技术程序的价值具有双向性特征，有时会处于罪与非罪的灰色地带。中立帮助行为如提供开源代码、通用算法等基础技术，若未针对具体犯罪场景优化，一般不宜认定构成本罪。而判断技术支持者责任的关键在于考察程序、工具的属性定位与使用指向：标准化、开放式工具因具有广泛的适用场景，通常被视为中性技术开发行为；针对特定系统漏洞开发或者违法功能指向明确的工具，即使缺乏与特定罪犯的意思联络，同样可能以提供“专门程序”入罪。

从主观方面看，本罪并非法定的目的犯，被告人可以持有间接故意的态

^①刘畅、吴倩：“非法控制计算机信息系统罪的构成”，载《人民司法》2021年第23期。

案例

度,即明知自己提供行为可能会造成危害计算机信息系统安全的后果,但依然放任该危害后果发生。^①本案被告人将研发的“虚拟相机”软件放在外网出售,系因曾在国内售卖软件时遇到了各平台的警告和下架处理,主观上对他人可能利用该软件实现违法目的有一定了解。被告人以售卖软件的使用激活码为主要目的,并未通过设立境外购买门槛以外的方式筛选出售对象,缺少与实行者非法控制软件注册新用户达到获取平台返佣的合意。同时其销售金额超过100万元,达到了情节特别严重的标准,因此笔者认为其并不属于非法控制计算机信息系统的共犯,而是构成典型的提供侵入、非法控制计算

机信息系统程序罪。

值得强调的是,计算机信息网络的每一次突破,都不可避免地面临灰色地带的挑战。在具体量刑上,也应对技术提供行为秉持审慎处理的态度,综合考量其主观目的与客观危害,结合相关软件是否突破支付环节的人脸验证规则,以及是否有证据证明突破人脸识别后生成的账号被用于电信网络诈骗等其他违法犯罪行为,以判断其次生危害的严重程度。同时,还需结合被告人的认罪悔罪态度、退赃退赔情况及其在共同犯罪中的地位与作用等,合理确定基准刑。本案中,被告人苏某杰为家人治病想到贩卖软件牟利,到案后能如实供述

全部犯罪事实,主动配合查清案件经过,并退出全部违法所得,显示出较强的悔罪意愿。其开发、提供“虚拟相机”程序虽具有一定社会风险,但未有证据证实被用于诈骗等造成次生危害,主观恶性和实际危害均相对较轻。综合其犯罪动机、手段及悔罪表现,具备依法适用缓刑的基础。

在司法裁判活动中,既要通过刑事制裁的威慑效应来遏制技术的滥用,又要保持必要的谨慎和克制,避免用刑事手段对技术革新者不当施压,从而在保障维护网络空间秩序的同时护航科技进步。

(作者单位:上海市虹口区人民法院)

^①苏家成:“提供侵入、非法控制计算机信息系统程序、工具罪的认定”,载《人民司法》2013年第12期。