

DOI:10.19684/j.cnki.1002-4603.2026.12.026

利用“AI换脸”技术侵入计算机信息系统的行为定性

文/潘银幼（一审承办人） 郑玲玲 郑桂艳

【裁判要旨】 通过软件干扰或控制相关平台的人脸识别系统，让平台绕过实名活体检测，读取预先制作的“AI换脸”视频，进而通过平台人脸验证，侵入计算机信息系统。该行为系对计算机信息系统实施干扰、控制，应当认定为刑法第二百八十五条第二款“采用其他技术手段”非法控制计算机信息系统的行为。

□案号 一审：(2023)闽 0502 刑初 547号

【案情】

公诉机关：福建省泉州市鲤城区人民检察院。

被告人：傅某海。

泉州市鲤城区人民法院经审理查明：为牟取非法利益，傅某海在网上发布“AI换脸”广告，招揽需要利用他人身份信息通过平台人脸验证的客户。傅某海通过网上购买的软件，利用客户提供或自己从网上购买的公民信息，制作“AI换脸”视频，并将“AI换脸”视频预存在手机相册中，采用软件控制相关平台的人脸识别系统，让平台读取其指定的“AI换脸”视频，以此通过平台的人脸验证。2023年6月至8月初，傅某海单独或伙

同他人利用上述手段，帮助他人成功注册某短视频平台账号2000余个，非法获利7000元；2023年7月至8月，单独或伙同他人利用上述手段成功帮助客户通过某微信小程序人脸验证，并成功申购某品牌白酒至少90单，非法获利2万元。2023年8月，傅某海被抓获归案，后主动退缴全部违法所得，并预缴罚金。

公诉机关认为被告人傅某海应当以非法控制计算机信息系统罪追究刑事责任。

被告人傅某海对公诉机关指控的主要犯罪事实不持异议，对公诉机关指控的罪名有异议。被告人傅某海的辩护人提出：1.被告人傅某海并未让平台无法识别当前验证的视频信息，只是借助软件使系统读取到其预先制

作的人脸视频，并没有“控制”相关平台的人脸识别系统；2.被告人傅某海帮助他人通过实名认证的行为并不足以被定罪，应当就其购买和使用公民个人信息的行为以侵犯公民个人信息罪进行追究；3.所指控的被告人傅某海的非法获利应扣除其为了犯罪所支出的购买软件和学习费用；4.被告人傅某海系初犯、偶犯，具有坦白情形，其家属也代为退出违法所得并预缴罚金。综上，建议以侵犯公民个人信息罪对被告人判处1年以下有期徒刑，并适用缓刑。

【审判】

鲤城区法院经审理认为：被告人傅某海在帮助客户通过人脸验证的过

程中,使用软件让平台未能进行实名活体检测,而是读取其预先制作的“AI换脸”视频,其行为并未对平台的后台数据进行删除、修改、增加等,也未造成相关平台的计算机信息系统不能正常运行,而是对平台的后台系统进行干扰,该行为更接近为对后台系统的控制行为,故该行为符合非法控制计算机信息系统罪的犯罪特征,应认定为非法控制计算机信息系统罪,而非破坏计算机信息系统罪。被告人傅某海的行为也构成侵犯公民个人信息罪。被告人傅某海帮助客户进行人脸验证的身份信息均为其他公民的身份信息,该信息来源包括客户提供的他人信息,以及其自己根据客户提供的他人公民身份证号码等信息到网上购买的完整公民身份信息,被告人傅某海制作“AI换脸”视频并借此通过平台验证,未经验证人本人同意,且公民身份信息来源并非合法,故被告人傅某海的行为构成侵犯公民个人信息罪。被告人傅某海的犯罪行为同时构成非法控制计算机信息系统罪和侵犯公民个人信息罪,因两罪的关系是手段与目的的牵连关系,应择一重处罚。由于两罪均以非法所得作为入罪条件和情节的认定,根据查明事实,被告人傅某海的犯罪行为构成非法控制计算机信息系统罪重于侵犯公民个人信息罪,故依法应以非法控制计算机信息系统罪定罪处罚。综上,被告人傅某海违反国家规定,单独或伙同他人对“国家事务、

国防建设、尖端科学技术领域”之外的计算机信息系统实施非法控制,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。被告人傅某海辩解其行为不构成该罪及其辩护人辩解被告人应以侵犯公民个人信息罪判处等意见,不能成立,不予采纳。被告人傅某海辩称其违法所得应扣除其为了实施犯罪行为而学习的费用,没有依据,不予采纳。被告人傅某海系坦白,全部退赃,并预缴罚金,予以从轻处罚。鲤城区法院遂判决:被告人傅某海犯非法控制计算机信息系统罪,判处有期徒刑3年,并处罚金5000元;已退出的违法所得2.7万元,予以没收,上缴国库。

一审宣判后,没有上诉、抗诉,判决已发生法律效力。

【评析】

本案系滥用“AI换脸”技术引发的新型网络犯罪。核心争议焦点在于,利用“AI换脸”技术规避平台活体检测并完成验证的行为是否属于危害计算机信息系统犯罪,以及该行为应认定为破坏计算机信息系统罪还是非法控制计算机信息系统罪。对此,应当紧扣危害计算机信息系统犯罪的构成要件,结合计算机信息系统认定标准与罪名界分规则开展综合分析。

一、计算机信息系统的审查认定

《计算机信息系统安全保护条例》(2011年)第二条规定:本条例

所称的计算机信息系统,是指由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。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》(法释〔2011〕19号)第11条第1款规定:本解释所称“计算机信息系统”和“计算机系统”,是指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。

根据上述术语解释,有些观点认为,计算机信息系统特指内置可编程、可安装程序的操作系统的数据化、智能化设备,^①是硬件载体与软件程序的有机集成,必须以计算机及相关配套设备、设施为物理依托。单纯的计算机软件即便具备自动数据处理功能,若脱离硬件载体支撑,也无法独立构成计算机信息系统。

但随着云计算、大数据、物联网技术深度普及,云计算、云服务器、虚拟主机等新型数字载体成为行业主流,企业与个人通过云端租用数据处理空间、依托专用软件完成数据处理已成为常态化模式,具备自动数据处理功能的系统早已突破实体硬件的单一范畴。从司法实务看,侵害计算机信息系统安全的行为,也大多针对软件程序、系统功能实施,直接损毁硬件设备的案件反而占比极低。

因此,笔者认为,判断是否属于

^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年第19期。

计算机信息系统，应将具备自动数据处理基础功能作为核心认定前提。具体而言，对于手机、电脑、DNS服务器、物联网终端等实体硬件，判定是否属于计算机信息系统，核心核查其是否具备自动数据处理功能。比如工业自动化控制设备、智能终端设备，即便不属于传统计算机，只要满足数据自动处理要件，即可认定为计算机信息系统。对于网站、手机APP、云端应用程序、小程序等软件载体，则注意整体看待，以用户终端、服务端、网络通讯端三大模块为框架，梳理软硬件协同关系，避免割裂看待软件与载体。例如域名解析服务器劫持、APP非法篡改、云端数据删除等行为，均是对完整计算机信息系统的侵害，需结合系统整体功能受损情况认定案件事实。

二、刑法第二百八十五条中“非法控制”行为认定及罪名界分

当前，刑法及相关司法解释对刑法第二百八十五条中“非法控制”的客观表现形式未作具体界定，司法实践中普遍认为“非法控制”是指行为人通过技术手段使计算机信息系统脱离所有权人或管理人的掌控，转而由行为人主导其运行，既包括对整个系统的完全控制，也包括对系统部分功能、程序或数据的非法操控。

值得注意的是，在审理危害计算机信息系统犯罪过程中，要重点区分“破坏”与“非法控制”两个

犯罪行为。

从刑法第二百八十六条列举的破坏计算机信息系统罪的三种行为模式上看，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加、干扰等操作属于该罪的罪状。但从实际情况上来看，无论是要“非法控制”还是“破坏”计算机信息系统，行为人都需要先侵入计算机信息系统，取得浏览、修改、增加、删除、替换等权限，从而取得计算机信息系统的暂时控制权，或是彻底影响计算机信息系统的正常运行。由此可见，“非法控制”与“破坏”实质上具有行为关联性：非法控制往往伴随着破坏性操作，而破坏性行为又必然包含非法控制的要素。从行为逻辑来看，对计算机信息系统的非法操控是实施破坏行为的必要前置条件，破坏行为的实施过程必然包含对系统权限的非法获取与维持。这种双重属性使得两种违法行为在技术实现层面存在深度交织，形成互为表里的关系特征。有学者因此认为，“破坏”是“非法控制”的程度深化和较为极端的表现形式，规定非法控制计算机信息系统罪的法条是一般性法条，破坏计算机信息系统罪的法条是特殊性法条。^①二罪并不是对立关系。对计算机信息系统功能进行删除、修改、增加、干扰，或对系统内数据、应用程序实施删改增添操作，

完全可能同时契合“非法控制”的行为特征，仅依据操作行为本身，无法区分非法控制计算机信息系统罪与破坏计算机信息系统罪。

笔者认为，区分“非法控制”与“破坏”，核心在于判断行为是否对计算机信息系统功能造成实质性破坏或导致系统无法正常运行。计算机信息系统被“非法控制”后，虽功能发挥会受到一定程度的妨害，但“非法控制”状态一旦消除，系统通常可自动恢复原状，原权利人对计算机信息系统的使用便不再受非法阻碍。而“破坏”计算机信息系统的行为，往往直接冲击系统核心运行功能，影响数据处理准确性，实践中多表现为系统崩溃、运行中断、强制卡顿、响应迟缓等不可逆或持续性故障。从司法实务上说，主流观点亦认为是否对计算机信息系统功能造成实质性破坏或者无法正常运行是区分二罪的实质条件。最高人民法院指导案例145号张某某等非法控制计算机信息系统案认为，被告人虽对目标服务器的数据实施了修改、增加的侵权行为，但未造成该信息系统功能实质性的破坏，或不能正常运行，也未对该信息系统内有价值的数据进行增加、删改，其行为应认定为非法控制计算机信息系统罪。人民法院案例库入库案例何某骏等非法控制计算机信息系统案（入库编号：2023-04-1-252-001）认为，破坏计算机信

^①孙道萃：“‘流量劫持’的刑法规制及完善”，载《中国检察官》2016年第8期。

息系统的客观方面表现为违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行;或者对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,或者故意制作、传播计算机病毒等破坏性程序,影响计算机系统的正常运行,后果严重的行为。前者的核心在于未经授权或超越授权控制计算机实施特定的操作,而后者的关键在于造成计算机系统不能正常运行或者影响计算机系统正常运行。

综上所述,实务界的主流观点认为,通过修改、增加计算机信息系统数据,对该计算机信息系统实施非法控制,但未造成系统功能实质性破坏或者不能正常运行的,不当认定为破坏计算机信息系统罪,符合刑法第二百八十五条第二款规定的,应当认定为非法控制计算机信息系统罪。

三、利用“AI换脸”技术规避平台活体检测并完成验证的行为,应认定为非法控制计算机信息系统罪

人脸识别认证系统是以人脸生物特征为识别依据,通过图像采集、人脸检测、特征提取、活体校验与特征比对等技术,自动核验当前使用者身份是否与预存身份信息一致的身份核验系统,其具备自动数据处理功能,符合计算机信息系统的特征。同时,人脸识别认证系

统是用于保护用户操作系统,或者将人脸识别认证作为检验身份信息的计算机信息业务系统,故其属于计算机信息系统。

司法实务中,影响人脸识别系统的类型主要有:一是物理欺骗型,即通过化妆或使用道具等手段伪装合法用户的面部来骗过人脸识别系统,从而突破人脸识别认证;^①二是图像替换型,即通过软件使人脸识别认证系统读取事先制作的3D人脸视频,从而完成人脸实名认证;三是技术破解型,通过技术手段替换或篡改系统中各种关键模块或数据,从而突破人脸识别的限制。^②本案中,被告人傅某海的犯罪行为即属于上述图像替换型。该行为通过使用软件改变人脸识别认证系统的运行模式,影响计算机信息系统的正常运行和功能实现,具有侵害计算机信息系统安全的效果,其行为应评价为危害计算机信息系统犯罪。在具体罪名认定上,应从主观目的、客观行为及侵害后果进行综合认定。从主观目的看,被告人傅某海的核心目的是借助技术手段帮助他人通过人脸验证、牟取非法利益,为完成平台账号注册和商品申购,其需确保涉案平台、微信小程序的后台计算机信息系统正常运行,而非破坏其系统功能;从客观行为和侵害后果看,傅某海的行为仅干扰了系统的摄像头调用功能,未对系统后

台数据进行删除、修改、增加,也未造成系统无法正常运行,在退出第三方软件后,短视频平台、微信小程序可恢复正常使用,侵害程度未达到对计算机信息系统功能造成实质性破坏或者无法正常运行的程度。综上,傅某海的行为符合“非法控制”计算机信息系统罪的犯罪特征,应认定非法控制计算机信息系统罪,而非破坏计算机信息系统罪。

需要注意的是,被告人傅某海在破解人脸识别认证系统时,需要预先制作“AI换脸”视频,这个过程涉及窃取或以其他手段非法获取他人身份证件号码等其他公民个人信息的行为,侵害了公民的个人信息法益,根据傅某海的犯罪数额,应认定傅某海的行为同时构成侵犯公民个人信息罪。因傅某海的犯罪目的是破解人脸识别认证系统,从而完成账户注册或获取商品申购资格,制作“AI换脸”仅是破解人脸识别认证系统的手段,两犯罪行为存在手段与目的的牵连关系,根据牵连犯“择一重罪处罚”原则,结合本案被告人傅某海非法获利数额及犯罪情节,非法控制计算机信息系统罪处罚更重,最终法院以非法控制计算机信息系统罪对被告人傅某海进行定罪量刑。



(作者单位:福建省泉州市鲤城区人民法院)

①李高伦:“破解人脸识别认证行为的刑法规制”,载《社会科学动态》2023年第11期。

②纪康:“影响人脸识别系统案件的刑法认定”,载2022年9月5日《中国社会科学报》。