Dispute Settlement 争议解决, 2022, 8(4), 1096-1100
Published Online December 2022 in Hans. http://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2022.84148

Hans汉斯

论深度伪造技术侵犯他人声音权益的民法保护

仵思政

青岛大学法学院，山东 青岛

收稿日期：2022年10月17日；录用日期：2022年12月6日；发布日期：2022年12月13日

摘　要

深度伪造是一种人工智能的新兴技术，通过“深度学习”和“伪造”两个基本系统可以实现对他人声音的模仿，达到以假乱真的程度，引发了不法分子利用深度伪造技术侵犯他人声音人格权益现象的发生；而声音信息作为个人信息的一种，未经许可使用他人声音数据亦会侵犯权益人的个人信息权。与传统侵权行为相比，深度伪造侵权存在着亟待解决的新生问题，具体包括技术提供者的责任难以界定、受害人举证困难、侵权人身份难以确定三大内容。在明确声音权益保护法律依据的基础上，通过对技术提供者、音频传播者课以相应义务和完善深度伪造行为人责任追究规则，实现声音权益的妥善保护。

关键词

深度伪造，声音权益，声音信息

On Civil Law Protection of Infringement of Others' Voice Rights and Interests by DeepFakes Technology

Sizheng Wu

School of Law, Qingdao University, Qingdao Shandong

Received: Oct. 17th, 2022; accepted: Dec. 6th, 2022; published: Dec. 13th, 2022

Abstract

DeepFakes is a new technology of artificial intelligence. Through the two basic systems of “deep learning” and “fakes”, one can imitate the voice of others to the extent that it is false, which leads to the phenomenon that criminals use DeepFakes technology to infringe the personality rights and interests of others' voices. As a kind of personal information, the use of other people's voice data without permission will also infringe the rights of personal information of the obligee. Compared

文章引用: 仵思政. 论深度伪造技术侵犯他人声音权益的民法保护[J]. 争议解决, 2022, 8(4): 1096-1100.
DOI: 10.12677/ds.2022.84148

with the traditional infringement, the DeepFakes infringement has new problems that need to be solved urgently, including the difficulty in defining the responsibility of the technology provider, the difficulty in providing evidence for the victim, and the difficulty in determining the identity of the infringer. On the basis of clarifying the legal basis for the protection of voice rights and interests, the voice rights and interests can be properly protected by imposing corresponding obligations on technology providers and audio communicators and improving the rules for accountability of perpetrators of DeepFakes.

Keywords

DeepFakes, Voice Rights and Interests, Sound Message

1. 引言

前段时间，脸书(Facebook)首席执行官马克·艾略特·扎克伯格(英文：Mark Elliot Zuckerberg)在一段视频中宣称，“谁控制了数据，谁就控制了未来”，引发了不小的轰动，但事实上扎克伯格并未说过这句话，该视频最后也被证实为伪造。该视频的逼真程度令世人惊叹，而这要归功于深度伪造技术。从此，“深度伪造”一词也就开始走进人们的视野之中。如今，深度伪造技术愈加成熟，其在为人们的生活提供便易的同时，也出现了不法分子通过该技术侵犯他人权益的情况，产生了与传统侵权有所不同的新问题。本文出于解答这些新问题的目的，在理解深度伪造技术的概念和技术逻辑的基础上，讨论利用该技术侵犯他人声音权益民法保护的开展。

2. 深度伪造侵犯声音权益的现实案例

2019 年 3 月，一名诈骗犯利用 AI 语音模仿软件冒充公司大老板，成功让一家英国能源公司的 CEO 相信自己正在与德国母公司的老板通电话。电话中，对方的一口具有德国口音的英语听起来像极了德国母公司老板的声音，以至于对方要求该 CEO 转账时其深信不疑，最终导致 22 万欧元不翼而飞。据《华盛顿邮报》报道，这位 CEO 后来在一封电子邮件中指出，这个要求相当“奇怪”，但“大老板”的德国口音非常逼真，他觉得自己别无选择，只能服从。一些研究人员表示，这是世界上首次公开报道的人工智能诈骗案[1]。

毫无疑问，这一行为虽然目的仅仅是冒充老板诈骗公司钱财，但就结果而言其不仅造成了公司的财产损失，未经许可使用、伪造该老板声音的行为也侵犯了其声音权益。传统的多媒体编辑处理软件人为地对照片、声音和视频进行编辑处理，总有不自然之处[2]。而利用人工智能技术合成音频，其足以以假乱真的相似程度即使是熟知声音权益人的亲近之人也很难发现端倪。不难想象，在语音技术普遍应用于手机、房门解锁、网上购物付款的当下，如果有不法分子利用深度伪造技术伪造他人声音，每个人的财产都有随时被侵犯的危险，届时将人人自危，社会将处于动荡之中。因此，对利用人工智能侵犯声音权益的行为必须予以法律规制，而充分了解该人工智能技术则是前提。

3. 深度伪造的概念与技术逻辑

利用 AI 语言模仿软件模拟他人声音，其背后的支持性技术实质上是深度伪造技术。“深度伪造”

(DeepFakes)是国外的一项计算机数据伪造合成技术，传入我国后经直译而得名。其包含“deep learning”和“fakes”两部分，即由“深度学习”和“伪造”两个基本系统构成。“伪造”是一种数据处理的过程、行为，而“深度学习”是一种人工智能，其本质是一种计算机算法，通过该算法使得程序可以自动分析数据结果并加以纠正。现有的深度学习算法主要包括卷积神经网络(Convolutional Neural Network, CNN)和“生成性对抗网络”(Generative Adversarial Network, GAN)两种，前者是深度伪造产生之初使用的技术，而后者产生较晚、算法更优，为目前所最常使用。在深度伪造技术这一概念的涵摄域下，以其生成目标内容为区分标准，又可以将深度伪造技术具体分为图像深度伪造技术、声音深度伪造技术与视频深度伪造技术[3]。这三种分类只在输入的数据来源和输出的生成结果的表现形式是图像、声音还是视频有所区别，内部的工作原理是相同的。具体而言，“深度伪造”的核心技术在于“自动编码器”与“对抗生成网络”的人工神经网络[4]。以声音深度伪造技术为例，“自动编码器”即为“伪造”系统，实质是伪造声音的生成器，其工作原理是将输入的自然人声音进行数据解码，自动化、智能化地学习该声音的语速、重音、口音等等特征，进而生成伪造的声音结果。目前最常见的声音伪造手段是“语音克隆”技术，具体包括“说话者自适应(speaker adaption)”和“说话者编码(speaker encoding)”两种[5]。其中，“说话者自适应”是通过分析声音数据源的特征，从已有声音模型库匹配中最相似的声音模型实现声音伪造；而“说话者编码”是则是通过调整标准声道模型匹配声音数据源，从而伪造自然人声音[6]。一般而言，该编码器仅运行一次所生成的结果的相似程度是很低的，而“对抗生成网络”则具有鉴定“自动编码器”所生成结果的功能，在“自动编码器”生成结果达不到其设定的相似程度时，便会在作出相应调整后将生成结果输入“自动编码器”重新运行，经过两个系统之间数次“生成－鉴定－调整－生成”过程的重复，从而使最终输出结果达到以假乱真的效果。而该技术的使用门槛极低，非专业人员亦可使用，更是加剧了侵权隐患。

4. “深度伪造”侵犯声音权益带来的新问题

“深度伪造”侵权与传统声音侵权相比，存在一些新问题。

首先，技术提供者的责任界定存在问题。如今技术提供者主要有两种，一种是通过“深度伪造”计算机软件有偿为客户制作，将成品交付客户完成交易；另一种是制造低门槛的“深度伪造”APP 供用户自行制作。当侵权案件发生之后，“深度伪造”服务提供者和“深度伪造”APP 制造者往往以“技术中立”为理由主张免责。首先，“深度伪造”一词不同于“深度合成”，“伪造”本身就含有法律上的负面评价、带有贬义色彩，不能被认为是中立的；其次，新兴技术的好坏取决于使用人的行为，技术中立并不代表技术使用者的行为一定就是合法的，利用“深度伪造”技术伪造他人声音进行诈骗或者贬损人格的行为必然是违法行为，为他人提供“深度伪造”服务和制作“深度伪造”APP 的行为都可能涉及侵权。总之，如果技术提供者明知行为人从事侵权行为而仍然为其提供深度伪造服务的，“技术中立”不能成为阻却其承担责任的“避风港”，需要承担相应的责任。

其次，受害人举证困难也是亟待解决的问题。在“深度伪造”声音侵权案件中，行为人制作的假音频的逼真度极高，现有的司法鉴定技术无法辨明真伪，从而使得司法鉴定的结果可能丧失准确性，一些适用深度伪造技术伪造的音频可能被鉴定为真，这就导致现实中受害人很难证明该音频是伪造的，也难以证明其没有说过音频里的话，而民事诉讼中贯彻“谁主张谁举证”的原则，如果原告无法举证证明侵权行为就要承担败诉的风险，其权益也就无法得到保障。

最后，侵权人的真实身份的确定亦是一大难题。声音数据的获取也具有涉及声音侵权的可能性。生成深度伪造音频必须通过对声音数据进行深度学习才能完成，而声音数据的获取是前提。如今我们处在大数据时代，各种软件、APP 都有语音权限，我们的声音信息可能早已被非法获取、公开、使用，完全

暴露在互联网之中，大多数情形下这些行为皆未经同意，这些行为的本质实际上都是侵犯声音权益的违法行为。而互联网的复杂性、匿名性特征导致很难追查到深度伪造音频的最初来源，即使大费周章、最终找到了上传用户，也往往因该用户没有实名信息而最终使确定具体侵权人的愿望泡汤，权益受损却无法得到司法保护。

5. 深度伪造侵权的民法保护开展

5.1. 禁止利用深度伪造技术侵犯声音权益的法律依据

在我国，禁止深度伪造自然人声音的法律依据在于《民法典》第1019条和第1023条第2款。第1019条规定了不得“利用信息技术手段伪造”侵犯肖像权，其作为肖像权保护规范，经第1023条第2款这一“参照适用”条款适用于自然人声音的保护，即任何人不得以利用信息技术手段伪造的方式侵犯自然人声音权益。值得注意的是，《民法典》采取的措辞是“利用信息技术手段伪造”而非“深度伪造”。“信息技术”包括信息传递过程中的各个方面，即信息的产生、收集、交换、存储、传输、显示、识别、提取、控制、加工和利用等技术的总和[7]，是一个上位概念；内容丰富；而“深度伪造”只涉及其中的一部分，是一个下位概念，含义有限。可见，信息技术与深度伪造技术具有属种关系，深度伪造技术包含于信息技术之中[8]。故“深度伪造”作为信息技术手段的一种，其当然受本条文规制，即任何人不得利用深度伪造技术侵犯他人声音权益。

5.2. 规制深度伪造侵犯声音权益的可行方式

规制深度伪造行为，必须明确各方所担负的责任。

首先，对深度伪造计算机软件或者手机APP (以下统称深度伪造软件)的开发者、提供深度伪造音频服务的制作者课以强制标注义务[2]。作为侵犯声音权益行为链条的源头主体，其所掌握的技术水平远高于行为链其他主体，对该主体采取措施能够更容易也是更有成效地从技术方面减少侵权行为的发生。可以要求深度伪造软件开发者在自己的软件中写入相关程序、要求深度伪造音频服务者在自己的制作成品中强制标注例如“本内容为深度伪造效果”的提示声音，从而有助于他人分辨音频真伪，防止不法分子通过以假乱真的方式侵犯他人声音权益。

其次，对音频播放平台课以预先审查义务和强制用户实名制义务。在数字时代的当下，音频的传播速度迎来了质的飞越，一段音频上传之后仅需几秒就能做到“家喻户晓”。而音频播放平台作为音频传播者，一旦发生利用深度伪造技术侵犯声音权益的案件，其对权益人损害的产生、扩大所起到的作用甚至会大于伪造音频的制造者。因此，从音频传播这一环节加以规制是必要的。一方面，音频播放平台应当对用户上传的音频进行审查，拒绝侵权音频的上传服务。音频播放平台作为先进技术的掌握者，其有能力也有义务以自己所掌握的技术来开发审查程序以对抗深度伪造侵权。而就对音频播放平台课以的究竟是实质审查义务还是形式审查义务而言，虽然音频播放平台拥有一定的先进技术，但由于“术业有专攻”，其掌握的是音频播放而非深度伪造相关技术，如果对音频播放平台课以实质审查义务，平台出于现有技术的限制其无法实现查清音频是否为伪造的原因，为了规避实质审查不力带来的侵权索赔后果，其必然会采取措施把法律风险转移给用户，比如严格限制音频的上传，同时收集、掌控平台用户的更多真实信息以便日后追责等等，这是商事主体趋利避害天性的必然结果，而用户和音频产品同时减少，对我国的自媒体产业的伤害是巨大的，因此笔者认为实质审查义务太过沉重也并不现实，形式审查义务更为合理。另一方面，各平台应当强制其用户实名。实名制是实现对违法网络用户追责的最低要求，同时，很多用户之所以会在网络中从事不道德甚至违法行为，就是出于网络匿名制下无法追责的心理，实名制也会起到规制该部分用户行为的效果，从而减少侵犯他人声音权益行为的发生。

最后，完善追究深度伪造音频行为人民事责任的相关规则。这是整个声音权益保护构建环节中最重要的一环。可以说，没有利用深度伪造技术伪造他人音频的人，就不会有侵权行为的发生，也就不会有生成、传播等后续环节如何实现声音权益保护问题的讨论。离开实践空谈保护规则是不可取的，实现对声音权益的妥善保护必须从实践出发。但在如今我国的司法实践之中，可供研究和借鉴的相关案例几乎是空白状态，因此笔者也只能从抽象层面给出自己的见解。笔者认为，首先，就侵权责任的构成要件而言，如果前两部分的规制措施得到落实，那么侵权主体、侵权行为的明确必然会使诉讼证据的获取难度降低，相关的司法案件会增多，权益人的胜诉概率也会增加；其次，就侵权行为人的责任体系而言，既应当承担停止侵害、消除影响、恢复名誉、赔礼道歉的非财产性责任，也应当承担物质损害赔偿、精神损害赔偿的财产性责任，具体责任的轻重应当由法官根据权益人的损失和行为人的获利情况、主观恶性、经济负担能力以及侵权行为的恶劣程度、社会影响等因素综合考量。

6. 结语

现如今，高新技术的迅猛发展不仅方便了生活，造福了人类，同时也诞生了防不胜防的新型侵权手段，对个人权益、社会秩序以及国家安全造成了严重威胁。技术本身是中立的，这一点毫无疑问，但技术中立不是侵犯他人民事权益的理由。利用深度伪造技术侵犯他人声音权益，是受法律规制的违法行为。在现有规范无法有效防止深度伪造技术侵犯他人声音权益的今天，讨论如何设计相应规则以实现对声音权益人的妥善保护是必要而紧急的。“一项技术如何实施会带来如何的社会影响，技术正负价值比例如何，都需要法律予以自主的、前瞻的、现代化回应”[9]。在发现和防止深度伪造技术带来的不利后果的同时，我们也要深刻地认识到深度伪造技术为各行各业带来的有利影响，在充分利用深度伪造技术为人类社会带来福祉的基础上，去讨论如何规制而非禁止，决不可因噎废食。

参考文献

[1] 红星新闻. 世界首例 AI 诈骗案? 英国高管接“老板”电话, 被骗 22 万欧元[EB/OL]. https://page.om.qq.com/page/O-g1hNoDiFu1YtnarvQapNiw0, 2022-10-16.

[2] 冯婉淇. “深度伪造”背景下人格权保护的困境与应对[J]. 人权法学, 2022, 1(1): 97-114+157-158.

[3] 高阳. 论深度伪造技术中的自然人精神性人格权保护[D]: [硕士学位论文]. 济南: 山东大学, 2021. https://doi.org/10.27272/d.cnki.gshdu.2021.006324

[4] 宋凡. 《民法典》时代下“深度伪造”科技风险与应对模式[J]. 中国电信业, 2020(10): 28-32.

[5] 龙坤, 马钺, 朱启超. 深度伪造对国家安全的挑战及应对[J]. 信息安全与通信保密, 2019(10): 21-34.

[6] Arık, S.O., *et al.* (2018) Neural Voice Cloning with a Few Samples. arXiv.org

[7] 叶斌, 黄洪桥, 余阳, 主编. 信息技术基础[M]. 重庆: 重庆大学出版社, 201: 4-5.

[8] 孙道锐, 张丽洁. 利用信息技术手段伪造侵权的法教义学分析[J]. 法律适用, 2021(5): 166-176.

[9] 吴梓源, 游中豪. AI 侵权的理论逻辑与解决路径——基于对“技术中立”的廓清[J]. 福建师范大学学报(哲学社会科学版), 2018(5): 12.