

人工智能生成内容的肖像权与声音侵权问题研究

李明行

安徽财经大学, 中国·安徽 蚌埠 233030

摘要: 随着深度伪造、声音克隆等人工智能生成内容技术的迅猛发展与广泛应用, 未经许可利用他人肖像与声音数据合成高度逼真内容的现象日益泛滥, 对传统人格权保护制度构成了严峻挑战。主要体现在 AIGC 场景下的肖像权与声音权侵权问题, 核心在于解决生成式内容如何突破以“再现”为核心的传统侵权范式, 以及由此引发的侵权认定、责任分配等法律困境。同时,《民法典》等法律存在归责供给不足的问题。基于此, 应当重构了 AIGC 侵权的构成要件, 主张对“使用”行为作扩张解释, 并以“合理关联”为核心重构“可识别性”标准。在责任承担层面, 需要系统分析了终端使用者、模型开发者、服务提供者等多元主体的责任形态与划分规则, 最后, 应从立法、司法、行政监管及行业自治四个维度协同发力, 构建一套既能有效救济受害人权益、厘清各方责任, 又能为技术创新预留合理空间的综合性规制体系, 以期为实现数字时代人格尊严的妥善保护提供理论支撑与路径参考。

关键词: 人工智能生成内容; 肖像权; 声音权; 深度伪造; 人格权侵权

A Study on the Right of Publicity and Voice Infringement Issues in Artificial Intelligence-Generated Content

Li Mingxing

Anhui University of Finance and Economics, China Anhui Bengbu 233030

Abstract: With the rapid development and widespread application of artificial intelligence-generated content technologies such as deepfakes and voice cloning, the phenomenon of synthesizing highly realistic content using unauthorized portraits and voice data has become increasingly rampant, posing a severe challenge to the traditional system of protecting personality rights. This is primarily manifested in the infringement issues of portrait rights and voice rights in the AIGC (Automated Image and Video Generation) scenario. The core lies in addressing how generative content breaks through the traditional infringement paradigm centered on "reproduction", as well as the legal dilemmas arising from infringement identification and liability allocation. At the same time, there is a problem of insufficient imputation supply in laws such as the Civil Code. Based on this, it is necessary to reconstruct the constituent elements of AIGC infringement, advocate for an expanded interpretation of the "use" behavior, and reconstruct the "identifiability" standard with "reasonable association" as the core. In terms of liability assumption, a systematic analysis of the liability forms and division rules of multiple subjects such as end users, model developers, and service providers is required. Finally, concerted efforts should be made from the four dimensions of legislation, judicature, administrative supervision, and industry self-regulation to construct a comprehensive regulatory system that can effectively remedy the rights of victims, clarify the responsibilities of all parties, and reserve reasonable space for technological innovation. This aims to provide theoretical support and path reference for the proper protection of personality dignity in the digital era.

Keywords: AI-generated content; Right of portrait; Right of voice; Deepfakes; Infringement of personality rights

0 引言

我们正置身于一个由人工智能深度塑造的时代。生成式人工智能技术的突破, 特别是深度伪造和声音克隆技术的成熟, 极大地降低了制作超写实音视频内容的门槛。这项技术如同一把双刃剑: 它在影视制作、教育娱乐等领域展现出巨大潜力, 但同时也为恶意行为者打开了滥用之门。从制作色情视频恶意损毁他人名誉, 到模仿公众人物或亲

友声音实施诈骗, 再到未经授权利用明星肖像进行商业营销, 一系列社会事件频频见诸报端, 凸显了技术滥用对个体人格尊严与社会信任基础构成的严峻威胁。

传统的肖像权与声音权法律体系, 根植于对既有形象与声音的“再现”与“非法使用”。然而, AIGC 的本质是“无中生有”地合成全新的内容, 这使得侵权模式发生了根本性转变。当 AI 生成的虚拟面孔并非对某张照片的精确复

制,却足以让公众清晰地联想到特定自然人时,是否构成侵权?当模型开发者利用海量网络数据(包含无数人脸与声音)训练算法,这是否构成了对人格要素大规模、前置性的侵害?侵权链条上的数据提供者、算法开发者、平台运营者和终端用户,责任又当如何划分?这些问题暴露出以“可识别性”和“同意原则”为核心的传统法律框架在应对 AIGC 挑战时的滞后与无力。

尽管我国《民法典》人格权编为肖像和声音提供了坚实的权利基础,《个人信息保护法》与《生成式人工智能服务管理暂行办法》也从不同角度切入规制,但面对 AIGC 带来的系统性挑战,现有规则仍显得零散且缺乏针对性。司法实践亦因规则不明而面临认定难、裁判尺度不一的困境^[1]。因此,系统性地研究 AIGC 场景下的肖像权与声音权保护问题,不仅是回应技术发展对法学理论的深刻拷问,更是为司法裁判提供清晰指引、为产业合规发展厘清边界、为国家未来立法完善提供智识参考的迫切之需。

1 AIGC 的应用场景分析

传统人格权制度,特别是肖像权与声音权,建立在“表征自我”与“控制使用”的基本理念之上。其核心在于保护自然人对其自身外部形象标识(肖像)与声音标识(声音)的专属性与完整性,防止他人未经同意的非法再现与使用。然而,生成式人工智能技术的出现,从根本上撼动了这一制度的根基。它不再仅仅是对既有形象的“复制”与“传播”,而是开启了“合成”与“创造”的新范式^[2]。本章旨在深入剖析 AIGC 的技术特性,揭示其如何从侵权模式、权利核心、责任链条及损害后果四个维度,对传统的肖像权与声音权制度构成前所未有的系统性挑战。

要理解法律挑战的根源,首先需洞察其技术本质。生成式人工智能(AIGC)的核心技术,尤其是扩散模型和生成对抗网络,使其能够从海量的训练数据(包含无数人脸图像和音频片段)中学习底层规律与特征分布,进而生成全新的、在训练集中不存在但高度逼真的内容^[3]。

以深度伪造(Deepfake)为例,其过程通常涉及:(1)数据采集与训练:收集目标人物的大量肖像与声音数据,投入模型进行深度学习,以捕捉其独特的面部特征、肌肉运动规律、声纹、语调等生物识别信息。(2)内容生成:利用训练好的模型,将源视频或音频中人物的面部和声音替换为目标人物的特征,实现无缝“换脸”与“换声”^[4]。更为先进的技术甚至无需特定源素材,仅通过文本描述(如“生成一个具有 XX 明星微笑特征的虚拟人演讲视频”)即可直接合成内容。

生成式人工智能(AIGC)的主要应用场景包括以下几个方面:恶意与非法场景:这是法律规制的焦点。包括制作淫秽物品进行敲诈或名誉毁谤;模仿公众人物或企业高管声音发布虚假声明,扰乱金融市场;模仿亲友声音实施电信诈骗;未经授权利用明星肖像生成广告或为产品代言;中性或争议性场景:如在影视作品中让已故演员“复活”参演,或在历史纪录片中让历史人物“开口说话”。这些应用虽具有一定艺术或教育价值,但其法律边界,特别是关于死者人格利益保护与权利继承问题,依然模糊;创新性场景:如创建高度定制化的虚拟数字人进行直播、客服或陪伴。这些应用虽旨在创新,但其训练数据来源的合法性,以及生成内容与真实自然人形象的相似度边界,同样潜伏着侵权风险。

AIGC 技术的这种“从无到有”的生成能力,以及其依赖底层数据而非直接复制表象的特性,是引发后续一系列法律困境的总根源。

2 AIGC 对肖像权与声音权制度的挑战

2.1 从“再现”到“生成”:侵权模式的根本性转变

传统侵权法与人格权制度所预设的侵权模式,本质上是“未经同意的再现与使用”^[5]。例如,未经许可将某人的照片用于商业广告,或将某人的演讲录音用于产品推广。在这种模式下,被侵权的客体是客观存在的、预先固定的形象或声音记录。法律救济的核心是制止对该特定记录的非法传播和使用。

然而,AIGC 引入的是一种“未经同意的合成与创造”的全新侵权模式。侵权行为的对象不再是某个具体的、已存在的肖像或录音,而是构成自然人可识别特征的一系列生物识别数据(数据集合)。侵权行为的发生点大大提前并分散化了:从采集面部数据用于模型训练开始,到算法模型本身对人格特征的吸收与内化,再到最终用户通过指令生成侵权内容。这使得侵权行为的认定变得异常复杂,主要表现为以下几点:

首先是侵权客体的虚拟化:侵权的直接对象不再是固定的照片或录音,而是动态生成的、此前从未存在过的虚拟内容。其次是侵权行为的前置化与隐蔽化:最具侵害性的行为可能发生在模型训练阶段,而此时具体的侵权内容尚未产生,难以被权利人察觉和追究。最后是侵权与创作的模糊化:生成内容往往是算法“创作”的结果,夹杂着机器学习的随机性与创造性,这与传统的“复制粘贴”式侵权有本质区别,动摇了传统侵权认定中“实质性相似”等标准的适用基础^[6]。

这种从“再现”到“生成”的范式转变，是理解 AIGC 所带来的一切法律挑战的逻辑起点。

2.2 核心挑战的具体表现

基于上述范式转变，AIGC 对肖像权与声音权制度的具体挑战主要体现在以下几个方面：

2.2.1 “可识别性”标准的模糊化与瓦解

“可识别性”是肖像权与声音权保护的基石。传统司法实践中，判断是否构成侵权，关键在于被使用的肖像或声音能否被识别为特定的自然人。AIGC 技术使这一核心标准陷入了困境。

AIGC 生成的肖像可能并非对权利人任何一张现有照片的精确复制，它可能融合了多角度特征、改变了光影背景，甚至结合了其他人的部分特征。然而，由于其捕捉并再现了权利人最核心、最独特的生物特征（如眉眼间距、嘴角弧度、面部轮廓、声纹频率），其整体呈现效果足以让一般公众毫不犹豫地指认：“这就是 A 先生 / 女士”。此时，法律是否应提供保护？如果保护，是基于对哪张具体照片的侵权？这挑战了传统侵权认定中需要与原作品进行“比对”的思维。

更为极端的情况是，AIGC 可能仅仅“挪用”了某人极具特色的微笑、标志性的手势或独特的嗓音共鸣方式，并将其赋予一个完全虚拟的形象。这种对“特征”而非“整体”的利用，如果足以导致公众产生强烈关联，是否构成对肖像权或声音权的侵害？这迫使法律必须思考，保护的边界究竟是人脸的“整体形象”，还是足以识别个人身份的“关键特征”。

2.2.2 “同意原则”的虚化与架空

知情同意是人格权商业化利用和合法使用的核心原则。AIGC 技术的运作模式使得这一原则在多个环节被轻易绕过甚至彻底架空。

绝大多数 AIGC 模型的训练依赖于从互联网等公开或非公开渠道爬取的海量数据。这些数据中包含的数以亿计的人脸和声音，其权利人对此毫不知情，更未曾同意将其人格要素用于训练一个可能生成其虚假内容的模型。这种未经同意的数据利用，构成了大规模、系统性的前置侵权。

即便权利人同意在某一场合（如社交媒体分享照片）使用其肖像，这种同意也绝不能被解释为同意其肖像数据被用于模型训练，并可能被用于生成任何未知的、甚至是有损其名誉的虚假内容。AIGC 技术使得一次性的、有限的同意，面临着被无限扩展和滥用的巨大风险^[7]。

在公开场合被拍摄并用于训练数据，是否构成默示同

意？这显然不符合人格权保护的法理。人格权是绝对权，其授权使用应以明示、特定为前提。

2.2.3 侵权主体认定的复杂化与链条化

在传统的肖像侵权中，侵权主体通常是内容的直接制作者和传播者，关系相对简单。而在 AIGC 侵权链条中，参与者众多，责任划分极其困难。

一条 AIGC 侵权视频的背后，可能涉及：数据提供者（非法爬取或提供数据集）、模型开发者（设计并训练了具有强大生成能力的模型）、服务提供者（提供在线生成平台）、终端使用者（输入指令生成最终侵权内容）。这些主体在主观过错、行为作用、因果关系上各不相同^[8]。

模型开发者与服务提供者通常不会直接实施生成特定侵权内容的行为。他们是否承担责任，取决于其是否履行了合理的注意义务，例如在模型设计时加入过滤机制、对用户生成内容进行有效监管、在接到通知后及时采取补救措施等。认定其存在“明知或应知”的主观状态，在技术黑箱面前异常困难。

3 应对 AIGC 的完善建议

应对 AIGC 对于个人信息权的侵犯，我国相继出台了一系列法规，如《个人信息保护法》《生成式人工智能服务管理暂行办法》等，以更好的从法律层面为 AIGC 的发展明晰出路，但由于 AI 技术尚处于发展的早期，技术迭代日新月异，想要在当前阶段制定完美的法律体系并不现实，因此，在法律层面缺失的情况下，针对 AIGC 在目前存在的问题，应当为立法到司法的全过程确定较为明确的标准，以期在当前阶段实现技术发展与个人信息保护的平衡。

3.1 立法层面：推动专门立法与法律解释

制定《人工智能法》：在未来制定的《人工智能法》中设立专章或专条，明确规定 AIGC 技术开发与应用的基本法律原则。应确立“源头治理、风险分级、权责一致”的原则，明确要求基础模型提供商承担更高的合规义务，包括数据来源合法性审查、模型安全与伦理评估、输出内容过滤等。

出台司法解释：由最高人民法院尽快就审理涉 AIGC 人格权侵权纠纷案件出台司法解释。重点明确：（1）“可识别性”的司法认定标准，采纳“一般公众合理关联”标准；（2）多元主体的过错认定规则与责任承担比例；（3）损害赔偿的计算方法，引入“惩罚性赔偿”以遏制恶意侵权；（4）人格权侵害禁令在此类案件中的快速审查与执行程序。

3.2 司法层面：统一裁判尺度与强化能力建设

（1）发布指导性案例：遴选具有典型意义的 AIGC 侵

权案例作为指导性案例发布,为全国法院提供统一的裁判指引,有效减少“同案不同判”现象。

(2) 引入技术调查官制度:在审理复杂技术类案件时,引入人工智能领域的技术专家作为陪审员或技术调查官,协助法官理解技术原理,准确认定事实。

4 结语

我国对 AIGC 肖像权与声音权的法律规制已初具雏形,但远未完善。《民法典》奠定了坚实的权利基础,《个人信息保护法》提供了源头规制的有力武器,《暂行办法》则迈出了专门监管的关键一步。然而,立法原则化、司法实践困境重重以及监管碎片化的问题依然突出。未来,必须采取立法、司法、行政与行业自治“四轮驱动”的策略,通过高位阶立法明确规则、通过司法解释统一裁判、通过有效监管落实责任、通过行业自律促进合规,方能构建起一个既能有力捍卫个体人格尊严,又能为负责任技术创新预留空间的良性治理生态,从容应对人工智能时代对法律提出的持续挑战。

参考文献:

[1] 熊琦. 人工智能生成内容的著作权认定[J]. 知识产

权, 2017(03):4-5.

[2] 梁志文. 论人工智能创造物的法律保护[J]. 法律科学(西北政法大學學報), 2017(05):13-14.

[3] 徐小奔. 人工智能“创作”的人格要素[J]. 求索, 2019(06):15-16.

[4] 丁文杰. 通用人工智能视野下著作权法的逻辑回归——从“工具论”到“贡献论”[J]. 东方法学, 2023(05): 25-16.

[5] 张平. 人工智能生成内容著作权合法性的制度难题及其解决路径[J]. 法律科学(西北政法大學學報), 2024(03):16-17.

[6] 吴汉东. 论人工智能生成内容的可版权性: 实务、法理与制度[J]. 中国法律评论, 2024(03):12-14.

[7] 王诗童. 著作权法中“创作”概念在人工智能时代的新发展[J]. 知识产权, 2025(08):11-13.

[8] 支振锋. 生成式人工智能大模型的信息内容治理[J]. 政法论坛, 2023(04):11-14.

作者简介: 李明行, 男, 河南洛阳, 硕士研究生在读, 研究方向: 民商法。