Doi:10. 11835/j. issn. 1008-5831. fx. 2025. 09. 001

欢迎按以下格式引用:熊进光,张峥. 从ChatGPT到DeepSeek:生成式人工智能的法律风险与三维规制[J]. 重庆大学学报(社会科学版),2026(1):253-268. Doi:10. 11835/j. issn. 1008-5831. fx. 2025. 09. 001.

Citation Format: Xiong Jinguang, Zhang Zheng. From ChatGPT to DeepSeek: Legal risks and three-dimensional regulations of generative artificial intelligence[J]. Journal of Chongqing University (Social Science Edition), 2026(1):253-268. Doi:10. 11835/j. issn. 1008-5831. fx. 2025. 09. 001.

从ChatGPT到DeepSeek:生成式人工智能的法律风险与三维规制

熊进光,张 峥

(江西财经大学 法学院,江西 南昌 330013)

摘要:从ChatGPT到Sora再到DeepSeek,生成式人工智能在不断发展与创新,其潜在法律风险也日益增加。通过分析生成式人工智能的"准备—运算—生成"三阶段运行机制可知,其在不同阶段涉及的核心技术不同,存在的法律风险也有所差异。具体而言,生成式人工智能准备阶段的核心是海量数据与机器学习,运算阶段主要涉及算法技术、人工标注与自主学习,生成阶段则依赖于数据解码与样本生成。相应的,其法律风险主要在于准备阶段的隐私权与个人信息保护,运算阶段的数据安全与算法偏见,生成阶段的版权归属、意识形态与社会秩序。然而,现有立法无法对生成式人工智能的法律地位、监管尺度、样本归属等核心内容提供精细指引。基于此,在比较分析美国、英国、欧盟等域外国家治理范式与治理经验的基础上,结合我国国情与实践现状,应立足于"民法保护—监管尺度—行业规范"三维路径,规制生成式人工智能法律风险,保障公民合法权益不受侵害。首先,在民法层面,明确弱生成式人工智能的法律客体地位及强生成式人工智能的拟制法律主体地位;通过落实私密信息需明确授权与数据加密技术强化个人信息保护;从生成样本的属性及权利归属出发完善知识产权认定标准。其次,在监管尺度层面,对算法等技术实施涵盖"准备—运算—生成"阶段的全过程监管;通过制定技术透明度标准、引入可解释性技术及建立"问责—反馈"保障制度提高算法等相关技术的透明度;构建"政府—社会—企业"联动的特色监管模式,政府为公民与企业提供政策支持、公民积极参与监管治理并将侵权信息反馈给政府与企业、企业以政府政策与公民需求为导向,助力社会发展。最后,在行业规范层面,从生成式人工智能三种侵权形态出发明确其侵权适用的归责原则;落实服务提供者与使用者的法律义务,前者应承担内

基金项目:江西省社会科学"十四五"重点基金项目"元宇宙背景下虚拟数字人侵权法律问题研究"(23FX01);江西省研究生创新专项资金项目"生成式人工智能侵权风险分配与责任承担研究"(YC2025-B134)

作者简介:熊进光,法学博士,江西财经大学法学院教授,博士研究生导师;张峥(通讯作者),江西财经大学法学院博士研究生,Email:2234074912@qq.com。

容审查及安全保障等义务,后者应尽到合理使用与操作及信息反馈等义务;开放社会性咨询与反馈渠道,通过普及公民权利义务、规范公民的使用方法、加强企业与公民的联系等方式遏制侵权现象的发生,并提高侵权纠纷的解决效率。

关键词:生成式人工智能;法律风险;三维规制;ChatGPT;Sora;DeepSeek

中图分类号:D923;D922.17 **文献标志码**:A **文章编号**:1008-5831(2026)01-0253-16

一、问题的提出

2022年11月,美国OpenAI公司推出生成式人工智能大型语言模型ChatGPT,引发全世界的激烈讨论[1]。ChatGPT具有强大的自然语言识别和输出等能力,它的出现标志着通用人工智能与强人工智能时代的到来[2]。2024年2月,OpenAI公司发布人工智能文生视频大模型Sora,该模型可以根据用户的指令,生成长达60秒的视频,标志着生成式人工智能从文字、图片领域延伸到视频领域[3],它的问世对通用人工智能的发展具有里程碑式的跨越意义[4]。2025年1月,我国深度求索企业研发的生成式人工智能DeepSeek正式问世,其凭借卓越的技术实力、高性价比及开源共享的战略,成功在全球人工智能竞争中脱颖而出。它的崛起是我国人工智能领域从"追赶者"变为"规则改写者"的象征,标志着我国已成功构建起完整的人工智能生态系统。

从ChatGPT到Sora再到DeepSeek,生成式人工智能在不断发展与创新,其法律风险也日益凸显。2023年5月,纽约的一名律师在使用ChatGPT查找资料时,其杜撰了几起从未出现的案例,导致律师面临处罚;2023年6月,16名匿名人士向美国加利福尼亚旧金山联邦法院提起诉讼,称ChatGPT在未获得同意的情况下,搜集并泄露了其个人信息;2025年1月,OpenAI公司通过《金融时报》等媒体指控DeepSeek未经授权使用了其专有模型。此外,虽然Sora尚未产生具体的侵权纠纷,但其侵害人格权、著作权等权益的争议与趋势已然出现。

2024年政府工作报告提出要深入推进数字经济创新发展,深化大数据、人工智能等研发应用,开展"人工智能+"行动,打造具有国际竞争力的数字产业集群[5];2025年政府工作报告进一步提到要持续推进"人工智能+"行动,将数字技术与制造优势、市场优势更好结合起来,支持大模型广泛应用[6]。毫无疑问,生成式人工智能是数字经济创新发展、打造数字产业的重要环节,但技术应用过程中高质量发展与法律风险并存,需要审慎应对[7]。对此,本文在剖析生成式人工智能运行逻辑与法律风险的基础上,结合我国规制现状与困境,尝试在民法保护、技术监管、行业规范三个维度提出可行的应对之策,以期生成式人工智能在合规的基础上实现高质量发展。

二、生成式人工智能的运行机理与法律风险

生成式人工智能(Generative Artificial Intelligence,以下简称"GAI")是人工智能的分支,是基于算法、模型、规则生成文本、图片、声音、视频等内容的技术,其运行机制可分为准备、运算与生成三个阶段,基于不同阶段的特点,其潜在法律风险也有所不同。

(一)生成式人工智能的运行机制

GAI可以利用海量数据进行自我学习,掌握不同领域的知识和规则,再根据用户指令,输出符合逻辑和语法的内容[8]。根据GAI对海量数据进行抓捕、加工、传播等不同处理方式,可以将其运行

机制分为三个阶段：数据输入与训练的准备阶段、运用算法等技术整合处理数据的运算阶段、输出数据并进行传播的生成阶段[9]。

1. 准备阶段：海量数据与机器学习

准备阶段是GAI的起始阶段，也是运算与生成阶段的基础，核心是海量数据与机器学习。第一，不论是ChatGPT、DeepSeek与用户进行深度交流，还是Sora根据用户指令生成符合逻辑的长视频，都离不开GAI的“知识储备”，即海量数据是实现深层次人机交互的关键因素。因此，研发者在准备阶段需对其进行数据“喂养”，输入大量数据作为其运行与创作的基础。第二，在数据“喂养”之后，海量数据的分类与提取也是一大难题。而机器学习是计算机研究如何模仿人类的学习行为，获取新的知识或经验，并重新组织已有的知识结构，提升自身的表现[10]。它具有化繁为简的特性，能帮助GAI分析海量数据[11]，学习其规律和模式，解决信息分类、提取、应用等问题[12]，保障GAI的有效输入与深度挖掘。

2. 运算阶段：算法技术、人工标注与自主学习

运算阶段是GAI的第二阶段，其在该阶段主要对输入的数据进行整合与处理，核心是算法技术、人工标注与自主学习。首先，GAI主要通过算法技术对数据进行分析与处理，并改变数据的产生方式、组织形式与流转结构[13]。算法技术是其根据用户指令，对数据进行预处理与特征提取的关键。其次，较传统人工智能，GAI的一大亮点是能够基于用户指令，与用户进行深度交互。如ChatGPT与DeepSeek可以基于用户指令，与用户进行特定化交流并给予反馈。而人工标注则是实现该亮点功能的关键因素，GAI通过大量人工标注来修正和校对机器学习得出的结论，克服传统分析式人工智能的缺陷，推动自身的发展与完善[14]，实现人机交互。最后，GAI可以基于用户指令，生成多样化、创新化、目的化的新样本，实现深度人机交互。但在海量数据与多形态的用户指令下，仅靠人工标注远远不能满足现实需求，其只能帮助GAI理解用户指令并模板式地给出用户偏爱的形式回复，无法进行深度的持续交互。因此，自主学习是GAI在该阶段不可或缺的技术。具体而言，对GAI反复进行“用户指令—数据筛选与加工—任务表达”的模型训练，并给出正向或负面反馈，让其在接收到数据及指令时，无需人的介入，便能结合已存在的人工标注，自发地学习、挖掘其中蕴含的知识，灵活地回应用户指令[15]。

3. 生成阶段：数据解码与样本生成

生成阶段是GAI运行的最后阶段，即基于已经获取的知识与内部表示，以人类语言的形式创建新的目的化内容[16]，满足用户需要。该阶段的核心是数据解码与样本生成，助力GAI将抽象的内部表示转化为具体的外在产物，是实现与用户深度交互的接口。生成阶段主要分为三个步骤，首先是对运行阶段整合的数据进行汇总与筛选，形成机器语言样本；其次是对该样本进行数据解码，将抽象的二进制语言转化为具体的人类语言；最后是根据用户指令，将具体的人类语言以文字、图片或视频等形式输出，形成符合用户指令的目的化产物。GAI的生成样本具有多样性、目的性与创新性等特征，已被广泛应用于各个领域，如ChatGPT被用于辅助警方制定和评估侦查方案[17]；Sora被用于辅助教师设计有创新性的教学活动[18]；DeepSeek被用于高校图书馆学科服务等[19]。

（二）生成式人工智能的法律风险

GAI在不同运行阶段依赖的核心技术有所差异，故其涉及的隐私权、个人信息保护、数据安全等法律风险也有所不同。

1. 准备阶段:个人信息保护与隐私权

GAI在准备阶段主要是基于预设程序对数据进行抓取、提取与分析,存在侵害公民人格权益的安全隐患,主要集中于隐私权与个人信息保护。第一,个人信息保护风险。GAI在准备阶段输入了海量数据,但其数据采集的来源与方式并未公布,存在窃取的情况。如2023年7月,谷歌被指控未经用户知情或同意,窃取了用户的数据来训练人工智能Bard[20],该行为明显侵害了用户的合法权益,对个人信息保护提出挑战。第二,隐私权风险。GAI在收集海量数据时,并不会区分普通数据与私密数据,而未经公民同意对其私密信息进行"爬取"的行为,严重侵害公民的隐私权。如2023年6月,OpenAI被指控其研发的ChatGPT等产品擅自窃取数亿互联网用户的私人信息用于训练,涵盖医疗记录与儿童信息,违反了州和联邦的隐私法[21]。

2. 运算阶段:数据安全与算法技术

GAI在整合及处理数据时,存在严重的数据安全与算法偏见等隐患,会对样本及用户造成负面影响。第一,数据安全风险。GAI收集了海量数据,但其研发公司并不能保证这些数据不被泄漏及滥用。GAI的目的是与用户进行深度人机交互,满足用户的个性化需求,故犯罪分子可以针对ChatGPT及DeepSeek进行指令诱导以获取其采集的公民信息;也可利用Sora创建特定的视频,模拟真实场景欺诈受害人,实现犯罪目的。虽然研发公司会通过预设程序等方式制止用户利用其实施不法行为,但已有专家证实,在实践中ChatGPT可以绕开OpenAI的数据筛选器来构建恶意程序[22]。基于此,GAI存在严重的数据安全隐患,既不能保障数据的存储安全,也无法保证输出信息绝对真实。

第二,算法问题。算法具有高度不透明性,不能保证客观中立。算法滥用、算法误用、算法垄断等算法偏见赋权给一部分人时,也排斥和边缘化另一部分人[23]。算法偏见是算法侵权的核心原因,可以分为内外两部分。其一是内生性偏见。该偏见主要源自算法黑箱,由于算法工作原理与流程没有对外公开,用户在输入指令后只能得到生成样本,而不能知晓其逻辑[24]。虽然数据本身是客观的,但其蕴含的信息是主观的,当GAI获取海量数据后,算法会自发地提取并挖掘数据内容,形成偏向性样本。基于此,用户得到的创新性样本并不具备客观性与公平性,而是数据来源在算法中博弈的结果。其二是外生性偏见。该偏见主要源自GAI的预设性技术。在运算阶段,为紧跟数字信息的更新迭代,满足用户的多样化需求,人工标注与自主学习是GAI实现深度人机交互的关键,而这离不开研发者的人工操作[25]。研发者在进行人工标注时,不可避免地会带入自己的主观喜好,而自主学习的模型训练反馈,也会受到研发者自身观点、文化、经历等因素的影响。基于此,用户得到的生成样本中掺杂了研发者的态度与认知,难以客观地回应用户指令。

3. 生成阶段:版权归属、意识形态与社会秩序

GAI在输出创新性样本的过程中也存在侵权风险,主要在版权归属、意识形态与社会秩序三部分。第一,版权归属问题。一方面,国际上对GAI生成样本的版权问题还没有形成清晰的界定。从我国首例"AI文生图"著作权侵权案分析,我国实践上认为,其本质是人类利用工具进行创作,创作者享有著作权①。但我国学界对GAI成果的可版权性还存在较大争议。另一方面,GAI是在海量数据的基础上生成新的成果,若该成果与已有作品相似或相同,且未经授权或未遵循合理使用规则,则也可能引发版权纠纷。第二,意识形态问题。GAI的生成样本是结合用户指令、海量数据等加工

① 参见北京互联网法院民事(2023)京0491民初11279号判决书。

形成，其在提取、分析数据时，易受到研发者的影响，存在算法偏见隐患。而目前西方在GAI领域的发展优先于其他国家，当公民，尤其是未成年人，使用第一梯队的GAI时，会接触到更符合西方国家价值观的样本，存在意识形态渗透的风险[26]。第三，社会秩序问题。基于GAI的功能目的及用户指令，生成样本并不能保证真实有效。如自媒体博主为博人眼球，会利用Sora能够快速将创意转化为视觉内容的功能[27]，不断制造虚假视频。当虚假信息蔓延、发酵后，不仅会引发公众对真实信息的质疑，还会制造社会舆论，扰乱社会秩序[28]。

三、生成式人工智能法律风险的治理现状与困境检视

随着数字时代的发展，GAI已被广泛应用于各行各业，其法律风险也日益凸显。针对已出现的法律问题，我国在结合现有立法及行业规范的基础上，制定了一系列过渡性防控措施，但在实践中存在一定的阻碍。

（一）生成式人工智能法律风险的治理现状

针对GAI引发的法律问题，我国目前没有形成体系性规制方案，而是采取主体归责制，即由其多元主体承担。然而，2023年7月，国家互联网信息办公室等七部门联合公布《生成式人工智能服务管理暂行办法》（以下简称《暂行办法》），将多元主体简单地分为GAI服务使用者与GAI服务提供者。

1. 生成式人工智能服务使用者承担责任

使用者对GAI的产出起决定性作用，当生成样本侵权时，往往由其承担责任[29]。首先，GAI并不会自主生成样本，而是基于使用者的指令进行加工与运转，其侵权行为与使用者使用行为之间存在密切联系。其次，研发者在GAI中预设有安全审核过滤机制，若使用者在无意中输入了违禁指令，GAI将因安全审核过滤机制停止工作。只有使用者避开安全机制，才能让GAI产出违法或不良内容。此时，使用者主观上具有恶意，且服务提供者通常已尽到了注意义务，由其承担责任显然有失公平[30]，故应由使用者承担责任。最后，算法是GAI的核心技术，算法偏见不仅存在于GAI内部，也会根据使用者的指令、喜好、反馈等因素形成外部偏见。若使用者不断进行“输入—反馈”训练，致使生成样本侵权，其必然要承担相应责任。

2. 生成式人工智能服务提供者承担责任

根据《暂行办法》可知，GAI服务提供者，是指利用GAI技术提供服务的组织与个人[31]。据此，服务提供者在宏观层面既包括研发者，也涵盖平台等提供者，承担的义务与责任也更为重大。

第一，结合《暂行办法》相关规定，服务提供者需要承担训练数据来源合法性责任和个人信息保护、内容管控、防沉迷等义务，如果违反相关规定，不论是否出现侵权事件，服务提供者都需承担相应责任[32]。第二，在使用者合法使用的情况下，服务提供者需要对GAI的生成样本负责。如使用者在ChatGPT中输入“需要法学院教授性骚扰的例子及来源”的指令，其在经过分析、提取数据后，告知使用者特利教授在一次班级旅行中发表了性暗示的言论，并引用了《华盛顿邮报》的文章，但事后被证实为虚构事件，特利教授从未被指控性骚扰，邮报文章也并不存在[33]。该案件是服务提供者侵权的典型情况之一，由于使用者并未进行违规操作，服务提供者必须为此承担责任。但若使用者存在违规操作，进行了训练“诱导”，则还需考虑服务提供者是否尽到了注意义务，若不存在过错，则无需承担责任。

(二)生成式人工智能法律风险的治理困境

虽然我国于2023年发布了《暂行办法》,我国学者也于2024年提交了《中华人民共和国人工智能法(学者建议稿)》,以规制GAI侵权现象。但在实践中,现行规定难以满足社会需要,也不能系统、完全地保护公民合法权益。

1. 生成式人工智能法律地位认定不明

规制GAI侵权现象的核心问题是其法律地位认定不明,且不论是认定为法律主体还是法律客体,皆存在利弊。第一,法律客体地位。目前学界的主流观点是将GAI视为工具,赋予其法律客体地位。虽然该观点便于明晰侵权责任的承担人,但在GAI生成样本的属性认定方面存在局限性,有违著作权法鼓励创新的立法宗旨。如在"菲林诉百度案"中,法院认为作品应由民事主体创作完成,而争议的"分析报告"是由人工智能生成且使用者没有作出实质性贡献,故该分析报告不能被认定为作品②。第二,法律主体地位。虽然赋予GAI法律主体地位是时代所需,但从理论上说,GAI是非生命体,不存在理性与意志,不具备作为主体的客观条件[34]。且从损害赔偿角度而言,侵权责任的承担往往以财产为基础,而GAI并不具有独立的财产。虽然在赋予其法律主体地位之后,可以由其收支自负,但其侵权现象频发,大概率出现入不敷出的局面。因此相较于服务提供者或使用者,GAI并不具备对受害人进行充分补偿的条件与能力[35]。总而言之,无论将GAI视为法律主体还是法律客体都有一定的理论支撑和局限性,但其法律地位不明不仅不利于解决相关侵权纠纷,也不利于维持社会稳定。因此,明确GAI法律地位是数字时代亟须解决的问题。

2. 生成式人工智能技术监管尺度不明

GAI内含算法、模型等多种技术,应对相关技术采取何种监管措施也是治理其侵权纠纷的一大难题。目前,我国尚未明确采取何种监管尺度,但国际上对GAI技术的监管已趋于两极化。一方以美国为代表的宽松监管模式,主要追求技术创新以获取更多的国际利益,而不够重视技术泛滥或失控的风险与损害;另一方以欧盟为代表的强监管模式,其于2024年3月正式发布《人工智能法》,通过制定统一的法案实现对人工智能的全面监管,意图建立一个加强监督和执行的共同制度[36]。简言之,对于GAI技术的监管问题,若监管尺度过于宽松,侵权现象会日益严重,但若过于严格,又会阻碍技术的创新与发展。因此,结合我国国情明确采取何种监管方案与尺度是我国当下必须解决的难题。

3. 生成式人工智能生成样本归属不明

除了GAI的法律主体地位与技术监管尺度,其生成样本的类别归属也颇具争议。第一,司法界认为,当使用者或研发者存在实质性贡献时,其生成样本可认定为作品。在"腾讯诉盈讯案"中,法院认为人工智能生成的文章凝结了研发团队的创作意图,属于单位作品③。而在"菲林诉百度案"与"AI文生图案"中,前案法院认为原告没有实质性贡献,人工智能生成的"分析报告"不能归属于"作品";后案法院认为原告进行了智力投入,人工智能生成的涉案图片可以归属于"作品"。由此可知,法院往往基于"使用者是否存在实质性智力贡献",判决其生成样本能否归属于"作品"。第二,实务界与学界认为其生成样本不属于作品[37]。有律师认为,GAI具有不可预测性,算法技术具有不透明性,这与《中华人民共和国著作权法实施条例》中的"直接创作"存在冲突,不可认定为作品[38]。也有

② 参见北京互联网法院民事(2018)京0491民初239号判决书。

③ 参见广东省深圳市南山区人民法院民事(2019)粤0305民初14010号判决书。

学者从判决文书出发，认为判决结果中部分关键性问题缺乏系统论述，将GAI的生成物认定为“作品”是为了实现政策性目标[39]。总之，关于GAI生成样本的归属与定性问题，目前没有形成统一、公认的观点，这也是规制GAI侵害知识产权问题的一大困境。

（三）生成式人工智能法律风险的域外治理经验镜鉴

GAI引发的法律风险目前已成为全球性治理议题，世界各国也纷纷出台了一系列措施，以应对数字时代的新挑战。

1. 域外生成式人工智能法律风险治理的类型化分析

在GAI法律风险议题上，各国基于各自价值取向形成差异化治理路径，其中欧盟、美国和英国的治理模式具有典型研究价值。

欧盟坚持以人为本的理念，采取强监管模式[40]。一是在治理政策上，采取统一垂直的立法体例，通过颁布《人工智能法》实现技术创新、权益保护与公众安全的平衡。二是在治理主体上，引入监管沙盒，将监管主体及模式由政府主导转变为政府、企业等多主体契约共治，打破信息壁垒[41]。三是在治理目标上，通过细化风险，兼顾安全性与一致性。其将人工智能的法律风险细分为不可接受风险、高风险、有限风险和最小风险，并针对不同程度的风险制定差异化处理方案，实现风险分级的精细管理[42]。

美国采取较为宽松的市场主导治理模式。一是在治理政策上，联邦层面至今没有统一立法，而是通过一系列政策框架遏制法律风险，强调自愿性、灵活性和适应性，更依赖软法[43]。二是在治理主体上，采用多元主体的治理模式，坚持以市场和行业为主导，侧重于发挥市场主体的作用[44]。三是在治理目标上，相较于公众安全与公民利益，其更重视技术的创新以增强在人工智能领域的全球地位。

英国采取创新驱动的适度监管模式。一是在治理政策上，英国没有颁布正式的立法文件，采取“以原则性要求为准则、以道德伦理约束为补充”的治理方式，以“灵活监管、避免过度监管”为治理导向。二是在治理主体上，英国采取监管机构、数字企业、社会公众等多类主体参与的“多元化视角”治理方案，通过发布指南、创建平台、开展论坛等途径获取多方意见与建议。三是在治理目标上，英国以促进人工智能的创新与产业发展为根本宗旨，以维持其在该领域的领导地位。

2. 域外生成式人工智能法律风险治理范式的比较辨析

欧盟、美国与英国的差异化治理范式虽然具有示范与参考价值，但均存在一定缺陷，我国需对比分析域外应对模式，立足本土法治环境，在结合我国国情与实践的基础上，批判性地加以借鉴。

首先，欧盟的《人工智能法》是全球首部关于人工智能的综合性立法，为各国解决GAI法律风险提供了参考路径。但是，该部法律在实践中也存在制度悖论。第一，该法案采取以安全为核心的强监管模式，但过度严苛的合规会阻碍技术的创新与发展。第二，将人工智能的法律风险划分为四个等级，便于提供精细化管理。但静态的立法难以全面规制人工智能动态的演进特性与创新发展，立法的滞后性会带来规则盲区，立法的频繁更新又会影响法律实施的稳定性。第三，采取“长臂管辖”规则，其泛化的管辖范围忽视了当下人类命运共同体的趋势及数字时代多边合作的诉求，可能会加剧国际法律冲突。

其次，英美的治理模式存在效能局限的问题。美国的治理模式具有管理规制的特点，即主导者要求被规制者完善内部规则体系，自行制定计划并实施自我管理，实现特定的目标。该模式缺乏制

度性保障与刚性约束,极易导致技术创新与经济发展建立在牺牲公民人格权等合法权益的基础上[45]。与之相对应的是,英国采取的具有原则规制特点的治理模式,即不制定详细的规则,通过发布原则的方式进行治理,不以行业为导向。然而,在没有详细规则的情况下,治理依据缺乏确定性且预测性较低,极易导致监管主体与服务提供者因规则解释分歧产生制度性摩擦,削弱治理实效。

简言之,强监管模式会阻碍技术创新,影响我国在全球人工智能领域的竞争力、影响力及国际话语权,且泛化管辖会影响我国外交关系,不利于共建"一带一路"与"人类命运共同体"的推行;市场主导监管模式有违我国"以人为本"的核心理念,难以全面保护公民合法权益;创新驱动监管模式则缺乏详细的适用规则,不利于维护社会和谐稳定。基于此,我国应批判性地看待域外治理模式,充分考量本土政治、经济、社会、文化、生态等制度环境,因地制宜地探寻适合我国国情的法律风险应对之策与治理之法[46]。

四、生成式人工智能法律风险的三维规制

涉GAI法律纠纷呈多样化、复杂化的发展趋势,现有防控措施无法对其全面规制,在保障公民合法权益时初现颓势。基于此,在比较分析域外典型治理范式的基础上,笔者认为,应立足我国国情,结合我国实践现状与困境,从多角度出发,构建涵盖民法保护、技术监管与行业规范的三维规制方案来应对数字时代的法律挑战。

(一)落实民法对争议问题的保护路径

GAI侵权纠纷争议频发且难以规制,其根源在于法律空白及规则边界模糊。因此,应在民法层面对争议问题进行定性,强化权益保护力度。

1. 明确生成式人工智能的法律地位

GAI的问世意味着我们从弱人工智能向强人工智能迈出了关键一步,其法律主体地位也再次引发激烈讨论,学界当下主要存在客体说、主体说与拟制说三类观点。第一,客体说。客体说是学界的主流观点,认为GAI不具备法律主体地位。该观点认为GAI不具备人类的主体性[47],而是属于人类的工具,应归属于权利客体或对象的类别中[48]。首先,GAI不具备独立的意志。GAI不具有生命,其工作目的源自运行机制,与人类有目的、有意识的行为完全不同,不具备人的心性与灵性[49]。其次,GAI不具备权利与行为能力。GAI不具有意志、目的性与自律性特征[50],不能自主作出道德选择,其与自然人是主人与工具的固有关系[51]。最后,GAI不具备责任承担能力。GAI不可能产生生命权与财产权[52],其侵权的最终责任人是自然人[53],而只有将其视为工具时,自然人才能为其侵权行为负责[54]。第二,主体说。主体说秉持将GAI视为法律主体的立场。首先,GAI已初步具备人类意志等特征。当下,GAI已经具备较强的认知能力、一定的实践能力及初步的价值判断能力[55],可以视为具备了一定的意识。而权利来源于意识,既然GAI具备自我意识、人机互惠与交互能力,就应当获得人的权利[56]。其次,GAI具备行为能力。不论是在Moore v. Publicis Groupe SA案中,美国法院正式批准预测编码可以作为审查电子存储信息的可接受方式④,还是美国第十巡回法庭明确计算机程序的行为后果由保险公司承担,都是在司法实践上明确了GAI具有独立形成权利义务的资格[57]。基于此,GAI具备赋予法律主体地位的现实基础与可能性。第三,拟制说。拟制说立足于"GAI只能承担有限责任"的观点[58]。首先,有必要赋予GAI法律人格。GAI具备独立的行为能力和

④ See Moore v.Publicis Groupe SA,2012 WL 1446534 (S.D.N.Y.Apr.26,2012).

责任能力，赋予其法律人格是规制相关法律风险的必要且有效的路径。其次，GAI无法独立承担责任。GAI运行的各个阶段都依赖于人类提供的硬件与软件基础，且不具备财产，而财产是所有权的基础[59]，也是自然人与法人承担行为后果的基础，故GAI独立承担法律后果的能力不足[60]。因此，从现实需求出发，应将GAI定位为拟制法律主体，赋予其“有限”法律人格[61]。

从法理演进维度分析，三种学说均具备理论自洽性与实践基础，但在数字时代GAI技术发展趋势下，三者的现实适用性存在显著差异。首先，客体说最契合当下的技术发展，符合时代特征与应用趋势。从技术治理角度审视，数字时代的社会复杂性不断增长，且GAI迭代迅速，明确其客体地位，有助于构建客观理性的治理框架，以应对技术迭代的治理挑战[62]；从本体论层面考量，尽管GAI展现出拟人化交互特征，但其仅存在于数字空间，没有“具身化”参与人类社会，将其视为法律主体，存在法理逻辑与实践应用的现实障碍[63]。其次，拟制说反映了法律制度的发展规律。法律主体范畴的扩张是文明演进的重要表征，通过赋予GAI拟制法律主体地位来应对其侵权问题，契合社会发展趋势与制度创新需求。但拟制法律主体地位以独立行为能力和责任能力为必要前提，现阶段的GAI尚不具备该核心要件，故该学说虽具前瞻价值，但现阶段难以实质适用。最后，主体说具有未来可能性但缺乏现实基础。仅当GAI演进为通用人工智能，且真实涌现出“类人”的自主意识、认知架构、思维与理解能力时，才具备成为主体的法哲学基础与技术支撑[64]。而在当前及未来的技术发展中，其“意识涌现”仍处于假设层面，故该学说仅具理论探讨价值，无法形成有效的制度供给。

结合上述分析，笔者认为，虽然ChatGPT与DeepSeek的出现，标志着全球人工智能领域的重大突破，具有里程碑式的意义，但现阶段GAI仍属于弱人工智能。从技术与功能分析，弱GAI是指在执行特定任务且仅限于这些任务的智能系统；而强GAI是指拥有甚至超越人类水平的智能系统，能够用与人类认知相似的方法去理解、推理、学习并解决各种复杂问题，具备自主学习、跨领域推理、理解情感等能力。因此，对于弱GAI，应赋予其法律客体地位，但对于强GAI，应赋予其拟制法律主体地位。

第一，弱GAI不具备成为法律主体的理论支撑与现实基础。首先，GAI没有自由意志，其生成样本都是基于用户指令加工而成，不具备独立的意思表示能力。其次，现阶段GAI不具备独立的财产，当GAI侵权后，受害人起诉的对象及司法判决的责任承担人都是研发公司，GAI不具备责任承担能力。再次，即使是主张“主体说”，认为GAI具有道德和主体地位的多数学者，其研究对象也是未来的强GAI[47]，而非现阶段的弱GAI。最后，数字企业等服务提供者履行义务具有责任驱动性。基于理性经济人假设，仅当市场主体面临直接法律归责风险时，方能形成有效激励，推动GAI的规范化进程。若将弱GAI视为法律主体，将导致双重制度困境。一方面，服务提供者可能基于主体资格转移产生规避法律责任的心理倾向；另一方面，由于弱GAI不具备独立财产与责任能力，将形成权利救济真空，致使受害人难以获得充分的法律救济，不利于社会治理与社会和谐稳定。

第二，强GAI具备成为拟制法律主体的理论基础与制度支撑。首先，虽然强GAI目前还处于“假说”状态，其能否具备自主意识并独立思考是难以回答的问题[65]，但GAI会随着技术的发展不断突破，逐渐具备类人的意志特征及行为能力，为成为拟制主体提供理论基础。其次，法律主体的范围随着时代与技术的发展不断扩大[66]，从“人可非人”到“非人可人”，为赋予强GAI拟制主体地位提供了现实基础。再次，赋予强GAI拟制主体地位是时代需要。若强GAI成为拟制主体，则可以直接承担侵权责任，有利于解决责任分配难题。最后，基于责任自负原则，在强GAI具备自主决策机制

与独立民事责任能力后,确立其有限法律人格具有制度合理性。且在该基础上配套建立技术责任保险与损害赔偿机制,可以保障受害人获得合理的法律救济,实现技术应用、社会秩序、公民权利保障的价值平衡。

2. 强化公民个人信息保护

GAI在各个阶段都离不开海量数据,对公民隐私权、肖像权、个人信息等产生极大威胁。基于此,应落实个人信息分级分类,强化公民人格权益保护。首先,在准备阶段落实使用个人私密信息需明确授权。GAI的准备阶段主要通过"爬取"社交媒体、互联网、语料库等数据进行输入[67],涵盖普通信息与隐私信息,若不对该行为加以限制,极易侵害公民人格利益,损害公民人格尊严[68]。因此,当GAI爬取的信息涉及公民肖像、私人空间等隐私权益时,应明确是否得到公民的授权。只有明确授权后,才能进一步提取、分析与运用,且不能因该信息发布在社交媒体,就默许随意使用。其次,在运算阶段引入数据加密技术。GAI运算阶段存在数据安全风险,应对数据分级分类,区分普通信息与敏感信息,对涉及个人身份信息等内容的敏感数据实行严格的密钥管理与访问控制机制[69]。最后,在生成阶段进行数据脱敏。GAI在生成样本时,应使用通用字符代替敏感信息,避免使用者直接关联到本人。即使用户指令明确需要,也应得到公民的明确授权,反之则应进行脱敏处理。

3. 优化知识产权认定标准与归属规则

GAI生成样本的权利归属及能否受著作权保护充满争议,主要存在人类中心主义论、法律主体地位论和法律解释论三种观点[70]。从传统上分析,版权属于自然人、法人或非法人组织,而GAI属于工具,不具备法律主体地位,因此其生成样本不具有著作权。但是从立法与实践角度分析,激励创新是著作权的立法目的之一,GAI可以生成多样化、创新化的样本,且实践中已出现认定其可以版权化的司法判决。基于此,应顺应时代需要,优化并完善知识产权的相关规定。

第一,明确生成样本的属性。《人工智能生成物的版权问题决议》提出,人工智能生成物在生成过程中若有人类的干预且符合其他条件,则能够获得版权保护。但GAI的运行是基于使用者的输入指令,或多或少都会受到人类的干预。如此,GAI的生成样本应都具有版权性,但这有违《决议》的精神。所谓作品,是指在文学、艺术领域内具有独创性,同时也可以以一定形式表现出来的智力成果。因此,可以将"人类干预"限缩到是否存在"实质性智力贡献"。若生成过程中,使用者存在实质性智力贡献,则该生成样本可以认定为作品,受著作权保护,反之则不受著作权保护。这也是当下法院在审理案件时的主流标准。第二,明确知识产权权利归属。一方面,相较于传统人工智能,GAI需使用者输入指令、反馈需求,其生成样本具备部分人的意志,为样本的独创性提供了基础性要素[14]。另一方面,GAI的核心技术是机器学习与人工标注,后者体现了人的意志,且会随GAI的运作而不断流转,赋予生成物创新性与独特性的特征。基于此,生成样本的知识产权应属于使用者,这也符合OpenAI《共享和发布政策》中的相关规定[71]。

(二)完善算法等新兴技术的监管尺度

我国目前没有明确算法等新兴技术的监管方案,但监管尺度对GAI的创新发展具有深远影响,也是规制GAI法律纠纷的重要路径。

1. 实施全阶段全过程审查监管

GAI的运行离不开硬件与软件的支撑,为实现对算法等新兴技术的全方位监管,遏制侵权的频

繁发生，应对GAI实施全过程、全阶段动态审查。第一，审查准备阶段的数据合规性。应对GAI收集数据的来源、爬取方式进行检测，保证数据来源合法、手段与方式合法、应用途径合法，保证数据具备合规性。第二，审查运算阶段的算法偏见。算法黑箱是运算阶段的核心问题，故该阶段主要审查监管两方面：一是算法在筛选数据时是否公平公正，不能有所偏颇或遗漏；二是人工标注的数据是否公平公正，不能掺杂个人观点或喜好。如果发现算法黑箱问题，对无实质性影响的轻微偏见应记录下来，上传至终端；对存在实质性影响的偏见应进行人工干预。三是审查生成阶段的虚假信息与道德标准。在生成阶段，需要审查生成样本是否真实有效、与道德标准是否冲突，防止虚假信息及不良思想给使用者造成困扰，维护社会稳定。

2. 提高算法等技术的透明度

算法等技术具有不透明性，外部人员难以知晓其内部逻辑，应提高相关技术的透明度，遏制算法偏见的泛滥。第一，制定技术透明度标准。从根源出发，制定算法等技术的透明度标准，要求服务提供者在不涉及机密的基础上，公开披露技术的基本原理、逻辑、运行过程及决策方式[72]，帮助专家对相关风险进行有效评估。第二，引入可解释性技术。制定透明度标准的目标群体是专家及专业人员，但对非专业人员而言，由于行业壁垒，他们难以理解算法相关的专业知识。此时，应引入可解释性技术，如可视化软件等，帮助非专业人员理解算法等技术的运作原理与运行模式，知晓算法偏见、意识形态等现有问题，增强使用者的自主决策[73]，提高生成样本的可信度[74]。第三，建立“问责—反馈”保障制度。虽然研发企业提供了意见反馈渠道，但缺乏实效性，且缺乏问责的反馈难以保障提高技术透明度等措施的落地[75]，因此，应建立“问责—反馈”保障制度，为提高技术透明度保驾护航。

3. 形成“政府—社会—企业”联动的中国特色监管范式

目前，国际上对GAI的监管并未形成统一模式，各国态度也有所不同。欧盟由“软”到“硬”逐渐过渡，通过颁布《人工智能法案》实施严格监管，强调基于风险的全过程监管[76]。美国的监管模式较为宽松，对内是“一体四翼”的监管模式，发挥联邦政府的监管主体作用，从设定首要目标原则、指定高级别监管机构、聚焦核心企业、关注重大风险四个方面协调推进；对外则突出多边合作和针对性发难，形成立足国际、加强联盟以及对华打压的“三轮驱动”模式[77]。英国基于现有立法，实施相对宽松、避免过度监管的方案，鼓励技术创新与产业发展，以保持自身在GAI领域的全球领先地位。

我国始终坚持统筹发展和安全原则，可以适当借鉴域外经验做法，逐步构建起具有中国特色的“政府—社会—企业”联动的监管模式。第一，政府层面。政府应支持制定GAI法律框架、安全标准与合法行为准则，强调数据安全与权益保护，从宏观层面把握GAI的监管与行业发展方向，适时举办相关讲座，为公民与企业提供政策支持与方向引领。第二，社会层面。公民应积极参与GAI监管治理，捍卫合法权益不受侵害[78]，在使用GAI时还应对研发企业进行监督，并将信息反馈给政府与研发企业，形成良好的正向循环。第三，企业层面。企业应结合技术发展，不断更新自我管理准则，进行自我监管。当收到公民与政府的反馈信息时，企业要及时更正，形成良性发展，并始终以政府政策与公民需求为导向，为社会进步贡献力量。总而言之，我国应始终坚持问题导向与目的导向相结合，根据国情与实践需要，联动政府、社会与企业，构建符合我国实际的GAI监管模式。

（三）细化生成式人工智能的行业规范

GAI存在大量模糊地带，明确行业规范是有效规制其法律风险、保护公民合法权益的重要

途径。

1. 明确生成式人工智能侵权的归责原则

GAI法律风险日益凸显,应明确其归责原则,规范行业秩序,助力行业发展。基于GAI行为特点,其侵权形态可分为三类,即服务提供者侵害个人信息权益类、GAI固有缺陷侵权类以及其他侵权类。第一,侵害个人信息权益类采取过错推定原则。该类侵权主要源自服务提供者利用GAI实施侵权行为,如不正当利用公开信息、没有尽到安全保障义务、非法爬取等。在服务提供者大规模采集个人信息的背景下,应采取"过错推定"的归责模式[79],由服务提供者证明自己没有过错,反之则应承担相应责任。第二,固有缺陷侵权采取过错责任。固有缺陷引发的侵权纠纷应采取何种归责原则存在一定争议,有学者支持采取严格责任,认为GAI的内部缺陷应由制造者承担责任,无需考虑过错因素[80]。也有学者持不同态度,认为虽然该损害是由固有缺陷引起,但该缺陷的严重性、现有技术能否克服或避免、服务提供者是否尽到了安全保障义务都没有定性,故应采取过错责任而非严格责任。若各方主体没有尽到合理注意义务,则都需承担相应责任[81],本文赞同该观点。第三,其他侵权适用过错责任。GAI的其他侵权形态与一般侵权类似,原则上应适用过错责任。当多方主体都存在过错时,应根据过错大小及对损害造成的影响等因素,综合判断各自应承担的法律责任。

2. 明确服务提供者与使用者的法律义务

虽然GAI存在法律风险,但若服务提供者及使用者能尽到相应义务,可大幅度降低损害发生的可能性。第一,提供者的法律义务。服务提供者存在利用GAI过度收集并滥用个人信息的情况,因此,服务提供者应依据《暂行办法》相关规定,遵守法律、行政法规,尊重社会公德和伦理道德,尊重他人合法权益,不得侵害他人肖像权、名誉权、荣誉权、隐私权和个人信息权。此外,基于GAI运行机制,服务提供者还应承担内容审查、过滤及安全保障义务,并提示使用者在合理范围内使用GAI[82]。第二,使用者的法律义务。使用者存在利用GAI生成虚假信息并进行传播的情况,因此,使用者在使用时须尽到注意义务,输入的指令应合法明确,操作行为应符合规范[83]。当察觉生成样本涉及虚假信息、敏感信息或存在版权等问题时,其还须尽到保密与反馈义务。在实践中,数字化侵权十分隐蔽,落实提供者与使用者的义务是遏制侵权发生的重要途径。以DeepSeek版权问题为例,传统观点基于避风港规则,认为当收到生成样本侵权通知后,提供者应删除样本链接,否则将承担连带责任。但DeepSeek在准备与运算阶段收集了大量数据,其生成样本是多个作品的集合,权利人难以发现侵权行为。此时,可以将"准备阶段"也纳入考量范围,即权利人可以提前向服务提供者声明,明确拒绝作品被GAI等数字技术采集、存储及应用。此时,服务提供者应将该作品从数据中删除,否则将承担间接侵权责任[84]。由此可知,在应对GAI版权问题中,提供者的作为义务是版权保护与责任承担的关键因素,使用者的反馈义务对版权保护也有所裨益,应在行业中明确二者的相关义务,遏制侵权现象的发生。

3. 开放社会性咨询与反馈渠道

虽然政府与企业提供了反馈渠道,但涉及面较窄,反馈后的行动较慢,促进行业发展的效力不强。为更好地解决GAI法律风险并促进行业自我管理及稳步发展,应建立面向公众的社会性咨询与反馈渠道。第一,开放社会性咨询渠道。设立面向全民的咨询渠道,告知公民GAI的基本情况、法律义务、操作流程并解答相关疑问,在激发公民使用兴趣,促进行业发展的同时,规范公民的操作

方法，帮助其牢记使用者义务，减少GAI侵权的发生。第二，开放社会性反馈渠道。设立面向全民的反馈渠道，可以迅速获取GAI在应用过程中的不良状况，有助于行业落实自我监管，促进技术发展与突破。此外，由企业自己开设反馈渠道，技术人员能在第一时间处理故障或进行人工干预，不仅可以遏制侵权现象的扩大，减少受害者的损失，还能增强企业与公民的互动，提高行业的整体信誉，促进行业发展。

结语

从大型语言模型ChatGPT到文生视频大模型Sora，再到国产开源大模型DeepSeek，GAI随着数字时代的发展不断突破与创新，呈现出与人类社会深度融合的发展趋势。但与此同时，GAI的法律风险也日益凸显。基于此，我们应分阶段厘清其法律风险，构建“民法保护—监管尺度—行业规范”三维治理路径。即在民法层面明确GAI的法律地位、强化个人信息保护、完善并优化知识产权的认定与归属原则；在技术监管层面对算法等技术实施全过程监管、提高技术透明度、形成“政府—社会—企业”联动的特色监管方案；在行业规范层面明确GAI侵权的归责原则、落实服务提供者与使用者的法律义务、开放社会性咨询与反馈渠道。总体而言，规制GAI的法律风险是数字时代亟须解决的难题，希望三维路径的提出能够为保障我国公民合法权益添砖加瓦，助力GAI在法治轨道上实现高质量发展，为构建安全、便利、高效的数字未来奠定坚实基础。

参考文献：

[1] 蒋雪颖，刘欣. 生成式人工智能技术下的学术生产与出版：变革、失范与路径[J]. 数字图书馆论坛，2023(5)：64-71.
[2] 高奇琦. ChatGPT的“创造性破坏”效应及其风险应对[N]. 中国社会科学报，2023-03-06(06).
[3] 陈力丹，荣雪燕. 从ChatGPT到Sora：生成式AI浪潮下强化新闻专业意识的再思考[J]. 新闻爱好者，2024(4)：4-8.
[4] 周文康，费艳颖. Sora生成视频的著作权规制困境及化解路径[J]. 出版广角，2024(5)：35-42.
[5] 李强. 政府工作报告：2024年3月5日在第十四届全国人民代表大会第二次会议上[N]. 人民日报，2024-03-13(01).
[6] 李强. 政府工作报告：2025年3月5日在第十四届全国人民代表大会第三次会议上[N]. 人民日报，2025-03-13(01).
[7] 顾男飞. 生成式人工智能发展的产业促进与风险规制：以Sora为例[J]. 图书馆论坛，2024(11)：120-128.
[8] 岳伟，于润泽. 危机还是机遇：ChatGPT对大学生数字素养提升的价值和路径研究[J]. 内江师范学院学报，2024(1)：61-67.
[9] 马羽男. 生成式人工智能的风险与治理：以ChatGPT为例[EB/OL]. (2024-05-16)[2024-11-01]. https://cssn.cn/skyl/skyl_skrp/202405/t20240520_5753491.shtml.
[10] 阿培丁. 机器学习导论[M]. 范明，昝红英，牛常勇，译. 北京：机械工业出版社，2009：1-280.
[11] 刘闻博，王丛虎. 公共管理研究中的机器学习方法：原理、应用及挑战[J]. 公共管理与政策评论，2024(5)：152-168.
[12] 杨剑锋，乔佩蕊，李永梅，等. 机器学习分类问题及算法研究综述[J]. 统计与决策，2019(6)：36-40.
[13] 曹树金，曹茹烨. 从ChatGPT看生成式AI对情报学研究与实践的影响[J]. 现代情报，2023(4)：3-10.
[14] 刘艳红. 生成式人工智能的三大安全风险及法律规制：以ChatGPT为例[J]. 东方法学，2023(4)：29-43.
[15] 朱光辉，王喜文. ChatGPT的运行模式、关键技术及未来图景[J]. 新疆师范大学学报(哲学社会科学版)，2023(4)：113-122.
[16] 杨建武，罗飞燕. 类ChatGPT生成式人工智能的运行机制、法律风险与规制路径[J]. 行政与法，2024(4)：101-115.
[17] 金益锋，马忠红. 刑事侦查中人工智能的应用：实践样态、风险挑战与发展策略[J]. 科技导报，2023(7)：15-27.
[18] 王佑镁，王欣颖，柳晨晨. 教育领域生成式人工智能应用的伦理风险管理框架研究[J]. 电化教育研究，2024(10)：28-34.
[19] 李丽. 大语言模型视角下DeepSeek赋能高校图书馆学科服务研究[J]. 图书馆建设，2025(4)：75-83.

[20] 远洋. 谷歌遭遇集体诉讼,被指窃取数亿美国人的网上数据用于训练AI[EB/OL]. (2023-07-13)[2024-11-10]. https://www.ithome.com/0/705/607.htm.
[21] 金融界. ChatGPT开发商OpenAI遭集体起诉:不择手段窃取信息,将导致文明崩溃![EB/OL]. (2023-06-30)[2024-11-10]. https://www.sohu.com/a/692637279_114984.
[22] 张弛,翁方宸,张玉清. ChatGPT在网络安全领域的应用、现状与趋势[J]. 信息安全研究,2023(6):500-509.
[23] 董青岭. 人工智能时代的算法黑箱与信任重建[J]. 人民论坛·学术前沿,2024(16):76-82.
[24] 弗兰克·帕斯奎尔. 黑箱社会:控制金钱和信息的数据法则[M]. 赵亚男,译. 北京:中信出版社,2015:55.
[25] 龙柯宇. 生成式人工智能应用失范的法律规制研究:以ChatGPT和社交机器人为视角[J]. 东方法学,2023(4):44-55.
[26] 商建刚. 生成式人工智能风险治理元规则研究[J]. 东方法学,2023(3):4-17.
[27] 令小雄,王鼎民,唐铭悦. ChatGPT到Sora:Sora文生视频大模型对影视创作的机遇、风险及矫治[J]. 新疆师范大学学报(哲学社会科学版),2024(6):128-137.
[28] 邓建鹏,赵治松. 文生视频类人工智能的风险与三维规制:以Sora为视角[J]. 新疆师范大学学报(哲学社会科学版),2024(6):92-100.
[29] 张璐. 生成式人工智能使用者的法律责任问题研究[J]. 中国价格监管与反垄断,2024(10):59-61.
[30] 袁曾. 生成式人工智能治理的法律回应[J]. 上海大学学报(社会科学版),2024(1):28-39.
[31] 国家互联网信息办公室. 生成式人工智能服务管理暂行办法[J]. 中华人民共和国公安部公报,2023(5):2-5.
[32] 马永强.《生成式人工智能的风险挑战与监管框架:兼谈〈生成式人工智能服务管理办法(征求意见稿)〉》[EB/OL]. (2023-04-24)[2024-11-12]. https://m.thepaper.cn/baijiahao_22843718.
[33] Verma P, Oremus W. ChatGPT invented a sexual harassment scandal and named a real law prof as the accused[J]. Washington Post,2023,14:685-710.
[34] 曹险峰. 人工智能具有法律人格吗[J]. 地方立法研究,2020(5):67-75.
[35] 付其运. 人工智能非主体性前提下侵权责任承担机制研究[J]. 法学杂志,2021(4):83-90.
[36] 童云峰. 走出科林格里奇困境:生成式人工智能技术的动态规制[J]. 上海交通大学学报(哲学社会科学版),2024(8):53-67.
[37] 郭鹏,李展鹏. 论复杂人工智能生成物在著作权法的定性:兼评"AI文生图著作权案"[J]. 科技与法律(中英文),2024(4):73-82.
[38] 王春晓. AI著作权宣判,判赔500元[EB/OL]. (2023-12-08)[2024-11-12]. https://mp.weixin.qq.com/s/PjPfoFw5q4JuIm7lO4oZSQ.
[39] 李汶龙,郭佳仪. GenAI版权分析需超越基础概念框架:评北互/李昀锴案[EB/OL]. (2023-12-04)[2024-11-12]. https://mp.weixin.qq.com/s/cycYiC1Ze9owHi1TXL_7rg.
[40] 卢安文. 生成式人工智能:风险、监管与治理模式探究[J]. 重庆邮电大学学报(社会科学版),2025(3):113-121.
[41] 徐伟,张丽梅. 人工智能立法:欧盟经验与中国路径[J]. 德国研究,2024(6):76-93.
[42] 刘子婧. 欧盟《人工智能法》:演进、规则与启示[J]. 德国研究,2024(3):101-128.
[43] 曾雄,梁正,张辉. 人工智能软法治理的优化进路:由软法先行到软法与硬法协同[J]. 电子政务,2024(6):96-107.
[44] 曾雄,张辉. 规制理论视野下的人工智能治理模式比较及启示:基于英美治理实践的观察[J]. 中国科技论坛,2025(2):117-126.
[45] Roberts H, Cowls J, HINE E, et al. Achieving a "good AI society": comparing the aims and progress of the EU and the US[J]. Science and Engineering Ethics, 2021,27(68):14.
[46] 张凌寒. 人工智能法律治理的路径拓展[J]. 中国社会科学,2025(1):91-110.
[47] 范进学. 人工智能法律主体论:现在与未来[J]. 政法论丛,2022(3):3-17.
[48] 刘强. 人工智能对知识产权制度的理论挑战及回应[J]. 法学论坛,2019(6):95-106.
[49] 吴汉东. 人工智能时代的制度安排与法律规制[J]. 社会科学文摘, 2017(12): 76-78.
[50] 刘练军. 人工智能法律主体论的法理反思[J]. 现代法学,2021(4):73-88.
[51] 甘绍平. 机器人怎么可能拥有权利[J]. 伦理学研究,2017(3):126-130.

[52] 赵万一. 机器人的法律主体地位辨析:兼谈对机器人进行法律规制的基本要求[J]. 贵州民族大学学报(哲学社会科学版),2018(3):147-167.
[53] 郑戈. 人工智能与法律的未来[J]. 探索与争鸣,2017(10):78-84.
[54] 冯洁. 人工智能体法律主体地位的法理反思[J]. 东方法学,2019(4):43-54.
[55] 袁曾. 生成式人工智能的责任能力研究[J]. 东方法学,2023(3):18-33.
[56] Hubbard F P. Do androids dreams: personhood and intelligent artifacts[J]. Temple Law Review, 2010,83:405-432.
[57] Rothenberg D M. Can Siri 10.0. buy your home: the legal and policy based implications of artificial intelligent robots owning real property[J]. Washington Journal of Law, Technology & Arts, 2015,11:452 .
[58] 杨清望,张磊. 论人工智能的拟制法律人格[J]. 湖南科技大学学报(社会科学版),2018(6):91-97.
[59] 陈军. 财产权、正当性及多元主义:现代财产权基本理论探析[J]. 中南大学学报(社会科学版),2013(6):132-141.
[60] 张劲松. 人是机器的尺度:论人工智能与人类主体性[J]. 自然辩证法研究,2017(1):49-54.
[61] 苏令银. 人工道德主体:哲学假设与认识论挑战[J]. 西南民族大学学报(人文社科版),2018(3):62-68.
[62] 孙笛. 人工智能体刑事主体资格否定论[J]. 政法论丛,2022(3):40-50.
[63] 储陈城. 人工智能时代刑法归责的走向:以过失的归责间隙为中心的讨论[J]. 东方法学,2018(3):35.
[64] 孙那. 确立人工智能法律主体地位的再思考[J]. 法学论坛,2024(5):112-121.
[65] 杰瑞. 卡普兰. 人工智能时代:人机共生下财富、工作与思维的大未来[M]. 李盼,译. 杭州:浙江人民出版社,2016:1-160.
[66] 叶欣. 私法上自然人法律人格之解析[J]. 武汉大学学报(哲学社会科学版),2011(6):125-129.
[67] Villalobos P, Ho A, Sevilla J, et al. Will we run out of data? Limits of LLM scaling based on human-generated data[EB/OL]. 2022: arXiv: 2211.04325. https://arxiv.org/abs/2211.04325.
[68] 季卫东. 数据、隐私以及人工智能时代的宪法创新[J]. 南大法学,2020(1):1-12.
[69] 蔡智权. 生成式人工智能助力新质生产力的价值证成、技术隐忧与战略因应[J]. 西南金融,2024(7):89-102.
[70] 孙祁. 规范生成式人工智能产品提供者的法律问题研究[J]. 政治与法律,2023(7):162-176.
[71] 丛立先,李泳霖. 聊天机器人生成内容的版权风险及其治理:以ChatGPT的应用场景为视角[J]. 中国出版,2023(5):16-21.
[72] Shin D, Park Y J. Role of fairness, accountability, and transparency in algorithmic affordance[J]. Computers in Human Behavior,2019,98:277-284.
[73] Diakopoulos N, Koliska M. Algorithmic transparency in the news media[J]. Digital Journalism, 2017,5(7):809-828.
[74] 苗菊,吴聪聪. 数字认知与传播中的多语言多模态术语知识库:社会应用与价值实现[J]. 中国科技术语,2023(4):12-20.
[75] 杜燕,谢新洲. 平台可供性视角下算法的嵌入与可见机制研究[J]. 信息资源管理学报,2024(5):91-103.
[76] 陈凤仙,连雨璐,王娜. 欧美人工智能监管模式及政策启示[J]. 中国行政管理,2024(1):77-88
[77] 邢亚杰,戚凯. 论当前美国政府的人工智能监管政策[J]. 国际观察,2024(4):31-57.
[78] 郭小东. 生成式人工智能的风险及其包容性法律治理[J]. 北京理工大学学报(社会科学版),2023(6):93-105.
[79] 王利明. 生成式人工智能侵权的法律应对[J]. 中国应用法学,2023(5):27-38.
[80] Lior A. AI strict liability vis-à-vis AI monopolization[J]. Columbia Science and Technology Law Review, 2020,22:90-92.
[81] Buiten M, DE STREEL A, PEITZ M. The law and economics of AI liability[J]. Computer Law & Security Review,2023,48:105794.
[82] 刘晓林. 生成式人工智能作品的版权风险与规范[J]. 传播与版权,2024(18):108-110.
[83] 宁园. 论人形机器人使用者的注意义务[J]. 东方法学,2024(3):38-48.
[84] 鲁甜. DeepSeek生成内容的版权侵权问题研究[EB/OL]. (2025-03-12)[2025-04-20]. https://mp.weixin.qq.com/s?__biz=MzA4MjY4MzM1NA==&mid=2649882149&idx=1&sn=517ae89783480d374defb2448fce1377&chksm=86aa5f222d2b055893fdde3240d3f4bfc7490b83edb6d7e031a0dc4d0c25123a6fe4648c50b9&scene=27.

From ChatGPT to DeepSeek: Legal risks and three-dimensional regulations of generative artificial intelligence

Xiong Jinguang, Zhang Zheng

(*School of Law, Jiangxi University of Finance and Economics, Nanchang 330013, P. R. China*)

Abstract: From ChatGPT to Sora and then to DeepSeek, generative artificial intelligence is constantly evolving and innovating, but its potential legal risks are also becoming increasingly serious. By analyzing the three-stage operation mechanism of preparation-operation-generation of generative artificial intelligence, it can be known that the core technologies involved in the three stages are different so that the existing legal risks also vary. Specifically, the core of the preparation stage of generative artificial intelligence lies in massive data and machine learning. The operation stage mainly involves algorithm techniques, manual annotation, and autonomous learning. The generation stage relies on data decoding and sample generation. Correspondingly, its legal risks mainly lie in the protection of privacy and personal information in the preparation stage, data security and algorithm bias in the operation stage, and copyright ownership, ideology and social order in the generation stage. However, the existing legislation fails to provide detailed guidance on the core contents such as the legal status, regulatory standards, and sample attribution of generative artificial intelligence. Based on this, on the basis of a comparative analysis of the governance paradigms and experiences of countries such as the United States, the United Kingdom, and the European Union, in combination with China's national conditions and practical status, we should focus on the three-dimensional path of civil law protection-regulatory standard-industry norms to regulate the legal risks of generative artificial intelligence to safeguard the legitimate rights and interests of citizens. Firstly, at the civil law level, we should clarify the legal object status of weak generative artificial intelligence and the fictitious legal subject status of strong generative artificial intelligence, strengthen the protection of personal information through explicit authorization of private information and data encryption technology, and improve the intellectual property determination standards based on the attributes and rights ownership of generated samples. Secondly, at the regulatory standards level, we should implement the whole process supervision covering the preparation-operation-generation stage for technologies such as algorithms, enhance the transparency of related technologies by formulating technical transparency standards, introducing interpretable technologies and establishing an accountability-feedback guarantee system, and form a characteristic regulatory model of government-society-enterprise linkage that the government provides policy support for citizens and enterprises, citizens actively participate in regulatory governance and feed back infringement information to the government and enterprises, and enterprises, guided by government policies and citizens' demands, contribute to social development. Finally, at the industry norms level, we should clarify the applicable liability principle for its infringement through the three infringement forms of generative artificial intelligence, implement the legal obligations of service providers and users that providers should undertake obligations such as content review and security guarantee, while users should fulfill obligations such as reasonable use and operation as well as information feedback, and open up social consultation and feedback channels to curb the occurrence of infringement phenomena and improve the efficiency of resolving infringement disputes by popularizing citizens' rights and obligations, standardizing citizens' usage methods, and enhancing the connection between enterprises and citizens.

Key words: generative artificial intelligence; legal risks; three-dimensional regulations; ChatGPT; Sora; DeepSeek

(责任编辑 刘 琦)