

深度伪造肖像侵权的教义学阐释

——以《民法典》第1019条为中心

刘子奇

中国政法大学证据科学研究院，北京

收稿日期：2026年5月14日；录用日期：2026年5月27日；发布日期：2026年6月25日

摘要

《民法典》第1019条第1款将“利用信息技术手段伪造”规定为独立的肖像侵权类型，但该条款的规范意涵、与“未经同意不得制作”的关系以及实际规制效果等方面仍存在教义学争议。文章以法教义学为基本方法，围绕第1019条展开体系化阐释，论证该条款区别于“丑化”、“污损”的独立侵权属性及其填补传统侵权类型功能不足、拓展人格权保护范围、构建多元归责结构的三重独立价值。针对侵权认定中的核心争议，提出“可识别性”标准的场景化调适方案及举证责任适度倒置的应对路径，并构建制作者、网络平台、技术提供者三方责任分层分配机制，以期为该条款的司法适用提供融贯的解释论方案。

关键词

深度伪造，《民法典》第1019条，肖像权，分层责任

A Doctrinal Interpretation of the Infringement of Deep Forgery Portrait

—Focusing on Article 1019 of the *Civil Code*

Ziqi Liu

Institute of Evidence Law and Forensic Science, China University of Political Science and Law, Beijing

Received: May 14, 2026; accepted: May 27, 2026; published: June 25, 2026

Abstract

Article 1019, paragraph 1 of the *Civil Code* defines “forgery by means of information technology” as

an independent type of portrait infringement. However, there are still doctrinal disputes on the normative meaning of this article, the relationship with “no production without consent”, and the actual regulatory effect. Based on legal dogmatics, this paper systematically explains Article 1019 and demonstrates its independent tort attribute, which is different from “ugliness” and “defilement”, and its triple independent value of filling the functional deficiency of traditional tort types, expanding the protection scope of personality rights, and constructing a multi-element liability structure. In view of the core dispute in the determination of infringement, this paper puts forward the scenario adjustment scheme of “identifiability” standard and the appropriate inversion of burden of proof, and constructs a hierarchical distribution mechanism of responsibilities among producers, network platforms, and technology providers, with a view to providing a coherent interpretation scheme for the judicial application of this clause.

Keywords

Deep Forgery, Article 1019th of the *Civil Code*, Portrait Right, Hierarchical Responsibility

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

深度伪造(Deepfake)技术依托生成对抗网络(GAN),通过对目标人物面部特征、表情动作的系统性学习,实现高度逼真的图像与视频伪造[1]。该技术具有高度真实性、泛在普适性和快速演化性特征,普通人未经专业训练难以辨别真伪。随着“一键换脸”等应用程序的普及,深度伪造技术对现有肖像权保护体系形成系统性冲击:侵权客体呈现复合性,侵权主体趋于分散化匿名化,被侵权人面临严峻的举证困境。《中华人民共和国民法典》(后文简称《民法典》)第1019条¹第1款将“利用信息技术手段伪造”法定化为独立于“丑化”、“污损”的肖像侵权类型,但引发了若干教义学争议:其一,利用技术手段伪造并不必然导致丑化或污损效果,三者并列是否妥当;其二,该条款是否具有独立于第2款“未经同意不得制作”的规范价值;其三,第1019条在实际适用中能否有效规制深度伪造侵权。本文以法教义学为基本方法,围绕上述争议展开体系化阐释。

2. 深度伪造技术特征与侵权风险的类型化

深度伪造对个人权利的侵害呈现显著的复合性特征,往往同时触发多项人格权及财产权的保护机制。

在人格权领域,“深度伪造”视频在视听呈现上,主要使用的人格标识是肖像和声音,根据《民法典》第1023条²对自然人声音的保护参照适用肖像权保护规则[2]。在常见侵权场景中,制作者未经权利人同意,利用信息技术手段将他人面部形象、声音移植至特定视频中是一种明显的侵犯肖像权的行为。当伪造视频内容涉及侮辱、诽谤信息时,也将同时构成对名誉权的侵害。据调查,2019年12月全网共有14,678个深度伪造视频,其中96%属于不当内容性质[3],该行为除了对受害人隐私权与名誉权的侵害,也侵害了私人生活安宁。

¹《民法典》第1019条: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。未经肖像权人同意,不得制作、使用、公开肖像权人的肖像,但是法律另有规定的除外。

²《民法典》第1023条:对姓名等的许可使用,参照适用肖像许可使用的有关规定。对自然人声音的保护,参照适用肖像权保护的有关规定。

在个人信息领域，“深度伪造”通过提取他人的声音、面部等生物识别信息进行深度学习以生成伪造内容。根据《中华人民共和国个人信息保护法》(后文简称《个人信息保护法》)第 28 条³，生物识别信息属于敏感个人信息，一旦泄露或非法使用，将直接危及信息主体的人格尊严与人身财产安全[4]。深度伪造在未经信息主体同意的情况下，对上述可识别性信息进行提取与加工，违反了《民法典》及《个人信息保护法》关于个人信息处理的基本规则，构成对敏感个人信息的非法处理。

在财产权领域，声纹与面部特征均具有可识别性，能够精准指向特定自然人，且具有不可更改性，但因其可复制的特性，存在被非法获取的显著风险。深度伪造技术的迭代降低了此类犯罪的门槛与成本，使得利用人脸、声纹等生物识别信息侵害他人财产安全的可能性显著增强。贾章范更是指出“技术迭代愈快，运用人脸信息实施精准诈骗的速度和难度就随之降低，侵害他人财产安全的可能性就愈强”[5]。

3. “利用信息技术手段伪造”的规范意涵与独立价值

1) 规范意涵：区别于“丑化”、“污损”的独立侵权类型

从文义解释出发，“丑化”与“污损”均以肖像外观的贬损性改变为核心要素，前者侧重于歪曲、贬低肖像形象，后者侧重于破坏肖像的物理完整性。而“利用信息技术手段伪造”则依托人工智能技术，将原有的肖像转移、嫁接至他人身体或特定场景之中，其侵害本质并非外观贬损，而是对肖像主体身份的盗用与表达篡改。换言之，即使伪造后的肖像并未呈现丑化或污损效果，甚至更加“美观”，仍可能构成侵权。

三种行为方式在构成要件层面也存在显著差异：

就侵权行为而言，根据《民法典》第 1019 条第 1 款，“利用信息技术手段伪造”肖像虽然与“丑化”“污损”同样构成对肖像完整性的破坏，但破坏程度存在明显区别：“丑化”“污损”的破坏效果直观可见，而深度伪造的破坏性则更为隐蔽，往往在伪造内容经网络传播后才逐步显现。如果不单独规定“利用信息技术手段伪造”以明确其违法性，则可能难以阻断此类行为引发的连锁性损害后果。

就损害事实而言，《民法典》取消了“以营利为目的”的限制，对肖像权提供更为全面的保护。实践中利用深度伪造制作视频的行为通常不会直接导致财产损失，其损害后果主要表现为精神损害。侵权视频借助网络平台传播后，影响范围迅速扩大，对肖像权人权益造成的损害随之加剧，而精神损害本身又难以精确量化。

就主观过错而言，“丑化”、“污损”他人肖像的行为通常可推定行为人具有主观故意。而在深度伪造的场景中，制作者可能仅出于技术展示或娱乐目的使用他人肖像，其主观意图并非必然指向侵害，过错的认定需结合多种因素综合判断，因此展现出更为复杂的责任认定问题。

在因果关系层面，深度伪造侵权呈现出不同于传统肖像侵权的特点：“深度伪造”技术是所有侵权结果共同的“因”，虽然技术本身不可能成为法律上的责任主体，但因为技术提供者在特定情形下对下游侵权行为承担责任的正当性，也应当进入规范评价的视野[6]。

2) 独立价值之一：填补传统侵权类型的功能不足

有观点质疑“利用信息技术手段伪造”的独立规定是否必要，认为该行为可被第 1019 条第 2 款“未经肖像权人同意，不得制作、使用、公开肖像权人的肖像”所涵盖[7]。这种质疑虽然关注到了规范的重叠现象，但忽视了“伪造”条款不可替代的独立功能。

从规范功能来看，“未经同意不得制作”属于赋权性规范，以“知情同意”为核心机制，赋予肖像权人对其肖像使用的控制权。然而，在深度伪造场景中，“知情同意”机制面临着实质性的失灵风险。一方面，深度伪造所需的源数据往往来自网络公共空间的海量信息，制作者难以逐一获取权利人的授权；另

³《个人信息保护法》第 28 条第 2 款规定：只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

一方面，即使权利人作出了概括性的许可，也难以预见其肖像将被嫁接至何种具体场景——尤其是暴力等不可控的情境之中[8]。在此背景下，若仅依赖“未经同意不得制作”的规则，将导致在同意获取不能或概括同意效力存疑的情形下，深度伪造的违法性难以得到及时确认。

“利用信息技术手段伪造”条款的功能正在于此：它将深度伪造行为本身直接宣告为违法，不依赖于同意与否的判断，从而绕开了“同意失灵”的规制盲区。“深度伪造”具有很强的负面效应，如果不首先将其肖像侵权的违法性明确，则伪造的视频可能被进一步不当利用。在这个意义上，“利用信息技术手段伪造”条款是一种“底线规则”——即使尚未造成实际损害，利用信息技术手段伪造他人肖像的行为本身即具有不法性。

从立法技术的角度观察，《民法典》的立法者显然有意回应人工智能技术发展的现实需要。《中华人民共和国民法典人格权编(草案)(二次审议稿)》在第799条增加了“不得利用信息技术手段伪造等方式侵害他人的肖像权”的规则表述，最终在第1019条形成正式规范[9]。这一立法演进表明，“利用信息技术手段伪造”条款并非对既有规则的简单重复，而是立法者对新型技术风险的前瞻性应对。

3) 独立价值之二：保护范围的周延拓展

“利用信息技术手段伪造”的独立价值还体现在对人格权保护范围的拓展上。传统肖像侵权主要关注面部形象的未经授权使用，而深度伪造技术使得侵权形态超越了这一范畴，侵权客体呈现复合化特征。

“利用信息技术手段伪造”条款与一般人格权条款共同构成了开放性的保护结构。一方面，第1019条明确列举了具体的禁止行为；另一方面，第990条第2款⁴保留了基于人身自由、人格尊严产生其他人格权益的保护空间，为未来可能出现的新型人格利益提供了规范接口。

4) 独立价值之三：归责主体的多元构造

传统肖像侵权通常涉及侵权人与被侵权人两方主体，责任认定相对简单。而深度伪造侵权涉及技术开发者、服务提供者、内容使用者以及网络传播平台等多元主体，责任分配呈现出显著的复杂性，这一特殊性本身也构成了“利用信息技术手段伪造”条款独立规制的重要理由。

在规范体系层面，《民法典》第1019条作为基本法层面的禁止性规范，对下位法规具有统领作用。尽管《网络音视频信息服务管理规定》《互联网信息服务深度合成管理规定》等部门规章也对深度伪造作出了细化规定，但“《民法典》作为一部位阶高的法律，对其他立法具有统领性的作用。因此，要完善对‘深度伪造’技术规制的法律体系，首先应完善《民法典》第1019条”。

4. 深度伪造侵权责任的多层分配机制

1) 内容制作者的第一性责任

内容制作者直接实施了利用信息技术手段伪造他人肖像的行为，应当承担首要侵权责任，归责原则上适用过错责任原则。过错的认定应与视频内容性质相关联：涉及侮辱、诽谤等违法内容的，可推定制作者存在侵权故意；仅用于观点表达或技术展示的，过错的认定则应更为审慎。

制作者应当承担两项核心义务。其一，显著标识义务，制作者应以明显方式标注该内容系利用信息技术手段生成。《网络音视频信息服务管理规定》第11条⁵、《互联网信息服务深度合成管理规定》第14条至第16条⁶对此均有明确规定。其二，事前授权义务，在制作涉及他人肖像或声音的深度伪造内容

⁴ 《民法典》第990条第2款规定：除前款规定的人格权外，自然人享有基于人身自由、人格尊严产生的其他人格权益。

⁵ 《网络音视频信息服务管理规定》第11条第1款规定：网络音视频信息服务提供者和网络音视频信息服务使用者利用基于深度学习、虚拟现实等的新技术新应用制作、发布、传播非真实音视频信息的，应当以显著方式予以标识。

⁶ 《互联网信息服务深度合成管理规定》第14条侧重于训练数据安全与生物识别信息编辑功能的告知同意义务；第15条规定了用户真实身份信息认证与生成内容的通用标识义务；第16条则针对不同类型深度合成服务的标识要求进行了细化规定，特别强调了人脸、人声等生物识别信息编辑功能的显著标识义务与使用者单独同意要求。

前，应当取得权利人的明确同意。未履行上述义务的，制作者应承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任。

2) 网络平台的审查义务与过错认定

网络平台是深度伪造内容传播的关键节点，其责任配置应当在保护权利与促进技术创新之间寻求平衡。

在义务内容上，平台应当从单纯的事后“通知-删除”向事前预防延伸，建立分级分类的内容审核机制。具体而言，平台事前审查义务的范围和标准应当按照以下递进结构进行设计：其一，基础审查义务。平台应当在用户协议中明确禁止上传未经授权的深度伪造内容，设置关键词过滤、已知伪造内容特征库比对等基础技术筛查手段，并对用户进行真实身份信息认证。该项义务适用于所有平台，不因平台规模大小而有所区别。其二，重点监控义务。对于具有较大社会影响力的平台——参照《互联网信息服务深度合成管理规定》对“具有舆论属性或社会动员能力”的界定——还应当承担更高层次的审查义务，包括但不限于运用深度伪造识别算法对高风险内容进行自动检测、对涉及公众人物或敏感议题的合成内容进行人工复核、建立深度伪造内容特征数据库并与其他平台进行必要的信息共享。其三，及时处置义务。平台在发现或接到通知得知侵权内容后，应当在合理期限内及时采取删除、屏蔽、断开链接等措施。对于经多次通知仍反复出现的同类侵权内容，平台应当采取更为彻底的处置措施，如限制发布账号的部分功能或暂停服务。

过错的判断可以类推适用避风港规则：平台在接到权利人通知后及时采取必要措施的，对扩大损害不承担责任；若平台对显而易见的侵权内容视而不见，则可认定存在过错。只要平台对深度伪造的音视频履行了与其技术能力相匹配的实质审查义务，但因现有技术手段的客观局限未能识别出部分侵权内容，则不应对其进行追责^[10]。这一“技术能力相匹配”的判断标准，既为平台设定了可预期的合规目标，也为司法裁判提供了具有可操作性的认定依据。

3) 技术提供者的第三性责任

技术提供者处于侵权链条的上游，其责任认定涉及“技术中立”命题的判断。技术提供者责任的判断核心在于产品设计是否存在缺陷。如果技术提供者采取了内容过滤、嵌入不可移除的水印、要求用户实名注册等合理安全措施，应当认定已尽到注意义务。相反，如果技术提供者将产品设计为“一键换脸”等诱导侵权的形态，则不应享有“技术中立”的抗辩空间。软件提供者“对利用其开发的软件制作的视频负有强制添加水印等表明该视频为‘深度伪造’的标识的义务”。

为在鼓励技术创新与防范技术滥用之间寻求恰当的平衡，本文建议在技术提供者责任的认定中引入“安全港”条款。具体而言，技术提供者同时满足以下条件的，可以免除侵权责任：第一，在产品中嵌入了不可移除的标识水印，确保其生成的内容能够被追踪和识别；第二，建立了用户实名注册和身份核验机制；第三，设置了合理的内容过滤或限制生成功能，有效防止用户利用该技术生成明显违法或高度侵权风险的内容；第四，对用户协议或许可条款中明确禁止滥用技术的行为作出了清晰告知。安全港条款的核心功能在于为技术提供者提供明确、可预期的合规指引——只要技术提供者达到了法律设定的最低安全标准，即可免于承担侵权责任，从而在创新发展与风险防控之间形成良性的制度激励。

在归责方式上，考虑到技术提供者与受害者之间在信息掌握上的显著差距，对技术提供者宜采取过错推定原则，由技术提供者证明已履行安全义务或存在免责事由。当技术提供者主张适用安全港条款时，应当对其符合安全港条件的各项事实承担举证责任。

在多元主体责任衔接上，被侵权人可以根据侵权事实选择向一个或多个责任主体主张权利，各责任主体之间根据各自过错程度承担按份责任，特定情形下依法承担连带责任。

5. 结语

《民法典》第 1019 条为数字时代的肖像权保护提供了重要的规范基础。本文试图在教义学层面厘清该条款的规范意涵，并提出若干解释论方案，但所作分析仅为初步探讨。深度伪造技术的持续演进必将带来新的解释难题，第 1019 条的教义学展开仍有待理论与实践的进一步检验，期待本文能为该条款的司法适用提供些许参考。

参考文献

- [1] 王禄生. 论“深度伪造”智能技术的一体化规制[J]. 东方法学, 2019(6): 58-68.
- [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] 曹剑锋. 关于“深度合成”技术的十个误解[EB/OL]. 腾讯研究院网, 2020-05-12. <https://www.tisi.org/14419>, 2026-05-15.
- [4] 杜嘉雯, 皮勇. 人工智能时代生物识别信息刑法保护的國際視野与中国立场——从“人脸识别技术”应用下滥用信息问题切入[J]. 河北法学, 2022, 40(1): 144-167.
- [5] 贾章范. 《民法典》视野下深度伪造技术的法律风险与规则应对[J]. 东北农业大学学报(社会科学版), 2021, 19(1): 71-78.
- [6] 桂兵, 张凤逸. “深度伪造”侵犯肖像权问题研究[J]. 湖南师范大学社会科学学报, 2023, 52(6): 119-120.
- [7] 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): 166-167.
- [8] 王利明. 《民法典》人格权编的实施与未来展望[J]. 中国法学, 2026(1): 121-143.
- [9] 王博勋. 人格权编草案二审: 及时回应新情况新问题[J]. 中国人大, 2019(9): 16-17.
- [10] 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.