Open Journal of Legal Science 法学, 2026, 14(4), 282-292
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.144118

Hans汉斯

论生成式人工智能数字化人格的侵权风险以及规制路径

顾兴志

常州大学史良法学院，江苏 常州

收稿日期：2026年3月16日；录用日期：2026年3月30日；发布日期：2026年4月27日

摘　要

生成式人工智能技术下数字化人格的广泛应用已成为数字时代的重要趋势，但其引发的侵权风险与规制空白问题已成为亟待解决的法律难题。本文聚焦生成式人工智能数字化人格的侵权风险及规制路径问题，采用文献分析、比较研究等方法，从剖析侵权特殊性、梳理国内外规制现状、借鉴域外经验等角度展开研究，剖析其侵权手段隐蔽、客体多元等特殊性，梳理我国现有法律在个人信息保护、侵权责任归责等方面的规制缺陷，结合欧盟、美国等域外经验，提出构建“统一立法 + 分别立法”的双轨法律规制体系、强化技术治理措施、构建多元共治机制的规制路径，并明确生成式人工智能的链式责任分配框架，为数字化人格的法律保护提供理论支撑与实践指引。

关键词

生成式人工智能，数字化人格，侵权风险，法律规制

On the Infringement Risks and Regulatory Paths of Digital Personality in Generative Artificial Intelligence

Xingzhi Gu

Shiliang Law School, Changzhou University, Changzhou Jiangsu

Received: March 16, 2026; accepted: March 30, 2026; published: April 27, 2026

Abstract

With the iterative upgrade of generative artificial intelligence technology, the generation and

文章引用: 顾兴志. 论生成式人工智能数字化人格的侵权风险以及规制路径[J]. 法学, 2026, 14(4): 282-292.
DOI: 10.12677/ojls.2026.144118

application of digital personality have gradually become popular. While enriching digital interaction scenarios, it has also triggered many new infringement risks. Especially in the field of protecting the digital personality of the deceased, the existing laws have obvious regulatory gaps. In the scenario where generative artificial intelligence "resurrects" the deceased, the protection of the deceased's personality interests has become an urgent legal problem to be solved. This article takes the infringement risks of digital personality in generative artificial intelligence as the research starting point, analyzes the particularity of infringement under its technical characteristics, sorts out the current situation and deficiencies of domestic and foreign legal regulation, combines foreign regulatory experience, and proposes to construct a dual-track legal regulation system of "unified legislation + separate legislation", strengthen technical governance measures, and construct a regulatory path of multi-party co-governance mechanism, and clarify the chain responsibility allocation framework of generative artificial intelligence, so as to provide theoretical support and practical guidance for the legal protection of digital personality.

Keywords

Generative Artificial Intelligence, Digital Personality, Infringement Risks, Legal Regulation

1. 问题的提出

数字化人格是依托生成式人工智能技术，通过收集、分析个人肖像、声音、行为习惯等多维度数据构建出的、能够高度还原个人特征并模拟个人行为与交互的数字化虚拟形象，是个人在数字空间的延伸与具象化呈现。当前，数字化人格的应用场景不断拓展，从虚拟客服、数字偶像到个人数字分身，已逐渐融入社交、娱乐、商业等多个领域，但同时也面临着诸多严峻挑战：其一，数字化人格的生成依赖于大量个人敏感数据的收集与使用，极易引发个人信息泄露、隐私侵犯等问题；其二，生成式人工智能技术的隐蔽性使得数字化人格的侵权行为难以被察觉与认定，且侵权客体涵盖人格要素与数据权益，呈现多元复合特征，导致侵权认定与责任划分难度较大；其三，现有法律对数字化人格的法律属性界定模糊，缺乏针对性的权利保护与规制规则，难以应对技术发展带来的新型法律冲突。

2. 生成式人工智能数字化人格的背景解析与侵权风险研判

2.1. 生成式人工智能技术特性与发展现状

生成式人工智能(Generative AI)的突破性进展带来了人工智能生成内容(AIGC)的爆炸式增长，结合现有研究来看，其技术特性呈现出对大量高质量训练数据的依赖性、无法处理长尾问题、通用性有限、对特定应用场景的依赖性以及人工智能开发者固有偏见等局限性[1]。这些技术特性使得生成式人工智能在应用过程中不可避免地将人们置于信息过载、信息噪声、信息安全等负面影响之下，也为数字化人格的生成提供了技术基础。

从相关研究的视角出发，生成式人工智能生成数字化人格主要包括三个阶段：数据处理阶段、模型建构与训练阶段、内容生成与交互阶段[2]。在数据处理阶段，技术通过收集、分析并训练特定个体多维度的历史数据，解决了数字化人格的全面性与准确性问题，这一阶段需要大量收集数字化对象的肖像、声音、个人信息、隐私等个人敏感数据，是“复刻”他人、“复活”逝者的前提条件。在模型建构与训练

阶段，利用深度学习、计算机视觉、自然语言处理等技术构建出被建模对象的数字化模型，能够高度还原其外貌特征、表情动作乃至行为习惯，甚至可以模拟出没有提取到的数据，从而增强数字人的真实感。在内容生成与交互阶段，用户可以通过人机交互系统实现与数字人的互动，数字人可以在与用户的互动中进行情感计算，从而不断掌握用户的习惯以及理解用户的需求，使得互动程度不断加深。

然而，生成式人工智能技术的不成熟性也带来了诸多风险，例如算法的可解释性弱、可泛化边界未知、逻辑推理能力有限等技术缺陷，可能导致生成的内容存在偏见或冒犯性言论，甚至引发社会矛盾[1]。

有研究对该问题进行了探讨，生成式人工智能训练数据的风险主要包括训练数据侵权风险、训练数据偏差风险和训练数据泄露风险[3]。训练数据侵权风险主要表现为大模型预训练时使用作品类数据可能违反《著作权法》的规定，使用个人信息数据可能违反《个人信息保护法》的规定；训练数据偏差风险包括价值性偏差风险、时效性偏差风险和真实性偏差风险；训练数据泄露风险则包括面向开发者的数据泄露风险和面向攻击者的数据泄露风险，攻击者可以通过技术手段从大模型中反向抽取出用于预训练的原始训练数据，或者通过特定的提示词诱导大模型输出其他用户所输入的外部数据[3]。同时，从其他研究的视角来看，生成式人工智能的技术特性还可能导致数字人格的异化，影响主体的自我认知与身份认同[4]。故而结合现有研究可以认为，生成式人工智能的技术迭代速度较快，现有法律难以跟上技术发展的步伐，导致规制滞后性问题凸显[5]。

2.2. 数字化人格法律属性界定

对于数字化人格的法律属性，目前学界尚未形成统一的界定，而与之相关的数据产权理论的争议也为这一问题的厘清提供了理论参照。当前学界关于数据产权的代表性观点主要分为三类：其一为确权说，该观点认为数据产权是一种与物权、知识产权并列的新型财产权，应明确数据处理者对数据的排他性财产权利，以激励数据的开发与利用[6]；其二为非确权说，该观点认为数据确权会引发反公地悲剧，导致数据流通受阻，因此应搁置传统的权属争议，以行为规制的方式调整数据利用关系[7]；其三为权益束说，该观点认为数据并非单一的权利客体，而是集合了所有权、使用权、收益权等多项权益的权利束，应针对不同主体、不同场景分别界定权益边界[4]。

基于上述理论梳理可以发现，数据产权理论的核心争议围绕数据的财产性利益展开，而数字化人格虽依托个人数据生成，但其核心并非财产性利益，而是人格利益。因此，数字化人格不能简单适用数据产权的财产权保护路径，而应作为既有权利的延伸进行保护：其本质是个人的肖像、姓名、隐私、名誉等人格权益在数字空间的延伸，是个人在数字环境中的人格具象化呈现，兼具数据属性与人格属性，其保护的核心是维护个人的人格尊严与自主决定权，而非财产利益的分配。

传统人格主要存在于物理空间，其行使依赖于主体的物理行为，权利义务基于现实社会关系产生；而数字化人格存在于网络空间，可脱离主体的物理身体独立存在，其权利义务基于数据交互关系产生，涉及个人信息保护、隐私权、肖像权等多个方面[6]。具体区别体现在以下几个方面：首先，存在空间不同。传统人格存在于物理空间，受物理时空的限制；而数字化人格存在于网络空间，其传播与交互不受物理时空的约束[4]。其次，表现形式不同。传统人格通过主体的物理行为和社会交往来体现，具有具象的物理载体；而数字化人格通过数据、算法等技术手段生成，以信息化的形式呈现，可被复制、传播和修改[4]。第三，权利义务范围不同。传统人格的权利义务主要围绕现实中的人格尊严、身体完整等展开；而数字化人格的权利义务还涉及数据的收集、使用、传播等环节，包括个人信息的控制权、数字化形象的使用权等新型权益[2]。

通过对比可以看出，数字化人格的特殊性决定了其侵权风险与传统人格侵权存在明显差异，这些差异也催生了新型的侵权类型，例如未经授权生成他人数字化人格、利用数字化人格实施网络欺诈、篡改

他人数字化形象等，这些侵权行为都需要针对性的规制规则进行约束。

2.3. 新型侵权特殊性

生成式人工智能数字化人格的侵权风险具有不同于传统人格侵权的特殊性，主要体现在以下几个方面：首先，侵权手段的技术性与隐蔽性。生成式人工智能技术可以通过深度伪造技术创建和修改图片、影像等内容，将某人的肖像换成他人的肖像，生成高度仿真、难以甄别的图像、视频，这种技术使得侵权行为更加隐蔽，难以被发现。例如，未经肖像权人许可，擅自制作、使用或公开其肖像，或者通过深度伪造技术生成与真实人物高度相似的虚假视频或图像，并借此制造谣言、误导公众或实施网络欺凌等，对肖像权人的形象造成不可逆转的损害[2]。实践中，此类侵权已引发多起司法纠纷，最高人民法院发布的 2024 年知识产权典型案例中，陈某诉上海易某公司 AI 换脸案便具有代表性，该案中被告利用 AI 技术对他人原创视频进行局部换脸合成，法院明确该行为不构成合理使用，网络服务平台不得以技术中立为由逃避侵权责任[8]。此外，北京互联网法院审理的何某诉某科技公司案中，被告未经许可使用原告的姓名、肖像创设 AI 虚拟人物，将原告的人格特点投射到 AI 角色上，最终被认定构成对姓名权与肖像权的侵害[6]。

其次，侵权客体的多元性与复杂性。生成式人工智能数字化人格的侵权客体不仅包括个人肖像、个人信息、个人隐私、个人名誉等人格权益，还包括数字人格本身，侵权客体的多元性使得侵权认定更加复杂。例如，在人工智能生成数字化人格的过程中，数字人的订购客户很可能未经被数字化对象本人或其近亲属的同意，擅自使用其生活中的私密信息生成数字人，并进行公开展示，这一行为既构成对被数字化对象隐私权或隐私利益的侵害，也构成对数字人格的侵害[2]。在数字永生这一新兴场景中，此类问题尤为突出，部分商家提供的 AI“复活”逝者服务，未经死者近亲属同意便收集逝者的社交数据、影像资料生成数字化人格并进行商业化利用，不仅侵害了死者的人格利益，也损害了近亲属的情感利益，此类行为已引发诸多争议[9]。

第三，侵权影响的广泛性与持续性。AIGC 事故影响客体的多元性、波及范围的广泛性、潜在危害的复杂未知性，使得侵权行为的影响更加广泛，并且由于网络信息的传播速度快、范围广，侵权影响具有持续性，难以消除[1]。例如，数字人在模拟场景中生成的内容或作出的虚拟行为存在不当乃至有悖伦理道德，交互对象很可能将其归咎于被数字化的主体，从而对其名誉造成难以挽回的损害，并且这种损害会随着网络信息的传播而不断扩大。

第四，侵权认定的困难性。由于生成式人工智能技术的不透明性和算法的复杂性，侵权认定往往面临困难，难以确定侵权主体和侵权责任。尤其是算法的不透明性、内在偏见与算法推荐技术固有的“信息茧房”效应相互叠加，使得公众在接收数字人相关信息时难以分辨虚拟与现实的界限，极易受到误导，从而难以确定侵权行为的实施者和责任主体。

此外，数字空间的侵权还存在特殊性，例如数字名誉的受损可能无法映射到现实社会评价，数字身体的侵害无法作用于现实身体，这些会导致传统的侵权认定标准难以适用。又比如说，假设某一虚拟主体因其在数字空间遭到的诽谤或侮辱导致其社会评价降低，但其现实中的控制者却不会受到任何影响，这种情况下，传统的名誉权侵权认定标准也将难以适用[5]。另外，生成式人工智能内容的风险也增加了侵权认定的难度，主要包括数据安全风险、劣质信息泛滥、训练数据来源合法性争议等。数据安全风险表现为训练数据可能存在准确性不足或系统性偏差，一旦关键数据外泄，将对企业运营、行业生态造成直接经济损失及品牌信誉损害；劣质信息泛滥则是指生成式人工智能凭借其强大的算力可批量生成虚假文本、编造不实信息，导致事实性错误泛滥；训练数据来源合法性争议则体现在海量数据训练场景下，要求开发者逐一对用户履行知情同意程序存在现实困难，同时训练数据若源于受著作权法保护的作品，

未经著作权人授权可能构成侵权行为[10]。

3. 生成式人工智能数字化人格侵权的法律规制现状与问题剖析

3.1. 我国生成式人工智能数字化人格规制的现状与不足

3.1.1. 现有规制现状

我国在生成式人工智能法律规制方面已经取得了一定的进展，2023 年 7 月发布的《生成式人工智能服务管理暂行办法》是我国首部专门针对生成式人工智能的法规，该办法从内容合规、算法透明、数据安全等维度提出了明确要求，例如禁止生成危害国家安全或社会稳定的信息，要求在算法设计、数据标注等环节防止歧视性输出[11]。此外，我国的《民法典》《个人信息保护法》《数据安全法》《网络安全法》等法律也为生成式人工智能数字化人格的保护提供了一定的法律基础。例如，《民法典》人格权编对肖像权、隐私权、个人信息保护等作出了规定，为数字化人格的保护提供了基本的法律依据[12]。

3.1.2. 现存规制不足

(1) 个人信息保护法律的局限性

现有个人信息保护法律在应对生成式人工智能数字化人格侵权问题时存在明显不足。在生成式人工智能训练语料的个人信息保护方面，《个人信息保护法》虽然规定了个人信息处理的基本原则和规则，但对于海量训练数据的处理，尤其是在生成式人工智能大模型训练场景下，现有法律的规定难以有效适用[13]。究其原因，生成式人工智能训练数据多通过爬虫抓取、公开数据聚合等方式批量获取，往往未对个人信息主体履行充分的告知义务，甚至未告知其信息将被用于生成式人工智能训练，而《个人信息保护法》第 6 条规定的目的限制原则，要求信息处理者在收集个人信息时应有明确、合理的目的，且在后续的处理过程中不偏离此目的，但在生成式人工智能训练中，训练数据的收集往往是大规模无差别的，且处理目的具有一定的模糊性，难以严格符合目的限制原则的要求，这导致个人信息主体的知情权和决定权被侵害，其信息被用于生成数字化人格却不知情。此外，现有法律对于个人信息的匿名化处理规定存在漏洞，虽然《个人信息保护法》第 73 条将“无法识别”和“不能复原”作为匿名化的双重标准，但实践中，由于技术追溯能力日益增强，匿名信息因技术进步仍存在被还原识别的风险，例如通过关联其他公开数据即可实现对匿名个体的身份定位，这些被还原的个人信息可能被用于生成该个体的数字化人格，进而引发肖像权、隐私权等侵权问题，使得数字化人格的个人信息保护面临严峻挑战[2]。

(2) 侵权责任归责原则的缺陷

在侵权责任归责原则方面，现有法律的规定难以适应生成式人工智能数字化人格侵权的特殊性。传统侵权责任以过错责任原则为基础，但生成式人工智能技术的不透明性和算法的复杂性使得过错认定变得极为困难。究其原因，生成式人工智能的算法具有“黑箱”特性，服务提供者无法清晰解释算法的决策逻辑和数据处理过程，法院难以通过技术手段查证侵权行为是否由服务提供者的过错导致，例如无法确定是算法设计缺陷还是数据标注问题引发了侵权内容的生成，即使受害人能够证明自己的数字化人格被侵权，也难以证明服务提供者存在过错，进而无法主张侵权责任。虽然有研究提出对生成式人工智能服务提供者适用过错推定责任[7]，但现有法律并未明确规定这一归责原则，导致在司法实践中缺乏统一的标准，不同法院对同类案件的判决结果差异较大，受害人的维权难度极大。此外，现行侵权责任架构无法妥善处理多主体的义务承担问题，生成式人工智能的应用涉及技术研发者、技术持有者、数据供应者等多圈层的主体，现有法律对各主体的责任划分不够明确，例如数据供应者提供了侵权的个人数据、模型开发者的算法存在偏见漏洞、服务应用者未履行内容审核义务时，各主体的责任边界模糊，容易导致责任推诿，比如某生成式人工智能平台生成了侵权的数字化人格内容，平台运营者主张是模型开发者

的算法问题，模型开发者主张是数据供应者提供的侵权数据，最终受害人无法确定追责对象，权益难以得到保障[14]。

(3) 数字人格保护的法律空白

现有法律对于数字人格的保护存在明显的法律空白。虽然《民法典》人格权编对人格权益的保护作出了规定，但对于数字化人格这一新型人格权益，现有法律并未明确其法律地位和保护方式。究其原因，《民法典》的人格权编主要针对现实物理空间的人格权益，未充分涵盖数字空间中人格权益的延伸形态，数字化人格的权利内容、侵权认定标准、救济方式等都缺乏明确的法律规定，例如对于数字人格的商业化使用、虚拟形象的篡改等行为，难以直接适用现有人格权的保护规则，比如某平台未经授权将他人的数字化人格用于广告宣传，受害人无法依据《民法典》人格权编的规定主张权利，因为现有规定未将数字人格纳入保护范围，导致在数字化人格遭受侵权时，受害人难以获得有效的法律救济。此外，现有法律对于死者数字化人格的保护也缺乏明确规定，在生成式人工智能“复活”逝者的场景下，死者的人格利益如何保护成为一个亟待解决的问题，例如死者近亲属是否有权主张死者数字化人格的肖像权、隐私权，以及保护的期限和范围等都没有明确规定，比如某平台未经死者近亲属同意，生成死者的数字化人格用于商业宣传，死者近亲属无法依据现有法律主张维权，无法有效应对逝者数字化人格被不当使用的侵权问题。

(4) 法律体系与规则协调不足

首先，现有法律规定较为分散，缺乏统一的人工智能基本法，导致各领域的规制规则不够协调[11]。当前我国针对数字化人格的规制规则分散在《民法典》《个人信息保护法》《数据安全法》以及《生成式人工智能服务管理暂行办法》等多部法律法规和规章中，不同规则之间存在衔接不足的问题，例如《个人信息保护法》要求处理个人信息需要告知同意，而《数据安全法》要求保障数据安全，两者在生成式人工智能训练数据的合规处理上缺乏统一的协调机制，导致平台不知道如何同时满足两部法律的要求，容易出现监管真空或重复监管的情况，比如平台按照《个人信息保护法》的要求告知了用户，但未按照《数据安全法》的要求采取足够的安全措施，导致用户信息泄露被用于生成数字化人格。其次，《生成式人工智能服务管理暂行办法》属于部门规章，法律位阶较低，难以对数字化人格相关的全领域进行有效规制，例如无法约束跨境提供生成式人工智能服务的主体，这些跨境平台可以不受我国法律约束，随意收集我国用户的信息生成数字化人格，进而引发侵权问题，也难以对上下游的技术研发、数据供应等环节形成有效管控，比如数据供应者提供侵权数据，由于缺乏上位法的约束，难以对其进行追责。再次，对于生成式人工智能使用者的注意义务规定不够明确，有研究指出我国现行规章制度主要聚焦于人工智能的技术风险治理与服务提供者监管，而未直接规范使用者[15]。当使用者利用生成式人工智能生成侵权内容、传播虚假信息时，难以依据明确的法律规定认定其责任，例如使用者未经授权使用他人信息生成数字化人格，并在网络上传播，现有法律未明确其应承担的具体责任，导致受害人无法向使用者主张权利。 最后，对于生成式人工智能生成数字化人格内容的版权归属问题缺乏明确规定，现有法律对于人工智能生成内容是否构成作品、版权归属于谁等问题没有作出明确规定，导致实践中存在大量的版权争议[16]，例如利用生成式人工智能生成的数字化人格内容的版权归属不明确，平台和使用者都主张对内容享有权利，容易引发侵权纠纷。

3.2. 域外法律规制的经验借鉴

3.2.1. 主要区域的规制经验

(1) 欧盟《人工智能法》的风险分级规制

欧盟《人工智能法》采取了风险分级的规制进路，将涉及数字化人格的人工智能应用按风险等级进

行分类规制，分为禁止性风险、高风险、有限风险和最小风险四类[17]。对于涉及数字化人格的高风险人工智能应用，欧盟《人工智能法》提出了一系列事前规制义务，包括建立风险管理系统、规范数据治理、编制和更新技术性文件、记录保存、保障透明度、提供必要信息、设置人为监督、确保准确性、稳健性与网络安全保障等。此外，还对这类高风险应用进行了事中与事后规制，要求提供者建立上市后监测系统，及时报告严重事件，并在不符合要求时采取纠正措施[17]。这种风险分级规制的方式为生成式人工智能数字化人格的规制提供了有益借鉴，能够根据不同风险等级采取针对性的规制措施，提高规制的有效性。

(2) 美国的行业自律与法律结合规制

美国在数字化人格相关的生成式人工智能规制方面采取了行业自律与法律规制相结合的方式。在数字化人格相关的知识产权保护方面，美国版权局以“独创性”为判断基础，认为涉及数字化人格的 AIGC 只有在具有“作者的创造性表达”时才可能受到版权法保护，并且只对人类作者完成的部分进行版权登记，对人工智能生成的部分不予登记[18]。在数字化人格侵权责任方面，美国法院在处理相关案件时，通常会考虑 fair use (合理使用)原则，判断使用版权内容训练生成式人工智能是否构成合理使用[19]。例如，在 Authors Guild v Google Inc 和 Authors Guild Inc v HathiTrust 案件中，法院认为大规模扫描和复制书籍用于搜索和展示片段的行为属于合理使用。此外，美国还通过制定相关的指南和政策，引导生成式人工智能在数字化人格领域的健康发展，例如美国版权局发布的《版权登记指南：包含人工智能生成材料的作品》[16]。

3.2.2. 特定场景下的规制经验(元宇宙)

在元宇宙这一特定应用场景下，数字化人格的法律规制面临更多的挑战，欧盟、美国等国家和地区也针对该场景探索了相应的规制措施：有研究指出，元宇宙中的生成式人工智能在数字化人格领域存在内容生成的虚假信息风险、隐私保护风险、知识产权争议等问题[20]。为应对这些问题，欧盟《人工智能法》将在元宇宙中使用生物数据生成数字化人格的人工智能应用列为高风险应用，要求进行严格的风险评估和安全措施[20]。相关研究指出，一些国家还注重加强元宇宙中的数据保护，要求元宇宙平台严格遵守数据保护法规，确保用户的个人信息和隐私得到有效保护，防止数字化人格被不当使用[21]。

4. 生成式人工智能数字化人格侵权的规制路径与链式责任分配

4.1. 完善法律规制体系

4.1.1. 协调法律体系，构建“统一立法 + 分别立法”的双轨模式

针对现有法律体系分散的问题，结合现有研究来看，我国人工智能立法应采取“统一立法 + 分别立法”的双轨模式[22]，在制定统一的《人工智能基本法》的基础上，针对数字化人格领域的人工智能应用制定专门的法规。对于生成式人工智能数字化人格的规制，首先应通过《人工智能基本法》明确数字化人格的法律地位、保护范围和基本原则，为数字化人格的保护提供统一的法律基础。在此基础上，分别立法需聚焦高风险领域进行针对性规制，具体包括：一是涉及生物识别数据的数字化人格生成领域，针对 AI 换脸、声音克隆等深度合成应用，细化《互联网信息服务深度合成管理规定》的合规要求，明确生物特征数据的收集与使用规则；二是死者数字化人格的商业化利用领域，针对 AI“复活”逝者这类新兴服务，制定专门的规制条款，明确近亲属的同意权与维权路径；三是虚拟偶像、数字代言人的商业代言领域，明确数字代言人的广告合规要求与责任归属；四是元宇宙场景下的数字化人格交互领域，针对虚拟空间中的人格侵害行为，制定专门的场景化规则。此外，还应完善相关的配套法规，如在《个人信息保护法》中增加关于生成式人工智能训练数据中个人信息保护的专门条款，明确训练数据的收集、处理、使用的规则，以及个人信息主体的权利和信息处理者的义务[13]。

4.1.2. 填补数字人格保护的法律空白，明确数字化人格的法律保护路径

针对数字人格保护的法律空白，结合现有研究来看，在生命数字化进程中，数字自我的法律保护需要从外在表征和内在本质两个维度展开[23]。对于数字化人格的法律保护，应充分挖掘《民法典》的规范潜力，通过扩张解释将数字名誉、数字人格标识等新型权益纳入法律保护范围。例如，对于数字名誉的保护，可以适用《民法典》第1024条，将数字空间中的社会评价纳入名誉的范畴，当他人在数字空间对数字化人格进行侮辱、诽谤时，认定为对名誉权的侵害。对于数字身体的保护，可以适用《民法典》第1003条、第1004条等条文，考察侵害行为是否损及当事人的身体完整、行动自由、身体信息与身体尊严[5]。此外，还应建立数字化人格的专门保护机制，例如设立数字化人格的登记制度，明确数字化人格的归属和权利主体，为数字化人格的保护提供明确的依据。

4.1.3. 调整侵权责任归责原则，完善侵权责任制度

针对侵权责任归责原则的缺陷，在侵权责任制度方面，应明确生成式人工智能价值链上各主体的责任划分。有研究指出，应沿着生成式人工智能价值链划分侵权责任，即沿着基础模型开发、系统集成、服务应用三个关键环节，针对各环节所涉责任主体分别设置合理的注意义务，以违反注意义务作为侵权过错判断依据[14]。对于基础模型开发者，应承担训练数据合规审查、算法透明度保障等义务；对于系统集成者，应承担模型安全评估、内容过滤等义务；对于服务应用者，应承担用户管理、侵权内容及时处理等义务。此外，还应完善过错推定责任制度，对于生成式人工智能服务提供者的侵权责任，适用过错推定责任，由服务提供者证明自己没有过错，否则应承担侵权责任[7]。有研究指出，生成式人工智能侵权责任的认定需要区分不同的主体类型，对于基础模型提供者和应用服务提供者应适用不同的归责原则[24]，这为完善侵权责任制度提供了思路。同时，应建立侵权责任的分担机制，当多个主体共同侵权时，根据各主体的过错程度和行为对损害结果的影响程度，合理分配责任[25]。还有研究指出，生成式人工智能服务提供者的间接侵权责任应当采用分层判定的方式，根据服务提供者的过错程度和行为与损害结果的因果关系来确定责任[26]，这为链式责任分配机制的构建提供了参考。

4.1.4. 完善个人信息保护规则，强化训练数据安全

针对个人信息保护法律的局限性，应在《个人信息保护法》的修订中增加关于生成式人工智能训练数据中个人信息保护的专门条款，明确训练数据的收集、处理、使用的规则，以及个人信息主体的权利和信息处理者的义务。例如，要求开发者增设“显著标识义务”，在收集和使用个人信息时，明确告知个人信息主体其信息将用于生成式人工智能训练，并获得其明确同意；要求开发者采取技术措施对训练数据进行匿名化处理，降低数据泄露的风险；建立训练数据的分类分级管理制度，对敏感个人信息采取更为严格的保护措施，例如加密存储、访问控制等[13]。

4.1.5. 借鉴域外法律规制经验

结合本文第三章梳理的域外规制经验，我国在生成式人工智能数字化人格侵权规制中，可针对性地进行本土化转化：1. 对欧盟《人工智能法》的风险分级模式，可结合我国《生成式人工智能服务管理暂行办法》的现有框架，细化数字化人格相关应用的风险分级标准，将涉及死者数字化人格、私密信息使用的场景列为高风险应用，设置专门的合规审查与安全保障要求[17]。2. 对于美国的知识产权与侵权责任规制经验，可在我国《著作权法》的修订中明确生成式人工智能生成数字化人格内容的版权认定规则，参考fair use原则的合理边界，划定训练数据使用的合理范围，平衡版权保护与技术创新[18] [19]。3. 针对元宇宙场景的规制经验，可在我国的元宇宙相关规制文件中增设数字化人格保护条款，明确元宇宙平台在数据保护、内容审核中的责任，防范虚拟空间中的数字化人格侵权风险[27]。

4.2. 强化技术治理措施

4.2.1. 加强训练数据的安全保护

生成式人工智能训练数据的安全保护是防范数字化人格侵权的关键。有相关研究指出，应通过加强开发者的法定义务，督促其防范训练数据的泄露风险[3]。例如，要求开发者增设“显著标识义务”，在收集和使用个人信息时，明确告知个人信息主体其信息将用于生成式人工智能训练，并获得其明确同意。同时，开发者应采取技术措施对训练数据进行匿名化处理，降低数据泄露的风险。此外，还应建立训练数据的分类分级管理制度，对敏感个人信息采取更为严格的保护措施，例如加密存储、访问控制等[13]。对于开源模型的训练数据，应建立数据来源追溯机制，确保数据的合法性和合规性[28]。

4.2.2. 提升算法透明度和可解释性

算法的不透明性是生成式人工智能数字化人格侵权认定困难的重要原因之一。有学者提出，应通过技术治理工具的嵌入，提升算法的透明度和可解释性[1]。但算法透明并非绝对的全维度公开，而是应构建分层的透明度义务，以平衡监管需求与企业的知识产权保护。具体而言：其一，针对监管机构，要求服务提供者向监管部门备案算法的基本架构、训练数据的来源、数据处理的基本规则，这部分内容仅对监管者开放，不向社会公开，以保护企业的商业秘密；其二，针对普通用户，要求服务提供者以通俗易懂的方式，向用户解释算法的基本决策逻辑，例如在生成数字化人格时，告知用户该应用会收集哪些类型的个人数据，数据的使用范围，以及可能存在的风险，无需向用户公开算法的代码、模型权重等核心技术信息；其三，针对社会公众，仅需要公开算法的伦理准则、合规情况等宏观信息，无需披露核心技术细节。同时，应建立算法解释制度，当算法对用户的权益产生重大影响时，用户有权要求服务提供者对算法的决策结果进行解释。此外，还应加强算法审计，定期对算法进行评估，检查算法是否存在偏见、歧视等问题，及时进行调整和优化[27]。

4.2.3. 建立侵权监测与预警机制

为了及时发现和防范生成式人工智能数字化人格侵权行为，应建立侵权监测与预警机制。可以利用人工智能技术本身对生成式人工智能的输出内容进行监测，识别可能存在侵权风险的内容，例如通过关键词过滤、图像识别等技术，发现未经授权使用他人肖像、个人信息等内容。同时，建立侵权预警平台，当发现侵权风险时，及时向相关主体发出预警，提醒其采取措施防范侵权行为的发生。此外，还应建立侵权举报机制，鼓励用户举报侵权行为，形成全社会共同监督的氛围[10]。

4.2.4. 加强技术标准建设

技术标准是规范生成式人工智能发展的重要依据。应制定生成式人工智能数字化人格保护的技术标准，明确数字化人格的生成、使用、交互等环节的技术要求，例如数据采集的标准、算法设计的标准、内容生成的标准等。同时，应建立技术标准的更新机制，随着技术的发展及时更新技术标准，确保技术标准的有效性和适应性。此外，还应加强技术标准的执行监督，对不符合技术标准的生成式人工智能应用进行整改，确保技术标准得到有效落实[29]。

4.3. 构建多元共治机制

4.3.1. 构建“多元 + 协调 + 制衡”的治理参与模式

现有研究提出，生成式人工智能治理需要政府、企业、社会三方形成“多元 + 协调 + 制衡”的治理参与模式[1]。在生成式人工智能数字化人格侵权的规制中，政府应发挥主导作用，制定相关的法律法规和政策，加强监管和执法，保障数字化人格的合法权益。企业应承担主体责任，遵守法律法规和技术

标准，加强内部管理，采取措施防范侵权行为的发生。社会力量应积极参与，包括行业协会、学术机构、社会组织等，行业协会可以制定行业自律规范，引导企业规范经营；学术机构可以开展相关的研究，为规制提供理论支持；社会组织可以开展宣传教育活动，提高公众的数字素养和维权意识。

4.3.2. 培育数字人格与数字伦理

也有研究指出，在人工智能技术实践中，培育数字人格是捍卫人的尊严的重要任务[27]。应加强数字伦理教育，提高公众的数字伦理意识，引导公众正确使用生成式人工智能，尊重他人的数字化人格。同时，应建立数字伦理准则，明确生成式人工智能应用的伦理要求，例如禁止利用生成式人工智能生成虚假信息、侮辱他人的内容等。此外，还应加强数字人格的培育，通过教育和培训，提高公众对数字化人格的认识和保护意识，促进数字人格的健康发展[30]。

4.3.3. 强化使用者的注意义务

还有观点认为，生成式人工智能使用者的注意义务是防范侵权行为的重要环节[15]。因此应明确使用者的注意义务类型和内容，例如使用者应承担内容标识义务，对生成的内容进行标识，明确其为人工智能生成的内容；承担结果审查义务，对生成的内容进行审查，确保其不侵犯他人的合法权益。对于专业使用者，还应承担风险管理与预防、输入数据质量控制、系统更新与维护等义务。同时，应建立使用者的责任追究机制，当使用者违反注意义务导致侵权行为发生时，应承担相应的法律责任。

4.3.4. 建立链式责任分配机制

也有学者表明，应建立生成式人工智能的链式责任分配机制，明确技术研发者、技术持有者、数据供应者等多圈层主体的责任[31]。技术研发者应承担研发责任，履行明确的负面清单义务与人机伦理要求，在违法研发明确禁止的技术时承担严格责任或无过错责任；技术持有者应承担运营主体责任，履行数据保护、内容管控、溯源标记等义务；数据供应者应承担数据质量责任，确保提供的数据合法、合规。同时，应建立责任分担机制，当多个主体共同导致侵权行为发生时，根据各主体的过错程度和行为对损害结果的影响程度，合理分配责任。

5. 结论

生成式人工智能技术的快速迭代，使得数字化人格的生成与应用场景不断拓展，其带来的侵权风险与法律挑战也日益凸显。本文通过剖析数字化人格侵权的特殊性，梳理我国现有法律在个人信息保护、侵权归责、数字人格保护等方面的规制缺陷，结合欧盟、美国等域外规制经验，提出了“统一立法 + 分别立法”双轨规制体系、技术治理与多元共治等针对性规制路径，明确了链式责任分配框架，为解决数字化人格侵权问题、填补死者数字化人格保护的规制空白提供了理论支撑与实践指引。

本研究仍存在一定局限，对跨境侵权规制、数字人格商业化使用的细化规则等问题的探讨有待深入。未来可聚焦死者数字化人格保护、跨境侵权规制等前沿问题，进一步完善相关法律规则，实现技术创新与人格权益保护的动态平衡。

参考文献

[1] 朱禹, 陈关泽, 陆泳溶, 等. 生成式人工智能治理行动框架: 基于 AIGC 事故报道文本的内容分析[J]. 图书情报知识, 2023, 40(4): 41-51.

[2] 任江, 吴舒颖. 人工智能生成数字化人格: 侵权风险、伦理挑战与法律规制[J]. 南京邮电大学学报(社会科学版), 2025, 27(1): 39-49.

[3] 黄锫. 人工智能大模型训练数据的风险类型与法律规制[J]. 政法论丛, 2025(1): 23-37.

[4] 朱程斌. 论个人数字人格[J]. 学习与探索, 2021(8): 82-90.

[5] 葛江虬. 论数字人格要素及其民法保护——以“元宇宙”为对象[J]. 比较法研究, 2023(6): 170-183.

[6] 罗有成. 数字权利论: 理论阐释与体系建构[J]. 电子政务, 2023(5): 50-62.

[7] 张新宝, 卞龙. 论生成式人工智能服务提供者的过错推定责任[J]. 北方法学, 2025, 19(5): 5-19.

[8] 中国法院网. 法治划清 AI 红线共治守好“脸面安全” [EB/OL]. https://www.chinacourt.cn/article/detail/2026/03/id/9214081.shtml, 2026-03-04.

[9] 中国新闻网. 用 AI “复活”逝者, 伦理和法律的边界在哪?专家解读[EB/OL]. https://www.chinanews.com.cn/sh/2024/04-06/10193655.shtml, 2025-10-25.

[10] 李植钧. 生成式人工智能内容的风险及法律规制[J]. 法学(汉斯), 2025, 13(11): 2475-2481.

[11] 高志宏. 回应与超越: 生成式人工智能法律规制——以《生成式人工智能服务管理暂行办法》为视角[J]. 社会科学辑刊, 2024(5): 121-130.

[12] 王利明. 迈进数字时代的民法[J]. 比较法研究, 2022(4): 17-32.

[13] 张新宝. 生成式人工智能训练语料的个人信息保护研究[J]. 中国法学, 2024(6): 86-107.

[14] 张凌寒, 于琳. 生成式人工智能价值链上的侵权责任划分[J]. 北京行政学院学报, 2025(5): 72-83.

[15] 刘承韪, 马瑞聪. 生成式人工智能使用者注意义务的规范来源[J]. 山东大学学报(哲学社会科学版), 2025(5): 152-163.

[16] Lucchi, N. (2023) ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation*, **15**, 602-624. https://doi.org/10.1017/err.2023.59

[17] 丁晓东. 人工智能风险的法律规制——以欧盟《人工智能法》为例[J]. 法律科学(西北政法大学学报), 2024, 42(5): 3-18.

[18] Yang, W. (2024) Legal Regulation of Intellectual Property Rights in the Digital Age: A Perspective from AIGC Infringement. *Science of Law Journal*, **3**, 164-173.

[19] Foong, C. (2025) Generative Artificial Intelligence Models and Copyright Infringement: Doctrinal Challenges and Regulatory Gap-Filling Using Unfair Competition Principles. *University of New South Wales Law Journal*, **48**, 1361-1398. https://doi.org/10.53637/uifz7074

[20] Tabassum, A., Elmahjub, E., Padela, A.I., Zwitter, A. and Qadir, J. (2025) Generative AI and the Metaverse: A Scoping Review of Ethical and Legal Challenges. *IEEE Open Journal of the Computer Society*, **6**, 348-359. https://doi.org/10.1109/ojcs.2025.3536082

[21] Golda, A., Mekonen, K., Pandey, A., Singh, A., Hassija, V., Chamola, V., *et al*. (2024) Privacy and Security Concerns in Generative AI: A Comprehensive Survey. *IEEE Access*, **12**, 48126-48144. https://doi.org/10.1109/access.2024.3381611

[22] 杨延超. 我国人工智能立法的制度创新与路径选择[J]. 治理研究, 2025, 41(2): 20-37.

[23] 张红. 生命数字化进程中的文化转向与制度因应——以数字自我的法律保护为中心[J]. 求索, 2025(3): 158-168.

[24] 周学峰. 生成式人工智能侵权责任探析[J]. 比较法研究, 2023(4): 117-131.

[25] 张华韬. 动态体系论下生成式人工智能侵权的归责与构成[J]. 法学杂志, 2025, 46(6): 82-101.

[26] 宁殿霞, 位涛涛. 生成式人工智能服务提供者间接侵权的分层判定与责任配置——兼论传统网络服务提供者间接侵权的归责困境与应对[J]. 内蒙古社会科学, 2026, 47(1): 96-103.

[27] 颜卉. 算法驱动型虚拟数字人涉侵权纠纷的规范解决路径[J]. 重庆大学学报(社会科学版), 2024, 30(2): 182-194.

[28] 张吉豫, 田雨阳. 生成式人工智能应用中开源模型提供者的侵权责任界定[J]. 数字法治, 2025(5): 128-143.

[29] 郑玉双. 人工智能与人的尊严的法理建构[J]. 浙江学刊, 2024(6): 37-47, 235.

[30] 王利明, 丁晓东. 数字时代民法的发展与完善[J]. 华东政法大学学报, 2023, 26(2): 6-21.

[31] 袁曾. 生成式人工智能责任规制的法律问题研究[J]. 法学杂志, 2023, 44(4): 119-130.