Interdisciplinary Science Letters 交叉科学快报, 2026, 10(2), 465-469
Published Online March 2026 in Hans. https://www.hanspub.org/journal/isl
https://doi.org/10.12677/isl.2026.102058

Hans汉斯

GAI知识产权安全与信息安全的关联性研究

马国巍

中国矿业大学公共管理学院(应急管理学院)，江苏 徐州

收稿日期：2026年2月17日；录用日期：2026年3月9日；发布日期：2026年3月18日

摘　要

随着生成式人工智能(GAI)技术的快速迭代，知识产权保护面临新的挑战，亟需在现有法律框架下探索适应技术特性的治理路径。本文首先梳理了相关文献，总结了GAI在打破数据、算法与内容边界后，引发的权利客体、主体及归属界定模糊等共性问题。基于此，本文分析了当前亟待解决的关键风险：核心数据资源的保护不足可能导致企业竞争优势的流失；算法与模型的过度专利化可能形成技术壁垒，进而抑制行业创新生态的活力；生成式内容的版权归属不清则加剧了法律确权与合规风险。针对上述问题，本文在分析欧美相关政策演变趋势的基础上，提出了完善法律法规确权、建立数据交易合规机制、构建多元协同治理体系等具体对策。旨在平衡GAI技术创新与知识产权保护，维护公平竞争的市场秩序。

关键词

GAI，知识产权安全，信息安全，产业竞争力

Research on the Correlation between GAI Intellectual Property Security and Information Security

Guowei Ma

School of Public Policy & Management School of Emergency Management, China University of Mining and Technology, Xuzhou Jiangsu

Received: February 17, 2026; accepted: March 9, 2026; published: March 18, 2026

Abstract

With the rapid evolution of Generative Artificial Intelligence (GAI) technology, intellectual property (IP) protection faces unprecedented challenges. It is urgent to explore governance approaches within existing legal frameworks that accommodate the specific characteristics of this technology.

文章引用: 马国巍. GAI 知识产权安全与信息安全的关联性研究[J]. 交叉科学快报, 2026, 10(2): 465-469.
DOI: 10.12677/isl.2026.102058

This paper first reviews relevant literature and summarizes common issues arising from the blurring of boundaries between data, algorithms, and content by GAI, specifically focusing on the ambiguity in defining the subjects, objects, and ownership of rights. Building on this analysis, the paper examines key risks that urgently need to be addressed: insufficient protection of core data resources may lead to the erosion of corporate competitive advantages; excessive patenting of algorithms and models may create technical barriers, thereby stifling the vitality of the industrial innovation ecosystem; and unclear copyright ownership of generated content exacerbates risks associated with legal determination of rights and regulatory compliance. In response to the aforementioned issues, this paper, after analyzing the evolving trends of relevant policies in Europe and the United States, proposes specific countermeasures such as improving laws and regulations for rights confirmation, establishing a compliant mechanism for data transactions, and constructing a multi-stakeholder collaborative governance system. These measures aim to strike a balance between technological innovation in GAI and intellectual property protection, while safeguarding a fair and competitive market order.

Keywords

GAI, Intellectual Property Security, Information Security, Industrial Competitiveness

1. 引言

在数字经济时代，生成式人工智能作为新兴技术的代表，正在深刻改变全球产业格局。现有文献普遍认为，GAI 不仅具备强大的内容生成能力，更通过海量数据的训练与迭代，逐渐渗透至金融、医疗、制造及教育科研等关键领域，成为推动经济社会发展的新动力。然而，技术的快速发展也带来了知识产权保护的新课题。传统的知识产权制度主要基于人类智力成果构建，而 GAI 涉及的数据投喂、算法黑箱及自动生成特性，导致权利归属、侵权认定及利益分配变得异常复杂。

梳理相关研究发现，当前制度设计存在一定的滞后性，这不仅引发了法律适用层面的争议，也对数据合规与市场秩序构成了挑战。在这一背景下，知识产权保护已不再单纯是法律层面的民事纠纷，而是演变为关乎产业核心竞争力、市场公平交易及企业数据资产安全的核心要素[1]。如果 GAI 相关的核心数据、算法模型及生成内容缺乏有效的知识产权保护机制，企业将面临数据资产流失、创新活力受损以及法律合规风险加剧等实际问题。因此，深入剖析 GAI 知识产权保护面临的具体问题，厘清其对数据安全与市场秩序的影响，对于构建适应新时代需求的治理体系具有重要的理论意义与现实价值。本文旨在通过分析 GAI 时代知识产权面临的新挑战，总结现有研究的不足，并针对性地提出相应的治理策略，以期为我国相关产业在智能化浪潮中实现创新发展与合规保护的平衡提供参考。

2. GAI 背景下知识产权保护的新挑战与风险分析

2.1. 数据训练阶段的知识产权侵权与数据合规风险

现有研究表明，生成式人工智能的研发与运行高度依赖大规模、高质量的训练数据，这使得数据采集与处理阶段面临着复杂的知识产权法律风险。众多 GAI 模型在训练过程中，未经授权抓取了大量受著作权保护的文学作品、艺术作品及代码库，这种行为虽然目前在法律定性上尚存争议，但已实质上触及

了原权利人的合法权益边界。从信息安全与合规管理的角度来看，这种大规模的数据爬取不仅涉及版权侵权问题，更涉及数据隐私与敏感信息保护。如果 GAI 训练数据中包含了涉及个人隐私、商业秘密或特定行业限制的数据，且缺乏严格的脱敏处理与知识产权界定，这些数据资源便可能在模型分发中被滥用或违规外泄。数据被视为数字经济时代的关键生产要素，现有研究指出，生成式人工智能的研发高度依赖大规模数据，数据采集面临复杂的法律风险[2]。因此，若缺乏有效的法律规制，企业在数字经济领域的竞争优势可能因数据合规管理缺失而受影响。这不仅是版权问题，更是数据资源的合法使用与合规管理问题。

2.2. 算法模型阶段的“黑箱”特性与技术失窃风险

算法与模型是 GAI 系统的核心组件，承载着研发主体的关键技术成果与商业秘密。然而，深度学习算法具有显著的“黑箱”特征，其内部的逻辑路径与参数权重难以被直观解释，这给知识产权的确权与保护带来了技术性难题。在当前的专利与著作权体系下，算法往往难以获得传统意义上的专利保护，而更多是作为商业秘密存在。但是，GAI 模型的分发与部署过程极易导致核心算法的逆向工程破解或非法复制。一旦掌握关键技术的 GAI 模型被竞争对手通过不正当手段获取并进行模仿或改进，原权利人的技术优势及市场地位将面临严重受损的风险。从产业竞争的视角审视，GAI 算法模型的不当获取或泄露可能导致企业研发投入无法获得预期回报[3]。在产业竞争中，若核心算法知识产权保护不力，企业在高端技术领域的市场地位将面临挑战，不仅影响经济效益，也可能制约产业的自主发展能力。

2.3. 生成内容阶段的权利归属模糊与内容合规风险

现有研究指出，生成式人工智能产出的内容在形式上与人类创作的作品高度相似，但由于其缺乏人类作者的独创性意图，导致其在法律层面的权利归属存在显著争议。一方面，若将生成内容的权利完全赋予使用者，可能会诱发针对海量作品的高频模仿与侵权，扰乱原有的文化创作市场秩序；另一方面，若完全否定生成内容的知识产权保护，则可能导致大量低质内容充斥市场，且在发生纠纷时无法进行有效追责，从而加剧市场失灵。这种权利归属的模糊状态，给内容生态的治理带来了极大的不确定性。

权利归属的模糊状态，给内容生态的治理带来了极大的不确定性。若生成内容缺乏有效规制，可能影响网络信息的真实性与多样性，增加信息甄别成本，对内容市场的健康发展构成挑战[4]。如不良行为者可能利用 GAI 生成误导性信息，利用版权管理的漏洞在网络平台上迅速扩散，增加了信息甄别的难度与网络治理的成本，造成公众认知混乱。此外，低成本生成内容的泛滥可能对本土文化创意产业的市场份额形成挤出效应，削弱原创内容创作者的动力。因此，生成内容阶段的知识产权风险已超越了单纯的经济利益范畴，上升为关系到数字内容市场规范化治理与网络生态环境健康发展的复杂议题。

3. GAI 知识产权安全与信息安全的关联机制分析

3.1. 技术自主关联

现有研究指出，技术自主性是产业健康发展的重要支撑，而 GAI 领域的知识产权保护状况直接关系到核心技术的可控性与完整性。GAI 作为当前全球科技竞争的制高点，其背后的知识产权布局——包括基础架构专利、核心算法版权及数据集控制权——构成了国家技术自主的基石。如果一个国家的 GAI 产业发展受制于外部的知识产权壁垒，或核心关键技术掌握在他国手中，那么其在该领域的战略主动权将丧失殆尽。正如相关研究所指出，知识产权与信息安全之间存在深刻联系，知识产权在知识权力化过程中具有基础性作用[5]。当前，以美国为代表的发达国家正通过完善知识产权保护体系来维护其在人工智能领域的竞争优势，并利用出口管制等政策工具对高技术知识产权的转让进行管理[6]。在这种国际环境

下，我国 GAI 产业的知识产权安全直接关系到能否突破技术封锁，实现高水平科技自立自强。一旦核心 GAI 技术的知识产权防线失守，不仅会导致巨大的经济损失，更会使国家在未来的智能产业变革中丧失话语权，直接威胁国家科技安全与长远发展利益。

3.2. 经济安全关联

GAI 产业链条长、覆盖面广，涵盖了上游的数据标注、中游的模型训练与下游的应用开发。知识产权安全在这一产业链中扮演着防火墙与助推器的双重角色。首先，知识产权是维护产业链韧性的关键。面对日益频繁的国际知识产权诉讼，特别是非专利实施主体(NPE)的恶意诉讼，我国 GAI 企业面临巨大的合规风险与市场准入障碍。如果不构建完善的知识产权防御体系，关键企业可能因高昂的专利费或禁令而停产，导致产业链断裂。其次，知识产权的对外转让审查是防范经济安全风险的制度阀门。随着外资并购与技术出口活动的增加，若缺乏完善的审查机制，国外资本可能通过收购掌握核心 GAI 知识产权的企业，对本土关键技术的控制权产生影响，进而增加产业发展的不确定性[7] [8]。研究表明，构筑知识产权壁垒已成为发达国家维护竞争优势的重要手段，技术迭代与行业竞争加剧了涉外知识产权诉讼风险。因此，强化 GAI 领域的知识产权安全，实质上是构建一道坚固的经济安全防线，确保我国 GAI 产业链在复杂的国际竞争环境中保持独立、完整与富有韧性，防止因知识产权纠纷或流失引发系统性经济风险。

3.3. 信息生态关联

GAI 具有强大的信息生成与传播能力，其生成的文本、图像、音视频等内容已成为信息传播的重要载体。在这个维度上，知识产权安全与国家的信息文化安全紧密相连。一方面，GAI 生成内容的版权归属与使用规则决定了谁有权力控制信息的生产与流动。如果部分技术主体利用其 GAI 技术的知识产权优势，主导内容生成的标准与平台，可能会通过算法推荐机制影响信息的多样性，这对我国本土文化产业的创新与发展构成了潜在的挑战[9]。另一方面，GAI 技术的滥用可能导致虚假或低质信息的泛滥，而知识产权制度的缺位使得监管和打击这些虚假内容缺乏有效的法律依据。当虚假信息涉及公共服务、商业信誉或社会秩序时，可能造成严重的负面后果，增加社会治理成本。因此，从信息安全的高度审视，确立 GAI 生成内容的知识产权规则，不仅是保护创作者权益的需要，更是争夺信息传播主导权、维护意识形态安全的重要手段。我国需要在保障言论自由与鼓励创新的同时，通过知识产权立法规范 GAI 的内容生成行为，防止利用技术漏洞进行有害信息的传播，筑牢国家信息文化安全防线。

4. GAI 知识产权安全的治理对策

4.1. 完善法律法规，明确权利归属体系

针对 GAI 生成内容版权归属不清这一核心难题，立法机关与司法部门应当采取积极且审慎的态度，加快完善相关法律法规体系，以适应技术快速迭代的现实需求。应明确区分 AI 生成内容与人类智力成果的法律属性，建议在著作权法框架下出台专门的司法解释或指导案例，确立人类智力贡献作为确权的关键标准，规定只有人类作者在创作过程中付出了实质性智力投入的生成内容，方可获得版权保护。对于纯由 AI 自动生成的各类内容，可探索设立邻接权或特殊的财产权益保护机制，赋予投资者或使用者有限的权益，既防止权利滥用，又避免因缺乏保护而导致优质数据资源供给不足。其次，建立 GAI 生成内容的强制标识与登记制度，通过立法明确要求生成式内容必须带有可追溯的数字水印或技术标识，这不仅有助于公众甄别信息的真伪，也为后续的权利流转与侵权追责提供了确凿的法律依据。

4.2. 建立数据合规机制，保障训练数据安全

数据作为 GAI 技术研发的基础燃料，其合规使用直接关系到产业的健康发展与知识产权安全的防线

稳固。针对数据训练阶段普遍存在的侵权风险与隐私泄露隐患，亟需建立一套涵盖数据采集、处理、存储全生命周期的合规管理机制。一方面，应推动建立适应 AI 特性的合理使用制度。考虑到 GAI 模型训练对海量数据的刚性需求，立法部门应研究并在特定条件下豁免部分非商业性、科研性数据抓取行为的侵权责任，同时建立透明的版权清算与付费机制，如设立著作权集体管理组织延伸许可制度，使得数据使用者在支付合理报酬的前提下合法获取训练数据，从源头上化解版权纠纷。另一方面，企业必须强化内部的数据合规治理能力。鼓励企业引入隐私计算、联邦学习以及数据脱敏等先进技术手段，在保证数据可用不可见的前提下进行模型训练，严格阻断个人隐私、商业秘密等敏感信息的泄露路径。

4.3. 构建多元共治格局，强化行业自律

GAI 技术的复杂性与应用的广泛性决定了单一的法律规制难以涵盖所有风险，构建政府引导、行业协同、企业自律的多元共治格局显得尤为紧迫。针对算法黑箱带来的伦理风险及内容生成的不确定性，行业协会应发挥桥梁纽带作用，牵头制定技术伦理标准与知识产权保护指引。如制定生成式人工智能的内容标识标准、算法透明度披露规范以及数据交易流通规则，填补法律法规在实操层面的空白。同时，企业作为创新的主体，应建立健全内部合规审查流程，设立专门的知识产权风险防控部门，对模型研发、应用推广等环节进行全流程的风险监测。落实算法备案与安全评估制度，主动披露模型的潜在风险与局限性，增强技术应用的透明度与可信度。

5. 结语

生成式人工智能的崛起不仅是一场技术革命，更对现有的知识产权安全体系提出了严峻考验，其与信息安全的关联性日益紧密。本文通过分析发现，GAI 知识产权安全已超越了传统的私权保护范畴，成为影响产业技术竞争力、经济产业链韧性以及信息生态环境的关键因素。面对这一形势，我国应统筹发展与安全，通过完善法律确权、强化数据合规管理、构建多元治理机制等具体措施，有效化解知识产权风险，在激烈的国际竞争中保障数字经济的健康可持续发展。唯有通过多层次、全方位的治理策略，有效化解 GAI 领域的知识产权安全风险，才能在激烈的国际科技竞争中立于不败之地，切实保障数字经济的健康可持续发展与公共利益。

参考文献

[1] 杨丽丽. 云计算环境下数字艺术类图书馆面临的信息安全及知识产权保护[J]. 情报科学, 2019, 37(10): 114-119.

[2] Fahmi, M.S., Rado, R.H., Klau, R.G. and Utami, G.A. (2023) Enhancing National Food Security by Protecting Intellectual Property Rights for Farmers in Breeding Local Plant Varieties. *IOP Conference Series*: *Earth and Environmental Science*, **1253**, Article ID: 012073. https://doi.org/10.1088/1755-1315/1253/1/012073

[3] McCarthy, D.R. (2021) Imagining the Security of Innovation: Technological Innovation, National Security, and the American Way of Life. *Critical Studies on Security*, **9**, 196-211. https://doi.org/10.1080/21624887.2021.1934640

[4] 张国有. 3D 打印开放式服务平台信息安全及知识产权保护[D]: [硕士学位论文]. 太原: 太原科技大学, 2021.

[5] 云仲伦. 国家工业信息安全发展研究中心、工业和信息化部电子知识产权中心联合发布《新一代人工智能专利技术分析》报告[J]. 科技中国, 2024(5): 99.

[6] Kirti, G., Andrei, I., Copan Walter, G. and Chris, B. (2025) Protecting Intellectual Property for National Security: A Transition Report for the New Administration. Center for Strategic and International Studies (CSIS).

[7] 付勇. 对《调查信息安全与知识产权保护》教学设计的分析与反思[J]. 教育科学论坛, 2020(12): 63-66.

[8] 纽约大学研发 3D 打印防伪技术助力保护知识产权和信息安全[J]. 中国品牌与防伪, 2021(6): 70-71.

[9] Yang, D.V. (2024) U.S. and China: Intellectual Property and Strategic Competition. Nova Science Publishers.