Dispute Settlement 争议解决, 2026, 12(2), 190-197
Published Online February 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.122060

Hans汉斯

AI换脸视频侵权行为的法律规制研究

胡金旭

青岛大学法学院，山东 青岛

收稿日期：2026年1月10日；录用日期：2026年2月3日；发布日期：2026年2月14日

摘　要

本文以人工智能时代的“AI换脸”(深度伪造)技术为研究对象，系统梳理了其发展历程、社会影响与潜在风险。文章指出，该技术虽在影视创作、文化传播等方面具有积极价值，但也引发了侵犯肖像权、隐私权、名誉权及著作权等问题，并可能扰乱社会秩序、破坏信息安全。通过对美国、欧盟等域外法律规制经验的比较分析，本文总结了我国现有法律在应对AI换脸侵权方面的不足，包括立法层次较低、专门法律缺失等。在此基础上，文章提出我国应加快专门立法进程，明确各主体责任，强化技术标识与平台监管，以平衡技术发展与权益保护，构建适应数字时代的法律规制体系。

关键词

AI换脸，深度伪造，法律规制，侵权，肖像权

Research on the Legal Regulation of Infringements in AI Face-Swapping Videos

Jinxu Hu

Department of Law, Qingdao University, Qingdao Shandong

Received: January 10, 2026; accepted: February 3, 2026; published: February 14, 2026

Abstract

Focusing on AI face-swapping (deepfake) technology in the age of artificial intelligence, this paper systematically examines its development, social impact, and potential risks. It points out that while the technology holds positive value in areas such as film production and cultural dissemination, it also raises issues such as infringement of portrait rights, privacy rights, reputation rights, and copyrights, and may disrupt social order and undermine information security. Through a comparative analysis of legal regulatory experiences in regions such as the United States and the European Union, this paper summarizes the shortcomings of China's existing legal framework in addressing AI face-

文章引用: 胡金旭. AI 换脸视频侵权行为的法律规制研究[J]. 争议解决, 2026, 12(2): 190-197.
DOI: 10.12677/ds.2026.122060

swapping infringements, including insufficient legislative coverage and the lack of specialized laws. On this basis, the paper proposes that China should accelerate the process of enacting specialized legislation, clarify the responsibilities of various parties, strengthen technical labeling and platform supervision, so as to balance technological development with the protection of rights and interests, and construct a legal regulatory system suited to the digital age.

Keywords

AI Face-Swapping, Deepfakes, Legal Regulation, Infringement, Portrait Rights

1. 引言

随着信息时代的不断更迭，一个数据化的新时代早已悄然到来。信息生产与信息传播的工具也在不断升级换代，人工智能技术的发展壮大为信息传播方式和内容带来新的可能。2019 年，一股“AI 换脸”的潮流将“深度合成”技术带到大众面前。在新媒体时代，它极大满足了人们娱乐的需求。但是技术红利和伦理隐患从来都是形影相随，如果没有完善且有效的规制体系来解决新生事物的侵权问题，那么无论是对技术本身还是对国家社会都会产生负面作用。因此，梳理 AI 换脸技术发展的来龙去脉，辩证分析其存在的合理性和产生的各类问题，在借鉴其他国家的规制经验的基础上，填补好我国在该领域的立法空白，是我们刻不容缓要做的工作。

2. AI 换脸视频技术概述

(一) AI 换脸视频技术

1、AI 换脸技术的发展历程

换脸视频其实是使用了一种名为“深度伪造”技术后的音像产物。这种技术本质上是利用了一种 AI 人工智能技术，从而进行合成并且伪造图像和声音，最终呈现出了某人做了某事的假象。

虽然现在看来这种技术已经屡见不鲜，但是这种技术却是存在已久。自上世纪六十年代，这种技术就已经被尝试在影视行业使用，一些好莱坞电影使用这种面部伪造技术以呈现不可能出现的场面。比如于 1994 年上映的经典电影《阿甘正传》中，出现了肯尼迪与阿甘握手的画面，这在现实是不可能实现的。事实是先拍摄了汤姆汉克斯和别人握手的画面，再找到肯尼迪与一个矮小的女人握手的早期视频，最后利用这项技术将汤姆汉克斯的形象覆盖在这个女人身上。虽然呈现出的效果比较模糊，但在当时是重大的技术突破，最终在当年的奥斯卡颁奖礼上，该片凭此获得了特技效果奖。在早期，此项技术的应用规模较小，这是因为使用成本比较昂贵，需要投入大量金钱和时间成本。随着“深度伪造”技术的不断改善和进步，面部伪造技术进化的更加简易，逐渐在社交网络流行起来。

第一次恶意使用深度伪造技术出现在 Reddit 上，像斯嘉丽·约翰逊这样的女演员的脸被植入淫秽视频。一名昵称为 Deepfake 的用户深入学习并掌握了该技术，不过他并没有用于正途，而是以更换成人影片中女主角的脸为乐，第一个中招的正是好莱坞当红女星盖尔加朵，由此引起了一场轩然大波。这项技术代码经过开源之后，Deepfake 技术走向流行。国内的流行稍稍滞后于国际，国内的这阵热潮首先掀起在年轻人比较多的视频平台哔哩哔哩弹幕网。94 版朱茵饰演的角色黄蓉早已深入人心，一段将朱茵换脸

黄蓉的影视片段在该平台迅速走红。而后这条视频的结局是因为侵犯他人肖像权而下架，在互联网上引发了激烈地讨论。在这之后，一个个更加方便于换脸的应用软件如雨后春笋般冒出。能够“一键换脸”的Fake App和“一键脱衣”的Deep Nude相继推出，2019年，我国也出现了第一款相类似的软件“ZAO”。之后换脸类视频蜂拥出现，在带给大众娱乐的同时，也带来了极大的法律风险。私下制作“AI换脸”视频无可厚非，若是将这些视频传播到互联网上，则会损害当事人的肖像权等合法权益，也会增加社会犯罪风险[1]。任何新生事物在最初都是野蛮生长的，AI换脸技术也不例外，因为法律是具有滞后性的。一项技术它本身是无罪的，如果解决不好相关的侵权规制问题，它会限制一项技术的发展。但是这并不意味着完全没有对策，对于技术的规制并不会没有超出法律体系的范围。要不要对其进行规制的问题已经解决，接下来主要解决的是如何对其进行规制的问题。

2、AI换脸技术的合理性

AI换脸技术的出现的起点是为了影视作品的拍摄和后期制作而生的，在影视相关领域给后期特效制作和某些画面的呈现提供了极大的便利，尤其是在早期影视发展起步时期起到了重要作用，因此它是一项科技进步。对于视频作者来说，它是在互联网时代中一个自由输出观点，发挥自身想象力和创造力的工具。对于文化传播和交融甚至创新来说都是新颖且有趣的。相比较于文字、图片、声音等传统信息传播方式，AI换脸视频是一种动态的形式，顺应着抖音、快手、B站等短视频迅速崛起的这股热潮，生动地向大众传播制作者的想法。

另外，细数最近几年的热门社会爆点，会发现在社交娱乐场景、在电影电视制作发行领域、最近兴起的线上教育领域以及产品营销等领域，各种关于人工智能的关键词渐渐成为互联网热点，并且不断衍生出各式各样的商业级移动应用。种种成功创业的新潮，都是深度合成技术发挥作用的结果。这些商业应用渐渐转化为商业价值，推动了新经济发展，出现了相关新业态。深度合成技术激发了新内容创造力。在AI类型娱乐全速发展的21世纪，经过不断探索和数轮淘汰以及更新换代的深度合成技术，在维持技术始终属于最新的前提下，不断下降使用的成本，可以预测到此项技术在人工智能生活场景应用的发展前景较为广阔。

3、AI换脸技术带来的问题和争议

现代人工智能的快速进步，降低了上手使用的难度，缩短了学习使用的时间，使得AI换脸的使用者范围不断扩大，普通人也能操作技术制作换脸视频，满足了人们娱乐社交等多样化的需求。但带来便利的同时，AI 换脸技术也带来不少问题：不少违法犯罪分子使用这项技术蒙骗受害人从而非法获取利益、利用技术换脸的方法侵犯他人肖像权、扰乱人脸认证破环正常生活秩序等。立足现代人工智能的AI换脸视频在传播中产生的伦理争议主要有以下三个方面。

(1) 信息内容失真，虚假视频弥漫。我们身处在智能媒体高度发达的时代，经历过图文时代的洗礼，短视频承载信息传播的优势逐渐显现出来，过去我们说“有图有真相”，但是那一瞬间的定格放到现在很有可能是别有用心的捕风捉影。然而，在AI视频换脸术、人像照变动态表情包技术等技术新浪潮下，有图有真相，被彻底颠覆……[2]视频的动态且连续的记录下，使人们越来越热衷于相信视频所反映出的真实信息，因为人们潜意识认为视频无法做假，因此视频常被作为可靠的媒体资讯来源或者法律依据。但是“AI换脸技术”的横空出世，大大降低了视频内容的真实性和权威性。借助这项“瞒天过海”的技术，无论是静态的图文抑或者是动态的视频，都能被随意地被合成、篡改、替换成任意一个对象。放任这种现象的结果就是虚假视频泛滥成灾，真实信息与虚拟内容边界不清，信息传播混乱，从而谣言肆意传播、各种误解不断产生、对立冲突迅速加剧。

(2) 威胁个人安全，侵犯个人隐私。当下在网络上流行的换脸视频基本上是对热门影视作品或者名人进行的带着娱乐性目的的二次创作，因而看上去没用什么威胁。但是这终归属于一项现代人工智能技术，

几乎所有的 AI 技术成长壮大都需要海量大数据来提供“饲料”，网民苦涩地开玩笑道：大数据时代，我们都毫无隐私。这反映了人们对于不正当使用个人数据的严重担忧。美国管理顾问和作家 Geoffrey Moore 曾说过：“如果没有大数据分析，企业就会变得既聋又瞎，像高速公路上的鹿一样游荡在网络上。”当技术进化到普通人的生物信息都被掌握时，人们担心它被利用在灰黑色领域，成为违法犯罪的工具和帮凶。众所周知，人脸识别技术已经广泛应用于支付、身份认证领域。如若这些承载着个人身份的面部信息泄露，将造成不可挽回的巨大损失。尤其是在这样一个社交媒体盛行的时代，人们有极强的分享欲望，在不经意之间上传的照片或者视频都有极大的被盗用的风险，一旦用作欺诈谋私，将会严重影响个人的名誉和信用。

(3) 危害公共利益，影响社会治安。2018 年，微软发表了《未来计算》一书，在提到的人工智能发展应遵循的六项原则中，第二条是要“可靠”，要“安全”。它的含义是指人工智能在被使用中的效果应当是不产生副作用，不作恶的。该项技术还在成长壮大发展阶段，并没有完全成熟，所以以这项技术开发的相关软件或多或少存在着某些缺陷，一旦被攻破入侵，影响的是大众的信息安全。2019 年 2 月，深圳某个相关技术企业发生了一起严重的信息数据泄露事件，涉及 250 多万人的核心数据失去了官方保护，有了被外界获取到的风险，外泄了预计 680 万条的用户记录，在这其中有个人生物身份信息、人脸识别数据及卫星定位数据等。同样是在 2019 年，在欧洲的一所类似的公司也曾遭遇信息泄露事故，事故涉及大规模的用户，造成数百万人的人脸数据泄露[3]。另外，一旦 AI 换脸这一魔手伸向其他领域，诸如政治、金融，扰乱官方话语权，制造出虚假信息，造成公众恐慌。

(二) AI 换脸视频涉及的主体

1、视频制作者

视频制作者，顾名思义，就是指利用深度伪造技术来实现换脸从而制作出承载虚假信息视频的主体。与人们的普遍认知不同，视频制作者不一定是单独的一个人，它也有可能是一个机构。如果是涉及多人的制作行为，应该根据实际的情况来分别判断，判断完成之后分别确定相应的责任。如果是团队或者机构制作，还要根据每个人在制作过程中的分工角色来分别进行讨论。一般来说，视频制作会经过收集阶段、处理阶段和生成阶段。如果图文视频收集者、数据处理者和视频生成者这三者不是在共同意志下进行的，最终不构成共谋，那么这时要分别考虑是否有主观过错。根据我国法律规定，生成者不管有没有侵犯他人权益，都要承担责任。收集者和处理者在没有侵犯意识并且没有产生侵犯结果的情况下，不承担责任。如果是在共同意识下共同参与制作视频的情况下，所有参与者都要承担相应责任。

2、视频传播者

传播者又被称为传者、信源等等，它是传播行为的引发者，也即信息传播过程之中的主动发出者。除了视频的原始创作者，这里的传播者主要是指有转发或者转载传播行为的人。根据传播的对象和范围划分，又分为以下两类：公共传播和私人传播。如果行为人只是将制作的视频私下传播给特定范围内的有限数人，并且没有在社会范围产生危害，那么即便是视频中含有侵权内容，也不会被定性为侵权行为；但是，如果行为人大肆地在公共范围内向不特定人传播，那么这种情况下就对社会产生了一定的危害性，可以被定性为侵权行为。

3．网络服务提供者

网络服务提供者主要是指通过信息网络向公众提供信息或者为了获取网络信息等目的提供服务的单位或者个人。在网络高速发达的信息时代，尤其是短视频盛行的环境下，诸如抖音、快手、西瓜视频、哔哩哔哩等短视频平台都是典型的网络服务提供者，这些平台提供的是信息发布的网络服务。对于提供 AI 换脸技术的“ZAO”等应用程序，也属于网络服务提供者之列，它们属于提供技术支持的网络服务提供者。AI 换脸 APP 中的人格权侵权，在具有传统人格权属性的同时，还涉及某些明确的财产属性[4]。由于

本文主要讨论换脸视频的侵权规制，技术不在作者讨论范围内，因此讨论对象主要是视频信息发布传播平台。

4、受害者

受害者是指人身财产等合法权益受到侵害的一方。根据实际操作和社会案例，采用深度伪造技术制作的换脸视频主要侵犯了两类主体的两种合法权益。换脸视频制作者随意使用他人的肖像，用作非法事务又会损害他人名誉和荣誉以及隐私，因此对于被换脸者而言，它主要损害了其民法领域的人格权；而对于原始视频例如影视作品的作者来说，它主要损害了其知识产权领域的著作权。

3. 国外对 AI 换脸行为的法律规制

(一) 美国《深度伪造责任法案》及各州法律规制

AI 换脸技术诞生于美国，并且借助于好莱坞影视业的兴盛得以迅速发展，也正因此最早头疼于处理此技术带来的棘手的“副作用”。再实务过程中，美国渐渐找到了立法的内在逻辑，因此是最早进行立法的国家，与该项技术相关的法案也越来越多，从中央联邦政府到地方州政府都有相关应急预案。美国立法者在承认该项技术对于文化、娱乐、社交层次有正面作用的基础上，主要对其在国家层面的潜在威胁做出限制。基于民众的担忧和信息安全的考虑，美国也是最早对 AI 换脸技术开始规范和限制的国家，其在立法和司法实践中的经验值得我们研习[5]。

2019 年 6 月，美国联邦众议院推出了《深度伪造责任法案》，目前在深度伪造技术领域，该法案是规定的最详细、最全面的一份法案，这项法案在制度设计上比较激进，同时法案明确设置了刑罚，要求视频制作者对发布传播的 AI 制作视频负责，带有恶意的深度伪造作品必须使用“不可删除的数字水印以及文本描述”来标记，否则将属于违法犯罪行为，除此之外还向受害者提供了各种救济渠道。

美国各州也迅速跟进立法，2019 年 6 月，德克萨斯州最先通过了一项《关于制作欺骗性视频意图影响选举结果的刑事犯罪法案》，此法案主要用来维护地方选举秩序，任何使用 deepfake 手段制作换脸视频阻碍干扰影响选举结果的行为都将承担刑事责任。弗吉尼亚州也在 2019 年 7 月正式颁布了一项《非同意色情法》的修正案，新增规制深度合成技术的内容，法案中提到的“制作、传播虚假的非法性内容”的行为可被认定为刑事类罪名，并把发布和传播深度伪造视频列入采取用情色复仇的方式之一，规定如果不遵守以上规则是罪行种类的第 1 类，判处的监禁时间最长可达 12 个月，罚款数额最多可到 2500 美元，在包含“深度伪造”内容的州立法领域，这是美国各州中首例[6]；2019 年 10 月，加利福尼亚州通过名为的《AB 730》法案，在法案中明确规定上传伪造、带有扰乱目的的影像，不利于候选人正常进行选举的行为涉嫌犯罪。这项法案的适用对象是处于在 60 天以内选举期内的所有候选人，其目的是清除带有不正确信息的虚假视频，从而降低对选举过程中产生的不利效果。

(二) 欧盟以及德国的法律规制

为了应对深度伪造技术的滥用带来的不可控局面，欧盟采用加强用户数据保护和管理信息平台两手抓的立法思路来限制相关技术的泛滥使用。一方面，欧盟在 2018 年 5 月公布实施了《通用数据保护条例》，此项法案实现了将网络用户的所有数据划入欧盟法律保护范围内，是专门针对于解决用户在网络社交媒体以及使用换脸技术的应用软件造成的隐私数据泄露问题的专项法案。另一方面，欧盟在 2018 年 9 月公布了面向互联网企业的《反虚假信息行为准则》，目的在于从源头治理网络虚假信息，强调互联网企业发挥作为平台的作用，自我审查、自我管控，加强社交媒体和搜索平台在打击网络虚假信息方面的行动力度。

德国作为欧盟一员，除了遵循欧盟制定的相关规制外，还根据自身国情进行了一系列本土化立法。2018 年，德国通过了专门针对社交媒体平台的法律《社交媒体管理法》，按照法案的规定，所有注册用

户数量超过 200 万的社交媒体公司必须制定一定的程序用来处理网站内被举报的内容，对于明显违背法律规定的虚假信息，限期在 24 小时内删除完毕。违法的个人最高面临 500 万欧元罚款，违法的公司最高面临 5000 万欧元罚款。该法案是打击网络空间虚假信息的一个良好开端。

(三) 无专门法律的其他国家

由于深度伪造技术近几年才走入人们的视野并出现滥用的现象。因此大部分国家还在探索治理当中，没有针对人工智能深度伪造技术的专门法律，不过有相关法律可以暂时适用，下面简单介绍新加坡、英国、韩国和俄罗斯这几个国家的相关规制法。

2019 年，新加坡深感深度伪造技术的日益影响，正式立法并实施了《防止网络虚假信息和网络操纵法案》，这项法案允许政府下令删除社交媒体平台上的虚假内容，适用于深度伪造技术制作的音视频所引起的损害社会公共利益的案件。对于违反法案的网络平台，最高可罚款 100 万元新加坡元，个人故意制作并传播虚假信息可被监禁最长 10 年之久。对比之下，英国特别注重对于个人生物信息的保护，因此颁布《数据保护法》，根据数据的不同类别采取不同措施保护，凡是与个人有关的数据都纳入保护范围。与英国相类似，韩国也出台了《个人信息保护法》，凡是没有经过本人的同意，任何机构禁止收集、使用、提供个人信息。违反者将面临 5 年以下有期徒刑或者 5000 万韩元以下的罚款。俄罗斯也比较类似，2016 年实施了《网站黑名单法》，如果网站传播虚假信息，政府有权将其纳入黑名单并关闭网站。

4. 我国对 AI 换脸行为的法律规制

(一) 国内立法规制现状

随着 AI 换脸技术的快速普及，其引发的肖像权侵害、个人信息泄露、虚假信息传播等侵权问题日益凸显。我国已逐步构建起以《民法典》为民事权利基础、《个人信息保护法》为敏感信息专项保障、《互联网信息服务深度合成管理规定》为技术应用核心监管规范的多层次规制体系[7]，同时配套以专项管理办法与司法实践，形成对 AI 换脸行为全流程、多维度的法律约束。

1、人格权与个人信息保护的基础支撑

《民法典》作为民事领域的基本法，为 AI 换脸侵权的权利救济提供了核心依据，其规制重点集中于人格权与个人信息的双重保护。在肖像权保护方面，第 1019 条明确规定“任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权”，直接将 AI 换脸中未经同意伪造他人肖像的行为纳入侵权范畴，且删除了原《民法通则》中“以营利为目的”的侵权构成要件，实现对肖像权的全面保护。针对 AI 换脸可能伴随的隐私权与名誉权侵害，第 1032 条、第 1024 条分别明确隐私权的不受侵扰权能与名誉权的保护边界，禁止通过换脸技术制作传播含有隐私内容或侮辱、诽谤性质的视频内容。

在个人信息保护层面，《民法典》第 1034 条将人脸信息纳入个人信息的范畴，明确其受法律保护，为后续专项立法奠定了民事权利基础。同时，该法第 1035 条确立的“合法、正当、必要”原则，成为 AI 换脸技术研发与应用中处理人脸信息的基本遵循，要求任何组织或个人处理人脸信息必须具备合法目的，不得超出必要范围。

2、《个人信息保护法》：敏感个人信息的强化监管

《个人信息保护法》将人脸信息明确列为“敏感个人信息”，构建了更为严格的专项保护规则，成为规制 AI 换脸中个人信息侵权的关键法律依据。其核心规制要点体现在三个方面：一是单独同意原则，根据第 27 条规定，处理敏感个人信息需取得个人的单独同意，意味着 AI 换脸服务提供者若需收集、使用他人人脸信息，必须获得被收集人明确、单独的授权，不得通过概括性同意条款规避义务。二是事前风险评估义务，第 55 条要求处理敏感个人信息前，必须进行个人信息保护影响评估，重点评估换脸技术应用对个人权益的潜在影响及安全防护措施的有效性，并形成评估报告留存至少 3 年。三是权利保障机

制，第 44 条赋予个人对其人脸信息的决定权，包括知情权、更正权、删除权等，明确个人有权撤回对换脸信息处理的同意，服务提供者需提供便捷的撤回渠道。

此外，《个人信息保护法》第 62 条针对人工智能等新技术新应用的特殊性，授权国务院有关部门制定专门的保护规则，为后续技术监管细则的出台预留了立法空间，体现了规制的前瞻性与灵活性。

3、《互联网信息服务深度合成管理规定》：技术应用的专项监管

2023 年施行的《互联网信息服务深度合成管理规定》(以下简称《深度合成规定》)作为针对深度合成技术的专门监管规范，将 AI 换脸明确纳入“深度合成技术”范畴，形成对其研发、应用、传播全流程的精细化规制。其核心要求包括：其一，严格的同意机制，第 9 条特别规定，利用深度合成技术制作、发布、传播涉及他人人脸、声音的合成信息，必须取得被合成人的单独同意；若合成信息为公众人物相关内容或用于新闻报道等法定情形，虽可豁免单独同意，但需履行显著标识义务。其二，全流程标识义务，第 16 条要求所有 AI 换脸生成的非真实信息，必须以显著方式标明“合成”字样或采取其他可识别方式，确保接收者能够清晰区分真实信息与合成信息，从源头遏制虚假信息传播。其三，算法与数据监管，第 19 条要求具有舆论属性或社会动员能力的深度合成服务提供者，需将其算法模型、数据来源等信息向网信部门备案；第 7 条明确禁止利用非法获取的人脸数据训练换脸算法，强化对数据源头的管控。

同时，《深度合成规定》还确立了“谁开发、谁负责，谁应用、谁负责”的责任原则，明确服务提供者、技术开发者的安全管理与内容审核义务，对违反规定的行为设置了警告、罚款、关停服务等行政处罚，构成犯罪的依法追究刑事责任。

(二) 配套规制与实践

1、专项监管办法的补充细化

为进一步强化人脸信息保护与技术监管，我国出台了一系列配套专项办法，与核心法规形成协同规制。2025 年 6 月 1 日起施行的《人脸识别技术应用安全管理办法》，虽聚焦人脸识别技术，但其中关于人脸信息存储、备案、安全保护的要求同样适用于 AI 换脸技术。该办法第 6 条重申处理人脸信息的单独同意原则，第 8 条明确人脸信息存储期限不得超过实现目的所必需的最短时间，且无特殊情形不得通过互联网对外传输；第 15 条要求处理人脸信息达 10 万人的主体向省级以上网信部门备案，强化对大规模人脸数据处理的监管。此外，《生成式人工智能服务管理暂行办法》《网络数据安全管理条例》等法规，分别从生成式 AI 服务的透明度要求、数据安全分级保护等角度，为 AI 换脸技术的合规应用提供了补充约束。

2、司法实践的权利救济落地

司法实践已成为检验与细化法律规制的重要途径，通过典型案例明确 AI 换脸侵权的裁判规则。在杭州互联网法院审理的“AI 换脸侵犯个人信息公益诉讼案”中，法院认定被告未经同意利用他人人脸信息制作淫秽换脸视频并传播，不仅侵害个人肖像权、隐私权，更损害社会公共利益，最终判令其停止侵权、赔礼道歉并支付公益损害赔偿金。该案明确了 AI 换脸中“单独同意”的必要性、人脸信息的敏感保护属性，以及公益诉讼在规制此类侵权行为中的补充作用[8]。此外，多地法院在相关民事侵权案件中，依据《民法典》第 1019 条，均认定未经同意制作传播换脸视频构成肖像权侵权，即便未以营利为目的，仍需承担民事赔偿责任，进一步明晰了侵权构成的裁判标准。

(三) 当前规制体系的特点与不足

随着 AI 换脸技术的快速迭代与普及，其在丰富内容创作场景的同时，也带来了人格权侵权、信息诈骗、舆论误导等风险。对此，我国已构建起“基础法律 + 专项法规 + 监管细则 + 司法实践”的全维度规制体系，为技术健康发展划定了法律红线，其核心特征凸显为三维协同的规制逻辑。

其一，权利保护与技术监管双向并行。在权利保障层面，《民法典》人格权编明确了人脸作为具体

人格权的法律属性，禁止非法利用人脸信息；《个人信息保护法》将人脸信息纳入敏感个人信息范畴，强化收集、使用环节的合规要求。在技术监管层面，《网络信息内容生态治理规定》《深度合成服务管理规定》等专项文件，明确了 AI 换脸服务提供者的备案义务、内容标识责任，从源头规范技术应用流程，实现权利救济与风险防控的有机统一。

其二，全流程闭环规制覆盖无死角。从人脸信息的源头收集，要求遵循“知情同意”原则且限定必要范围；到算法训练环节，禁止使用非法获取的人脸数据；再到换脸内容的制作、发布与传播，强制要求添加可识别标识，平台需履行内容审核义务，每个环节均有明确的法律依据与操作规范，形成全链条管控格局。

其三，多部门协同监管形成合力。网信部门统筹网络信息内容治理，公安部门聚焦打击利用 AI 换脸实施的诈骗、诽谤等违法犯罪行为，广电部门监管视听领域的换脸内容传播，各部门依据法定职责分工协作、信息共享，构建起跨领域、多层次的监管网络。

尽管规制体系已具雏形，但面对技术的高速发展，仍存在诸多短板。一是专门性立法缺位，现有规则分散于不同法律法规及规章中，对 AI 换脸“深度伪造”的技术特殊性考量不足，部分条款存在适用交叉、规制留白问题，难以形成系统性约束。二是监管技术手段相对滞后，传统人工审核、投诉核查模式，难以应对海量生成式换脸内容，对侵权行为的实时监测、精准溯源能力薄弱。三是惩罚性赔偿适用标准模糊，现有法律仅规定民事赔偿与行政处罚，针对恶意制作传播侵权内容、大规模泄露人脸数据等行为，缺乏细化的惩罚性条款适用规则，威慑力不足。这些问题需通过制定专门立法、创新监管技术、完善追责机制予以破解，推动规制体系与技术发展同频共振。

参考文献

[1] 董鑫. “AI 换脸”视频中的肖像权侵权问题探究——以 B 站的“AI 换脸热”现象为例[J]. 新闻研究导刊, 2021, 12(5): 64-65.

[2] 沈臻懿. AI 视频换脸术[J]. 检察风云, 2019(16): 32-33.

[3] 李江杉. AI 换脸 APP 中人格权侵权问题研究[J]. 法制博览, 2021(17): 30-31.

[4] 曹越. AI 换脸技术产生的危害与应对措施[J]. 南海法学, 2020, 4(4): 69-77.

[5] 张惠彬, 侯仰瑶. 从技术到法律: AI 换脸短视频的侵权风险与规范治理[J]. 北京科技大学学报(社会科学版), 2024, 40(1): 124-132.

[6] 洛桑丹增, 周书汛. AI 生成图片可版权性中美对比分析——以“AI 文生图著作权侵权第一案”为例[J]. 冶金管理, 2025(9): 67-71.

[7] 夏丽芳. AI 表演的版权侵权判定及声音权衔接保护——以“N + 1”结构为视角[J/OL]. 宜宾学院学报, 1-12. https://link.cnki.net/urlid/51.1630.Z.20251105.1755.002, 2026-02-10.

[8] 陈玥. 新兴人工智能法律主体资格的否定——基于自然人路径与法人路径的双重证伪[J]. 河南财经政法大学学报, 2025, 40(5): 63-77.