Open Journal of Legal Science 法学, 2025, 13(3), 459-465
Published Online March 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.133066

Hans汉斯

论生成式人工智能的法律风险及规制

姜高洁

青岛大学法学院，山东 青岛

收稿日期：2025年2月11日；录用日期：2025年2月25日；发布日期：2025年3月18日

摘　要

生成式人工智能已经获得普遍应用，在便利生活的同时，也带来了法律风险，包括但不限于数据信息风险、知识产权风险、伦理风险和垄断风险。为避免风险扩大，促进人工智能健康发展，我们应当进行专项立法，更有针对性地解决生成式人工智能暴露或可能存在的问题，其次，由于法律具有滞后性，立法工作需要时间和实践的积累，目前还应当从数字合规的角度，加强监管力度，最后，还应重视行业自治，发挥行业群体的主观能动性，以便更灵活、更高效地防范生成式人工智能的法律风险。

关键词

生成式人工智能，法律风险，法律规制

The Legal Risks and Regulation of Generative Artificial Intelligence

Gaojie Jiang

Law School, Qingdao University, Qingdao Shandong

Received: Feb. 11th, 2025; accepted: Feb. 25th, 2025; published: Mar. 18th, 2025

Abstract

Generative artificial intelligence has been widely applied, bringing convenience to life while also posing legal risks, including but not limited to data and information risks, intellectual property risks, risks to personality rights and ethics, and monopoly risks. To prevent the expansion of risks and promote the healthy development of artificial intelligence, we should carry out specialized legislation to more specifically address the problems exposed or potentially existing in generative artificial intelligence. Secondly, given the lagging nature of laws, legislative work requires time and the accumulation of practical experience. Currently, we should also strengthen regulatory efforts from the perspective of digital compliance. Finally, we should attach importance to industry self-

文章引用: 姜高洁. 论生成式人工智能的法律风险及规制[J]. 法学, 2025, 13(3): 459-465.
DOI: 10.12677/ojls.2025.133066

regulation and leverage the subjective initiative of the industry group to more flexibly and efficiently prevent the legal risks of generative artificial intelligence.

Keywords

Generative Artificial Intelligence, Legal Risks, Legal Regulation

1. 引言

随着人工智能技术的纵深发展和广泛应用，关于人工智能带来的法律风险也得到关注并引发了大量的讨论，科学技术是一把双刃剑，人工智能技术也是如此。2022 年 11 月，美国 OpenAI 公司基于人工智能的对话生成模型，发布了 ChatGPT，其使用自然语言处理和机器学习技术与用户进行自然对话。历经两年多的发展，以 ChatGPT 为代表的生成式人工智能(Generative Artificial Intelligence)业已成为推动新一轮数字变革的关键力量，其可以根据训练数据创造全新、原创的信息内容，实现了此类技术模型从“决策型”向“创造型”的重要转变。人工智能在得到快速发展、为科技进步和产业发展带来了巨大助力的同时，引发了一系列新的法律风险挑战。

2. 生成式人工智能的概述

2.1. 生成式人工智能的概念

人工智能是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。它是一种基于机器学习和人工智能技术的范畴，其目标是让计算机系统能够自主地生成包括但不限于文本、图像、音频、视频、代码等各种类型的数据，而不仅仅是对已有数据进行分析和处理。人工智能可以模仿人类的创造力和想象力，甚至在某些方面超越人类的能力。人工智能通常是先从大量的数据中学习模式和特征，然后基于所学到的知识和模式，根据用户的需求或给定的提示，生成新的、符合要求的内容。例如，在文本生成方面，它可以学习到单词之间的组合规律、句子的结构模式等，从而根据给定的主题或开头语句，生成一段连贯的文本；在图像生成方面，它可以学习到图像中的颜色、形状、纹理等特征的分布和组合方式，进而生成新的图像。总之，人工智能是人工智能领域中一个具有重要影响力和发展潜力的方向，它为人们提供了一种全新的方式来获取和创造各种类型的信息和内容。

2.2. 生成式人工智能的功能分类

人工智能可以根据学习到的数据自动生成文本、图像、音乐等内容，即利用人工智能实现自然语言处理、视觉艺术、音频合成等功能应用。生成式人工智能主要分为以下四类。

第一类即应用最为广泛的文本创作类，它可以进行文章创作，根据给定的主题或者关键词生成一篇完整的文章，还能进行故事编写，构建情节、人物等元素来创作故事。

第二类为对话生成类，对话生成类人工智能可以像聊天机器人一样与用户进行交互对话，依靠这种功能，人工智能可将收集来的数据经过训练或组合，根据问话中的关键词，自动输出为科普答案，能够提高检索效率。

第三类为图像创作类，在图像生成领域的生成式 AI，能够依据输入的条件或者随机噪声创作图像。

第四类为音频创作类，音乐创作软件利用它能根据用户设定的风格、节奏等条件生成音乐片段。同时，在音频创作方面人工智能对语音合成功能有诸多应用，一是文本转语音，根据输入的文本内容，生成自然流畅且富有情感的语音，这在有声读物制作、语音导航、智能客服等方面应用广泛；二是语音风格模仿，能够模仿特定人物的声音特点和说话风格进行语音合成。

3. 生成式人工智能或将带来的法律风险

通常认为，法律风险来自于行为，人工智能生成成果可以视为是一组代码或一项程序的运行，是编译程序的组织或个人的行为，该行为能够引起法律上的权利义务的产生、变动或消灭，尤其是能够带来法律上的风险，并且这种风险存在于生成式人工智能运用的全过程。

3.1. 数据信息风险

我国《个人信息保护法》的出台，代表了在数字信息时代，我国愈发注重保护个人信息安全，《个人信息保护法》要求处理个人信息应当取得个人同意，然而，这一要求已在实践中逐步沦为形式化，各大个人信息收集、使用的手机 APP 及软件，在使用前基本都会要求用户同意授权其处理和收集个人信息、使用信息等，否则无法使用。人工智能恰恰需要大量的数据训练，从而变得更加智能、更加符合用户需求，这些数据中不乏私密信息、敏感信息或个人隐私信息。不论是作为用户还是执法者，在未进入行政或司法程序前，都只能从外在观察信息的处理，而对于信息如何收集、如何分类、如何存储以及如何处理缺乏了解，甚至事实上也无法掌握。因此，数据信息由运营方单方掌握，带来了数据来源风险，部分运营商可能会“被迫”用户同意处理敏感信息，此外，数据存储时还可能被其他系统入侵，也即会受黑客的侵袭，而黑客拿到这些数据后，又有可能用于其他途径，由于其获取信息的来源就是非法的，因此不论其是否将获取的数据用于合法途径，都是非法的。

除了数据来源合法性风险外，还需考虑数据准确性风险。在人工智能训练初期，其数据样本主要来源于网络，这些数据具有基数大、内容多样、来源复杂等特点，准确性难以保障。如果投入模型进行训练的数据是错误的，那么生成式人工智能输出的成果产品也大概率是错误的。尤其是对于问答型人工智能，其不能主动产生信息，只能获取信息，并根据获取到的信息生成答案，那么如果训练时或者在模型构建时的数据信息就是不准确的，那么当用户对其提问，也会得到错误的答案。

3.2. 知识产权风险

知识产权风险分为两个维度，一是生成式人工智能所生产出的成果产品的知识产权风险，具体又可细化为知识产权归属、知识产权保护两方面问题；二是生成式人工智能所生产出的成果产品侵犯他人知识产权。

关于第一个维度，目前讨论较为热烈。首先必须肯定人工智能所产生的成果产品拥有著作权，其次还需关注该著作权归属于何方。北京互联网法院判决了我国首例人工智能生成图侵权案件[1]，原告李某使用开源软件 StableDiffusion 通过输入提示词的方式生成涉案图片，后将该图片以“春风送来了温柔”为名发布在小红书平台，被告刘某在自己的文章中使用了该图片，并且未标注原作者及出处，法院经审理，查明了案涉图片的生成过程，该软件可以根据用户的不同指令生成不同的图片，而案涉图片也是经过原告李某一步步的指令生成的，如果修改指令，图片就会发生变化。因此，法院认为案涉图片属于美术作品，主要原因为该作品符合“独创性”的要求，能够体现作者的个性化表达，故应当受到著作权法的保

[1]北京市互联网法院(2023)京 0491 民初 11279 号民事判决书。

护。至于著作权的归属问题，法院认为案涉作品虽然由人工智能产出，但是其著作权显然不能归人工智能所有，由于案涉图片是原告李某的智力投入产出的，体现的个性化表达也是李某的，因此著作权应归属于李某。从司法判例中，可以看出，生成式人工智能产出的成果如果具备了知识产权法所保护的智慧成果的特征，就应当受到知识产权法的保护，具备拥有知识产权的可能性。而对于知识产权的归属问题，学界有观点认为应在秉持以意思自治约定归属优先的同时，结合实质贡献、投资激励以及利益平衡原则分配著作权归属[1]，也即有约定依约定，没有约定依贡献度确定，前文所述案例中，北京互联网法院根据案涉图片是原告也即用户的表达的体现，确定著作权归属于原告。即便有确权原则，面对纷繁复杂的现实状况，如何确定人工智能输出的作品的权属问题，仍然存在困难，并且，需要警惕运营商会利用优势地位，在用户协议中提前约定著作权的归属。

关于第二个维度，生成式人工智能输出的内容，既可能在没有合法来源的情况下直接引用他人受法律保护的作品，还可能将使用者输入的自己的作品擅自提供给他人使用。人工智能的运行模式决定了人工智能输出的内容无法完全避免直接使用他人作品，不论这种作品是其主动获取的，还是由用户提供的，不论哪种，在没有授权的情况下，都会侵犯已有的知识产权。下文将具体列举几种情况。由于生成式人工智能可以根据程序编译作品，有可能侵犯他人作品的改编权，如用户将他人的小说作品通过指令，让人工智能生成视频作品，就会侵犯原小说作者的改编权。人工智能还可以将已有的作品进行编排，如将某位作者的全部作品进行汇编，就会侵犯该作者的汇编权。另外，未经授权和释明，利用人工智能将已有的作品改编或汇编，并在网络上传播，即使程度不构成侵犯原作者的改编权或汇编权，也会侵犯其信息网络传播权。判断是否侵权或将是一个难题，而确定侵权主体又将成为另一个难题。著作权侵权采用无过错原则，那么不论侵权模式如何，人工智能的运营商是否均应当承担赔偿责任？因为人工智能输出内容侵犯他人知识产权时，人工智能必然要参与到侵权过程中，既然是无过错归责原因，除非人工智能的运营商能够证明人工智能在使用过程中不存在侵权，否则，不论用户是否有侵权的意图，是否善用，也不论人工智能是否直接侵犯他人知识产权，既然人工智能无法追责，人工智能的运营商都将对外承担侵权责任。对知识产权的强保护原则，无疑会加重运营商的责任，迫使运营商在研发、运营等环节更加规范，进而促进人工智能健康发展。

3.3. 伦理风险

人工智能技术凭借其强大的数据处理能力，通过搜集、分析并训练特定个体的多维度历史数据，能够模拟并创造出其外貌、声音、表情及动作等独特特征，进而将这些要素转化为数字形式，实现对个体的“复制”与“再现”。从技术层面来看，人工智能生成数字化带来了双重挑战：一是人格权益受损的风险日益凸显，即在数字化过程中可能侵犯被数字化对象的肖像权、隐私权、名誉权等合法权益；二是伦理困境愈发严峻，即数字人在与用户的持续深入交互与训练过程中，其生成的内容愈发满足用户的特定需求与偏好，而与被数字化对象本人的意愿与期望相悖，导致用户产生情感错位、身份混淆等心理困扰，进而引发深刻的伦理危机[2]。

随着人工智能技术的不断进步与深度学习技术的快速发展，“深度伪造”(Deep fake)技术产生并迅速发展成熟，目前已经得到广泛的应用。所谓的“深度伪造”，简而言之，就是通过人工智能，可以获得一个与他人声音、容貌等高度相似的图像与视频，包括生成和替换，例如通过人工智能更换肖像，可将使用甲肖像拍摄的视频更换为乙肖像的视频，并且，人工智能更换的视频肖像会与乙本人高度相像，难以辨认真假。除了视频外，声音也同样可以“复制”，知名企业家雷军的 AI 语音就十分火爆，已引起央视新闻的关注并在新闻中报道，用户可以录制一段音频，通过人工智能技术转化，变成雷军音色的音频，不仅音色相像，语气、停顿等都十分自然，难以辨别其是否为雷军本人所述。因此，在未经授权的情况

下该技术能够轻易复制、修改甚至篡改他人肖像从而对肖像权等构成严重威胁。未经肖像权人许可而擅自制作、使用或公开其肖像，是最为常见的侵权方式，使用者可能出于不同的目的，擅自使用他人的肖像生成视频、图像等，一是出于商业化目的并从中牟取利益，二是为了获取流量或出于报复心理，恶意篡改和传播肖像，生产虚假视频，制造谣言。由此引申出，生成式人工智能输出的内容极有可能会侵犯他人的名誉权、隐私权等，降低他人的社会评价，不仅对于名人有不良影响，对于普通大众的消极影响也不容忽视，如男女朋友分手后，一方擅自使用另一方的肖像，制作恶搞视频，发布于互联网平台，并得到一定的转发、浏览或评论，很容易造成一方的困扰，即使一方后又删除视频或进行道歉，已经造成的不良影响也难以消弭。

事实上，目前的人工智能技术已发展到一定的高度，其不仅可以从外貌、声音等方面进行模仿、复刻，还可以表达情绪，容易引起人类的感情共鸣，从而引发更大的伦理危机。人工智能不具备真正的情感，只是通过学习模仿，对情感进行机械性展示，人类与人工智能进行情感交互，表面上是优化了人类的情感体验，但长此以往，存在削弱人类情感能力、淡化人际情感交往的风险[3]。装配生成式人工智能的数字人在社会中的定位变得异常复杂且充满争议，既然数字人能够模拟人类的行为，甚至模仿人类的情感，理应享有一定的身份认同，但如前文所述，其行为和情感只是基于机械的运转所表现出来的现象，哪怕再逼真、再贴切，人工智能也不具有主观意识，不能赋予其独立的法律地位。当前，有人利用人工智能“复活”逝者，得到情感依托和慰藉，尽管用户在主观上有强烈的赋予人工智能社会定位的需求，哪怕研发出形态逼真的拟人机器人，也无法将这种实体定位为社会中的“人”，而在运用人工智能模拟逝者的使用过程中，还可能引起用户生死观念的扭曲，导致生死观念混乱。

3.4. 垄断风险

生成式人工智能的研发、运营需要大量数据样本和超强计算能力，这样的经营者自然会具备市场优势地位，拥有较为深厚的经济基础和科技实力，这类经营者通常具有较高的垄断风险。一般说来，若某经营者在竞争的市场范围内占据极高份额，且长期设置壁垒阻碍、影响其他经营者进入该市场，就可以认定为垄断。

人工智能依附于运营商企业，运营商可以通过网络效应、技术屏障、规模效应等多种方法建立自己的市场壁垒，逐步形成市场垄断逐渐获得市场支配地位[4]。运营商获得市场支配地位的同时，锁定效应的产生会进一步巩固运营商的市场支配地位，提高市场垄断的风险[5]。此外，在生成式人工智能研发领域，技术垄断也并不罕见。技术垄断是指通过对某件或某类产品的关键技术拥有权将竞争对手排挤出局，进而达到生产此类产品的垄断权[6]。在拥有强大技术的支撑和对利润等经济利益的诱惑下，人工智能运营商很容易选择采用技术垄断的手段，来获取更高的经济效益和更先进的技术。因此，对于科技行业来说，技术力量与市场控制地位具有相互配合的特点，经营者极有可能会利用其市场支配地位，控制技术产生或分配，从而加固市场和技术的双重垄断。

4. 生成式人工智能风险的法律规制路径

4.1. 推动专项立法，形成体系化法律规制体系

我国目前有关于人工智能的立法，但现行法律法规分散在各类文件中，且法律规范的层级较低，没有形成统一的法律网格，效力上存在缺陷，治理效率也不高。另外，生成式人工智能所致风险涉及多领域，类型多样且十分复杂，其本身的特点导致相关法律很难直接予以规制。生成式人工智能法律风险规制的重心应当首先放在立法之上，针对人工智能进行专项立法，形成专门的法律体系，从而达到从源头规制生成式人工智能带来的法律风险的效果。

具体而言，应当从生成式人工智能的特点和特殊风险出发，综合考量社会因素、司法实践等方面的要求，进行适用范围广、适用难度低的立法。从立法内容上看，首先，应当明确保护个人隐私、防止歧视、确保知识产权等；其次，还应从法律层面具体确定生成式人工智能的范围和特征，以准确界定法律适用范围；最后，必须明确生成式人工智能技术的相关责任主体，例如技术开发者、服务提供者、使用者，并且规定这些主体在侵权责任承担中的相应责任以及义务，强调提供相关产品或服务的个体以及使用生成内容的个体都需承担相应的法律责任。现行法律中的网络服务提供者类型无法涵盖生成式人工智能服务提供者，以内容生产者对生成式人工智能服务提供者进行规制存在障碍，因此，在立法上应首先明确生成式人工智能服务提供者的法律地位。再者，可制定法律进一步提升人工智能算法的透明度。开发者有义务使用通俗易懂的语言向用户阐释算法的基本逻辑、算法结果的用途等，并为使用者、其他第三方创建申诉渠道[7]。

4.2. 加强监管，健全数字合规体系

在规制人工智能生成数字人技术的开发经营者与运营平台时，法律制度的针对性规定与数据合规层面的明确职责同等重要，以确保全面覆盖两者在数据生命周期的各阶段行为。

健全数字合规体系离不开对开发经营者建立的数据采集与审核机制，确保数据来源具有合法性，严禁非法抓取、买卖、滥用个人数据，此外，还应加强对合作第三方的数据监管。同样，应当着重审核数据供应商的资质，从事数据处理行业应获得专门的行政审批，加强审核数据处理流程，对数字处理实施全过程监管，例如数据收集、处理、存储、使用等所有环节，以经营商为抓手，通过严格的源头控制来降低数据合规风险，保障数字化对象与用户的合法权益。

由于目前算法的不透明性和潜在偏见正在损害用户权益，算法透明度制度的实施是提升算法公正性和可解释性的关键。除了对开发商实施数据层面的监管外，还应强制要求开发经营者对其算法进行透明度管理，包括公开算法的基本原理、训练数据、决策逻辑及潜在影响等，并对涉及用户权益的算法决策进行伦理评估，公开评估结果。此外，平台还需定期复审其运营的数字人技术，加强平台监管，确保持续符合数据合规要求，并评估算法的透明度和可解释性，防止算法歧视。

针对当前人工智能监管存在的多头管理、治理碎片化等问题，监管制度应构建沟通协调机制，凝聚监管合力。在尚未制定专门法律的情况下，可通过合理划分权力来加强协调配合，如明确网信办的核心地位，确保其在人工智能风险规制中的有效指挥和统筹；同时，厘清各部门在不同治理环节的责任分工，避免职责重合和交叉，建立常态化、规范化的联动机制，以破解多头监管难题，实现协同治理。

4.3. 加强行业自治，促进行业健康发展

人工智能行业作为新兴行业，法律从业者、执法者对其了解肯定远不如行业内部，相较于生成式人工智能的开发者，知识、信息的不对等导致风险治理主体和普通用户届处于弱势和不利地位。因此，必须建立健全行业自治机制，弥补法律规制的局限。并且，数据具有不可更改性，一经生成就不能修改，而法律具有滞后性，因此当生成式人工智能造成危害时，仅凭法律救济难以及时制止损失。为此，有必要建立自治机制，填补风险规制。

加重人工智能开发者及服务提供者的义务，要求其进行事前、事中及事后预案，预先评估数据安全风险并对生成式人工智能可能带来的风险，公布规制风险的具体方案，必要时，还应当对公布的方案进行解释，以减轻执法者的监督负担，也便于用户更加了解和掌握人工智能的正确使用途径，对于开发者及服务提供者而言，事前预案越充足，其事后的赔偿责任就会越轻。开拓救济申诉途径，当生成式人工智能滥用个人信息时，能有相应的救济途径。

更进一步来说，还应建立运营平台与服务经营者之间的合作与共享机制，确保人工智能生成数字化人格的全链条中数据流通的合法性和合规性。这涉及建立数据共享协议和标准，明确数据共享的范围、方式和责任分配，推动双方的数据共享与合作，促进数据的合规利用和创新发展。对于敏感数据，平台与经营者应采取严格的加密存储、访问控制等安全措施，防止数据泄露和非法使用，这既是行业合作，也是行业自治的方式之一。

5. 结语

面对生成式人工智能带来的挑战，我们既不能放任发展，也不宜过于畏惧，而是运用法律为人工智能技术划定发展及运营框架，确保法律的红线不被逾越的同时，保障技术革新，只有这样，我们才能确保人工智能技术在推动社会进步的同时，真正造福于全人类，实现技术与法律的和谐共生，共创一个更加智慧、公正、包容的未来。在这个过程中，每一步都需谨慎而坚定，因为这不仅关乎技术的健康发展，更关乎社会的公平正义与人类文明的未来走向。

参考文献

[1] 丛立先, 李泳霖. 人工智能文生视频大模型的作品风险、著作权归属及有效治理[J]. 载新疆师范大学学报(哲学社会科学版), 2024(6): 101-111.

[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. https://link.cnki.net/urlid/32.1771.C.20241106.1408.002

[3] 谢瑜, 王潇毅. 人工智能情感的伦理风险及其应对[J]. 伦理学研究, 2024(1): 133-134.

[4] 谢燕飞. 数字经济新业态下市场支配地位的认定问题研究[D]: [硕士学位论文]. 南昌: 南昌大学, 2022.

[5] 贵海军. 互联网平台市场支配地位的认定研究[J]. 黑龙江生态工程职业学院学报, 2021(3): 57-59.

[6] 刘永红, 李文颖. 生成式人工智能的法律风险及其规制路径[J]. 内江师范学院学报, 2024, 39(9): 94-100.

[7] 包思衡. 生成式人工智能的法律规制研究[J]. 电脑知识与技术, 2024, 20(23): 42-45.