

人工智能对“贸易面向型”数字知识产权规则的挑战及前瞻

周念利 罗 雨

内容摘要：人工智能作为第四次工业革命的关键技术，在深度融入跨境贸易的同时，也对“贸易面向型”数字知识产权规则构成严峻挑战。本文基于既有“贸易面向型”数字知识产权规则，深入分析算法的知识产权保护、人工智能大模型训练数据的侵权责任界定、人工智能生成物的知识产权保护及人工智能对数字知识产权执法的挑战等问题。研究发现：“贸易面向型”数字知识产权规则会制约算法的监管与保护；人工智能大模型训练阶段大规模复制受版权保护作品冲击着“复制权”规则；与人工智能生成内容相关的“贸易面向型”数字内容版权规则存在真空；人工智能的使用导致“贸易面向型”数字知识产权执法规则效力不足。未来，“贸易面向型”数字知识产权规则会呈现算法保护双重路径、嵌入“TDM 例外条款”“分层模式”应用及纳入“元数据标识”趋势。对此，作为数字贸易大国，中国应积极参与“贸易面向型”数字知识产权规则的塑造。

关键词：人工智能 区域贸易协定 数字知识产权规则 算法

DOI:10.14114/j.cnki.itrade.2026.04.003

一、引言

随着第四次工业革命的深入推进，数字技术成为数字贸易发展的关键引擎。由于数字技术具备知识密集型属性，其研发、应用与跨境流动均高度依赖知识产权保护。完善的知识产权保护体系既能激励创新，又能促进数字技术跨境传播，降低贸易成本与侵权风险。然而，数字技术尤其是人工智能(AI)的快速发展与跨境应用，使知识产权问题与数字产品和服务的跨境流动、数据要素配置、市场准入等贸易议题深度交织。在此背景下，国际层面对数字知识产权制度的探索呈现两种模式：一是“独立模式”，指各国或国际组织针对数字知识产权的发展特点及应用场景，专门制定和出台相关安排；二是“嵌入模式”，即以国际经贸协定为载体嵌入数字知识产权相关内容(周念利等，2024)。鉴于数字技术已深度融入数字贸易全流程，采用“嵌入模式”处理数字知识产权问题逐渐成为主流。尽管世界贸易组织(WTO)的《与贸易有关的知识产权协定》(TRIPS)为知识产权治理奠定了多边基础，但对数字技术发展的回应明显滞后。因此，数字知识产权规则构建重心逐渐向区域层面转移，《全面与进步跨太平洋伙伴关系协定》(CPTPP)、《美墨加协定》(USMCA)及《数字经济伙伴

[课题信息] 本文是国家社会科学基金重大项目“国际经贸规则重构背景下服务业高水平开放的制度创新与实践路径研究”(25&ZD102)的阶段性成果。

[作者信息] 周念利，对外经济贸易大学中国 WTO 研究院研究员；罗雨，对外经济贸易大学中国 WTO 研究院博士研究生。通讯作者：周念利，电子邮箱：znlube@163.com。作者感谢匿名审稿专家的宝贵意见和建议，文责自负。

关系协定》(DEPA)等区域贸易协定和数字贸易协定成为主要制度载体。这些协定将数字知识产权议题纳入贸易框架,推动形成更高标准的规则体系。例如,将电子形式的复制行为纳入保护范畴,强化数字知识产权执法措施,以及不得将源代码、算法、使用密码术的 ICT 产品访问、转让或披露作为市场准入条件等。相较而言,“嵌入模式”更易被主要经济体接受,也更具贸易关联性。基于此,本文聚焦此模式,将其界定为“贸易面向型”数字知识产权规则。

AI 是引领第四次工业革命的前沿数字技术。随着 AI 在跨境贸易中的广泛渗透,其引发的新型数字知识产权问题,如算法透明度、训练数据的合规性、生成内容的权利归属等已突破传统知识产权制度的框架,对现行“贸易面向型”数字知识产权规则构成严峻挑战。例如,现有的“源代码保护条款”面对 AI 算法“黑箱”时,存在算法透明度与公共监管问责的贸易平衡困境;AI 模型跨境训练大规模复制冲击“复制权”规则,导致海量数据版权获取的合规成本上升;AI 生成物跨境交付面临“贸易面向型”数字内容版权规则真空,导致贸易不确定性上升。尽管既有“贸易面向型”数字知识产权规则不断演进和细化,但其内容设计多源于应对传统数字环境下的知识产权问题,在面对 AI 所引发的非传统性、复杂性与动态性挑战时,显现出规则滞后、存在真空等局限性。鉴于此,本文对“贸易面向型”数字知识产权规则的主要内容进行梳理,重点分析 AI 给“贸易面向型”数字知识产权规则带来的挑战,并在此基础上对该规则体系的发展趋势进行前瞻性讨论。

二、文献综述

针对本文的研究主题梳理既有文献,与本文相关的研究主要集中在以下三类研究领域:

第一类是对与贸易相关的数字知识产权规则的发展演进的研究。目前,全球数字知识产权规则的发展经历了从传统规则扩展适用于数字贸易领域,到专门数字知识产权规则的提出,再到进一步深化拓展的三个阶段,并呈现出不同程度的“TRIPS+”特征(周念利等,2021)。虽然规则整体趋向高标准,但不同区域贸易协定的数字知识产权规则在约束效力(周念利等,2023)、执行强度(He et al., 2025)等方面仍存在差异。主要经济体之间对于数字知识产权规则相关议题也存在较大分歧(周念利等,2019)。具体而言,欧盟倾向于强调数字内容的版权保护,美国侧重于源代码以及其他关键技术的非强制转让,中国则立足于发展中国家立场,对美欧主张的高标准数字知识产权规则持审慎态度(周念利等,2021)。

第二类是对 AI 相关的知识产权国内规制及司法实践的研究。一方面,既有研究主要关注 AI 生成物的可版权性(Mercurio et al., 2021; 张笑尘, 2025)、著作权归属(徐家力, 2023)、著作权侵权认定(姚志伟, 2024)等问题。另一方面, AI 训练数据行为也受到学者的广泛关注,蒋洁如等(2025)、刘一帆(2025)、张伟君(2025)等认为大模型训练阶段的复制行为可能触发复制权的侵权风险。然而,也有学者持反对观点,李春晖(2025)主张 AI 训练过程中的复制行为并不会侵犯作品复制权。此外,为应对 AI 知识产权制度困境,学者们分别从制度创新(吴汉东等, 2024)、激励创新与权益平衡(宋河发等, 2026)等视角提出优化路径。域外经验也提供了重要参考,既有研究主要通过分析美国、欧盟等主要经济体的知识产权法律法规与相关经验,探索人工智能给知识产权法领域带来的挑战及相应的治理路径(张惠彬等, 2024; 邵永乐, 2025; Salle et al., 2025)。

第三类是对 AI 给“贸易面向型”数字知识产权规则带来的挑战及应对的研究。Irion(2022)解读并剖析了自由贸易协定中的源代码条款,发现源代码非强制转让条款可能会与数字技术的监管治理,尤其是算法问责制产生冲突。Jones(2023)和 Jones et al.(2024)对源代码非强制转让规则进行详

细分析,指出该规则阻碍了政府对算法和 AI 系统的有效监管和审计,并提出删除源代码非强制转让条款或大幅修改现行源代码条款的起草方式两种改革路径。

综上,既有文献多聚焦于国内立法与司法实践,而较少聚焦于国际规则层面。另外,与本文相关性最强的是第三类研究,但此类文献较为有限,且多着眼于某一特定条款,缺少从整体上对各个层面的“贸易面向型”数字知识产权规则的深层次分析。鉴于此,本文基于“贸易面向型”数字知识产权规则的主要内容,重点分析 AI 给该类规则带来的挑战,并在此基础上对其进行前瞻性研判。

三、算法的知识产权保护问题

(一) 算法在 AI 时代的重要性日益凸显

AI 算法持续突破计算机视觉、智能语音、自然语言处理等技术的商用门槛,实现大规模应用,从而为经济增长注入新动力。尤其在贸易领域,算法驱动的 AI 通过推动合规监管、消除语言障碍、优化信息匹配等途径有效降低贸易成本,进而扩大全球贸易(WTO, 2025)。例如,针对欧盟碳边境调整机制(CBAM)法案和合规的复杂性, AI 可协助企业高效地收集、管理和报告碳排放数据,降低合规成本与不确定性(Nexer, 2025)。此外,根据 WTO 预测,在 AI 与全球贸易深度协同的基础上,至 2040 年 AI 将推动全球实际贸易累计增长率上升 13.6 个百分点,以及全球实际 GDP 将提高 11 个百分点(WTO, 2024)。综上,算法在 AI 时代的重要性日益凸显,已成为推动技术创新与贸易增长的重要力量。

(二) 现有“贸易面向型”数字知识产权规则将算法纳入“源代码保护”条款

考虑到 AI 算法在数字贸易中的重要性,部分协定开始对“源代码保护”条款进行适应性调整,使“源代码非强制转让规则”的保护焦点逐步从源代码向算法延伸。当前,存在三种规则实践路径:其一,以 USMCA、CPTPP、《美日数字贸易协定》(UJDTA)为代表的“美式模板”,在源代码非强制转让条款中明确将“以源代码表达的算法”纳入适用范围,其中 USMCA 第 19.1 条将算法界定为“为解决问题或获得结果而采取的一系列明确步骤”,由此将算法与源代码一并纳入非强制转让保护客体。其二,《欧盟—日本经济伙伴关系协定》(EUJPEA)、《欧盟—英国贸易与合作协定》(EU-UK TCA)为代表的“欧式模板”,仅提及“软件源代码”,对“算法”保持沉默,算法能否获得与源代码同等保护,取决于对“软件源代码”外延的规则解释。其三,以《新加坡—澳大利亚数字经济协定》(SADEA)、《英国—新加坡数字经济协定》(UKSDEA)、《韩国—新加坡数字伙伴关系协定》(KSD-PA)等为代表的“新式模板”对“源代码非强制转让规则”的要求类似“美式模板”,但 SADEA 并不直接要求将算法纳入非强制转让条款,而是规定若一方在其他国际协定或其修正案中已承担算法非强制转让义务,则该义务延伸适用于另一方,从而实现对算法的间接保护。

(三) 现行“贸易面向型”数字知识产权规则制约算法的监管与保护

1. 算法延伸至“源代码非强制转让规则”制约对 AI 产品和服务的监督

第一,“算法黑箱”引致监管与问责困境。“源代码非强制转让规则”有助于降低算法被强制转让和披露的风险,但制约对 AI 相关产品与服务的有效监管,影响贸易秩序。一方面,基于深度学习的 AI 系统因决策逻辑隐匿于神经网络与海量参数中,构成“算法黑箱”,易内生算法偏见、歧视与数据安全风险。对跨境 AI 产品和服务进行系统性风险评估时,进口国监管机构需访问源代码、算法、权重参数等关键信息以解析底层逻辑(Jones, 2023)。然而,现行源代码保护条款赋予技术持

有者拒绝开放算法的权利，导致进口国无法有效审查，削弱了算法监管与问责机制。另一方面，应用程序接口（API）本身以源代码形式存在，是算法接收输入和查询并产生输出的通道，也是监管者对算法进行非侵入式审查的重要方式（Irion, 2022）。即使对“源代码”作狭义解释，也能合理将 API 包括在内，企业可主张 API 属于源代码范畴并拒绝开放。这进一步限制了各国监管 AI 相关产品和服务的空间（Jones et al., 2024），并可能加剧贸易摩擦。

第二，尽管现有“贸易面向型”源代码保护条款设有“例外条款”，试图为各国政府监管保留空间，但仍存在明显局限。首先，事后监管与事前合规之间存在制度张力。“美式模板”的“例外条款”严格规定源代码的获取必须是为了“特定调查、检查、审查、执法行动或司法程序”EU-UK TCA 修改为 EU-UK TCA，“欧式模板”相对宽松，允许监管机构基于在线安全法律提出要求（如 EU-UK TCA 第 207 条），但均仅限于逐案事后监管（Irion, 2022）。现代 AI 治理则逐渐强调事前合规，如欧盟《人工智能法案》要求高风险 AI 系统在上市前进行合规评估^①。然而，既有“例外条款”未预留 AI 事前合规检查空间，可能导致国内监管法规与源代码禁令冲突，增加贸易风险。其次，部分协定将例外扩展至“指定合格评定机构”（如 UKSDEA 第 8.61-K 条），但未明确定义。在各国政府日益依赖私营部门进行 AI 审计的背景下，第三方私人审计机构是否适用尚不明确（Jones et al., 2024）。最后，既有“例外条款”主要针对司法程序，忽略了跨境贸易中仲裁、调解、在线争议解决等非司法争议解决场景的信息披露需求，若例外条款不涵盖此类场景，将加剧贸易双方的信息不对称，阻碍贸易纠纷公平解决（Jones et al., 2024）。

2. 将算法视作版权、专利或商业秘密实施保护均面临困境

当前，将算法视作版权、专利或是商业秘密进行保护均面临不同问题。对于版权保护，TRIPS 强调版权保护的“思想与表达二分原则”，并要求“数据汇编或其他资料内容的选取或编排须构成智力创作”。AI 算法本质上是一系列数学运算、逻辑步骤，缺乏独创性的表达，加之其“智力创作”属性存疑，难以适用版权保护。若将算法视为专利进行保护，现有经贸协定中“关于专利的保护通常要求发明具有新颖性、包含创造性步骤且可供工业应用”（如 USMCA 第 20.36 条），但是 AI 算法尤其是一些基础算法更偏向于基本公式，因缺少“创造性步骤”，也难以申请专利保护。由于专利和版权保护的局限性，企业逐渐倾向于寻求商业秘密^②保护。然而，商业秘密保护虽具有无需注册、无限期不强制公开等优点，但易加剧算法的不可解释性，同时也易加剧数字鸿沟，不利于企业进行技术创新（许中缘等，2024）。此外，AI 算法易受到逆向工程、算法攻击或数据泄露等威胁（Igbinenikaro et al., 2024），在跨境流动中保密难度更大。既有协定规则仅提供事后救济，无法阻止秘密泄露，仅在泄密发生后赋予权利人提起诉讼的权利（Słok-Wódkowska et al., 2022），而跨境诉讼成本高、执行难，保护效果有限。

（四）“贸易面向型”数字知识产权规则将采取双重路径以保护算法

1. 细化升级“源代码非强制转让规则”的“例外条款”

为突破既有“源代码条款”对 AI 领域造成的监管困境，同时维护贸易便利化，“贸易面向型”源代码非强制转让规则应引入更广泛的监管例外。（1）在条款中明确“源代码”的定义，并澄清 API 不

^①欧盟《人工智能法案》（Artificial Intelligence Act）第 16 条（f）款规定：“高风险人工智能系统的提供者应确保高风险人工智能系统在投放市场或投入服务之前经过第 43 条所述的相关合格性评估程序。”

^②《中华人民共和国反不正当竞争法》第十条规定：商业秘密是指“不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息”。

适用该规则。(2)“指定合格评定机构”的相关安排不明晰,给人工智能相关产品和服务的监管带来极大挑战。对此,欧盟的域内实践可为破解该困境提供有益借鉴。具体而言,欧盟《人工智能法案》第 31 条从质量管理、资源、网络安全等方面,详细规定了“合格评定机构”的相关要求^①。因此,可参考该法案,在“例外条款”中进一步细化并明确“指定合格评定机构”必须满足的具体要求,以减少贸易不确定性并降低贸易壁垒。(3)明确“源代码条款”允许政府引入要求披露 AI 和算法系统信息的措施,以保护贸易中私人个体(企业、工人和消费者)或其代表在问责场景下的合法权益(Jones et al., 2024)。

2. 确立“技术应用导向”的算法专利保护标准

鉴于当前算法在保护范畴上存在模糊地带,实践中可借鉴《欧洲专利局审查指南》(以下简称《审查指南》)的做法对算法以专利进行保护。《审查指南》最新版本对“数学方法”一节进行扩展,并增设了聚焦“人工智能与机器学习”的专门小节(G-II第 3.3.1 节)。该部分强调仅依靠输入数据的限定并不能必然认定数学方法具备技术贡献,关键在于数学方法所达成的结果是否与实际技术效果之间存在直接关联(邵永乐, 2025)。例如,将人工神经网络应用于心电监测设备中以识别心律失常模式,被视为具备技术贡献,符合专利授权条件。对抽象数据记录或“电信网络数据记录”进行分类却未阐明分类结果的具体技术用途,则难以获得专利授权。考虑到算法本质上具备抽象数学特征,上述关于数学方法的指导原则同样适用,若算法能够转化为特定技术领域的实际应用,或针对具体技术问题提出解决方案,则可取得专利授权。因此,基于“技术应用导向”,能解决某一具体技术问题并获得技术效果的 AI 算法可被视作一种专利客体,获得专利保护,为跨境算法技术转让、许可贸易提供更清晰的法律框架,促进 AI 技术在国际贸易中的有序流动。

四、AI 大模型训练数据的侵权责任界定问题

(一) AI 大模型训练复制冲击“贸易面向型”数字内容版权规则

人工智能大模型的迅猛发展,建立在对数万亿级词元(Token)的深度学习之上。从技术原理来看,生成式 AI 大模型的训练必须通过对海量文本、图像、音视频等内容进行批量跨境抓取、复制、缓存和持续性存储,再对这些数据进行清洗、标注与算法分析,其中不可避免地包含大量受版权保护的作品。在“贸易面向型”数字内容版权规则框架下, AI 大模型训练数据的复制行为可能直接落入“复制权”的规则范畴。例如,根据 USMCA 第 20.57 条和 CPTPP 第 18.58 条规定,复制权涵盖“以任何方式或形式,包括电子形式”,对作品的全部复制行为。原则上, AI 大模型训练的复制行为很可能构成对作品的“复制”,若未取得权利人许可,形式上即存在侵权风险。然而,在实践层面,要求 AI 开发者对训练所涉的数亿级乃至百亿级作品逐一获取授权,在贸易成本、谈判周期和权利信息等约束下几乎不可能实现。另外,既有的“贸易面向型”数字知识产权规则最初主要着眼于作品在线传播、数字商品贸易和跨境执法协作,对以文本与数据挖掘(TDM)为核心的机器学习训练场景并未作出专门安排,也缺乏统一的例外或限制条款,导致 AI 企业在不同贸易伙伴国面临不同的法律风险,进而增加贸易不确定性,削弱企业在国际市场的竞争力。

^① European Parliament and Council. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [EB/OL]. (2024-07-12) [2026-02-10]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>.

(二) 嵌入“TDM 例外条款”缓解训练数据使用冲突

鉴于 AI 训练数据涉及大量文本、数据及图像，有必要在“贸易面向型”数字内容版权规则中设置“TDM 例外条款”。当前，全球在国内法层面对 TDM 的规制路径高度分化。欧盟《数字单一市场版权指令》(DSMD)第3条，允许科研机构和文化遗产机构在合法获取受版权保护材料的情况下进行 TDM；第4条允许对合法获取的作品或数据的任何复制和提取，并为著作权人设置了“选择—退出”权利。日本《著作权法》确立了较为宽泛的“非享受使用”TDM 例外，允许作品用于技术测试、数据分析和计算机数据处理等目的，前提是不得对版权所有者的利益造成不当损害，但这种宽泛例外可能挑战《伯尔尼公约》和 TRIPS 等国际协议的“三步测试”(Thongmeensuk, 2024)。英国在《版权、设计及专利法》中仅对非商业研究型 TDM 作出有限豁免，且只豁免了该技术过程中不可避免的复制行为，对于汇编、翻译等行为未作规定(Thongmeensuk, 2024)。美国则主要依赖著作权合理使用原则的四要素判断，但针对生成式 AI 的新一轮诉讼尚未形成稳定判例，主要基于是否构成转换性使用进行个案认定。

相比之下，欧盟 DSMD 第3条和第4条的规定，既支持科学研究又保持谨慎立场，为 AI 训练提供了合法性基础。欧盟《人工智能法案》进一步要求生成式 AI 模型的提供者应编制并披露一份关于受版权法保护训练数据使用情况的“足够详细”的摘要，该条款有助于提升透明度并缓解侵权担忧。因此，可以基于欧盟实践将 TDM 例外分为两类。第一类针对非商业用途，应强制实施，防止被合同排除或限制。第二类聚焦商业用途，包含两个关键条件：首先，生成式 AI 模型提供商应披露涉及受版权保护的训练数据使用摘要；其次，在训练 AI 时应赋予版权所有者“选择—退出”权利。

五、AI 生成物的知识产权保护问题

(一) AI 生成物相关“贸易面向型”数字内容版权规则真空会加剧保护不确定性

1. AI 生成内容的作品性认定存在碎片化问题

既有经贸规则均以“人类中心主义”为前提，强调作品必须体现自然人的独创性和智力劳动，而这一前提难以扩展到 AI 生成作品(Salle et al., 2025)。协定中通常只规定缔约方应给予保护的“最低标准”或“国民待遇”，以构建传统作品的跨境保护框架，但对于“AI 生成作品是否应受保护”未作规定，往往留给各国国内法自行裁量(Mercurio et al., 2021)。如 DEPA 第8.2条虽然规定“应促进采用支持可信、安全和负责任使用人工智能技术的道德和治理框架(人工智能治理框架)”，但未设定 AI 知识产权保护的实质性义务。具体而言，人工智能生成内容(AIGC)通常是基于概率模型的统计输出，这种输出是否等同于“创造性”，现有“贸易面向型”数字内容版权规则均无准确定论。规则空白导致各国在 AIGC 作品性认定上主要依赖国内法中“人类作者”与“独创性”要件解释，进而导致认定碎片化，即对于同一份 AI 生成内容，可能在认可“计算机生成作品”保护的国家(如英国)被视为作品，而在坚持“人类中心主义”的经济体(如美国、欧盟)则认为不构成作品。这种现状虽保留了制度创新空间，但增加了数字贸易的信息不对称成本，也为未来经贸争端埋下隐患。

2. AI 生成作品的权利归属者与责任承担者高度不确定

根据 TRIPS 第10条第1款规定，“计算机程序”无论是源代码还是目标代码，应作为《伯尔尼公约》下的文字作品加以保护。然而，《伯尔尼公约》规定只有自然人才能被认定为作者。AI 因不具备法律拟制的独立人格和自由意志，因此被排除在权利主体之外，这引发了关于谁拥有 AI 生成内容

权利归属争议的根本性问题。AIGC 生成过程由人类通过提示词输入、参数调整等方式引导,算法则完成从数据处理到内容生成的主要工作,此种协同机制使创作行为呈现复合性特征。算法设计者、数据提供者、投资者和使用者等,均以不同方式为 AIGC 运行提供技术与资源支撑,难以单纯以某一主体作为唯一的创作主体(孙正樑,2019)。另外,一旦涉及侵权责任,各主体又往往互相推诿,将“谁贡献更大”的争夺转化为“谁影响最小”的辩解(吴汉东等,2024)。依据权责统一原则,生成内容的实际控制者原则上应承担相应侵权责任,但前提是必须先明确各主体间权利配置与风险分担(吴汉东等,2024)。然而,既有“贸易面向型”数字内容版权规则对 AIGC 的权利归属与责任归属难题缺乏回应,导致国际贸易中相关主体的权益状态与侵权追责具有不确定性,从而抑制企业对 AI 的跨境投资决策并扭曲投资激励。

3. AI 生成内容的保护路径模糊

“贸易面向型”数字内容版权规则可通过赋予创作者对其作品的专有权来激励创新并促进技术扩散(如 USMCA 第 20.57 条)。然而, AI 生成作品的保护面临两难困境:若保护不足,企业的研发投入将面临严重“搭便车”问题,难以确保其预期收益,从而降低对 AI 技术的投资意愿、减少技术人员的跨境流动及新应用开发;若赋予其与人类创作作品同等保护,则可能形成新型技术贸易壁垒,使掌握底层大模型的跨国巨头垄断基础 AI 技术,限制后发竞争者获取关键技术,进而阻碍数字贸易中的协作创新(Salle et al., 2025)。此时,区分“纯 AI 生成”与“人机协作”显得尤为重要,因为即使 AI 系统本身不能被认定为可受版权保护作品的“作者”,人类在参与和引导系统开发及使用过程中的干预程度,仍可影响生成作品的可版权性。若存在足够的人类创造性和决策参与,真正的人机协作作品应获版权保护(Crouch, 2024)。然而,“贸易面向型”数字内容版权规则在应对 AI 生成内容可版权性时存在规则空白,从而加大全球数字鸿沟,削弱发展中国家通过数字贸易实现技术追赶的能力。

(二)采用“分层模式”保护 AI 生成内容

目前,“贸易面向型”数字内容版权保护规则在 AIGC 的保护上存在空白,国内立法和司法实践可为规则提供一定参考。英国 1988 年《版权、设计和专利法》第 9 条将“计算机生成的文学、戏剧、音乐或艺术作品”纳入版权客体,其版权归属于“为作品创作进行必要安排的主体”,但标准过于宽松。美国坚持严格“人类中心主义”原则,2023 年美国版权局发布的《版权注册指南:包含人工智能生成材料的作品》规定作者必须是人类,并要求申请版权登记的作品应包含人类创造性投入或干预,且必须披露 AI 生成内容。在《黎明的扎利亚》案^①中,美国版权局撤销了漫画书中 AI 生成图像的版权,但保留了人类编写的文字和对图片的排版布局的版权。可见,在美国仅保护有人类创造性投入或干预的作品,纯 AI 内容被拒绝版权保护,只能流入公有领域。日本亦遵循“人类中心主义”,并认为 AIGC 需满足“人类智力投入实质性贡献”标准。在此基础上,日本对 AIGC 的版权性基于以下因素逐案确定,包括用户的指令和输入提示的数量和内容、生成尝试的次数、从多个输出材料中进行的选择,以及后续人类添加和更正(张宪,2025)。基于以上实践,对 AIGC 不宜采取“全有”或“全无”的整体认定,而应按照人类干预程度建立“分层模式”规则。相比而言,日本模式更具灵活性,“贸易面向型”数字内容版权保护规则可借鉴其个案判定中的四类因素,完善规则内容,提升 AI 治理能力。

^① 《黎明的扎利亚》(Zarya of the Dawn)案确立了美国版权局对于“生成式 AI 辅助创作”作品审查的执法标准,对处理 AI 生成内容的版权纠纷具有深远影响。

六、AI对数字知识产权执法带来的挑战

(一) AI的使用导致“贸易面向型”数字知识产权执法规则效力不足

1. AI通用化规避削弱TPM执法效力

从规则层面看,技术保护措施(TPM)反规避义务具有技术中立性。CPTPP第18.68条、USMCA第20.66条等将“为规避之目的而制造、进口、分发、销售、出租装置、产品或组件,或者提供相关服务”的主体纳入TPM规制对象,并在行为具备商业利益目的且存在故意的情形下设定相应刑事责任。但这些规则主要以破解软件、硬件解码器等专门规避工具为预设对象,未预见大模型、智能爬虫、自动脚本等通用AI系统绕过TPM的情形。一方面,训练数据导向的AI爬虫可通过识别验证码、模拟人机交互、规避IP限流等方式,批量抓取受访问控制保护的内容,形成对TPM的功能性规避。另一方面,通用大模型及其API具有广泛合法和非规避用途,难以满足“主要设计目的为规避”“缺乏重要商业用途”等要件,不易被归类为“规避专用工具”或“以规避为主要目的的服务”,较难触发TPM条款预设的责任构成标准。此外,经贸协定通常要求相关技术措施“有效控制访问或使用”,而AI爬虫规避的弱口令、简单脚本等“软性门槛”,是否构成“有效技术措施”存在争议。总体而言,现行TPM规则在面对基于通用AI的自动化规避时,执法效力不足,暴露了现有经贸协定框架在AI时代的适用真空。这会瓦解跨境数字交易的安全信任基石,更因全球性盗版泛滥而严重扭曲数字产品的国际价值链。

2. AI系统性去除RMI导致溯源失效

在经贸协定中,权利管理信息(RMI)被视为对TPM的关键补充,通过保护作品上的权利标识信息,降低数字环境中“去标签化”“难溯源”风险。然而,AI自动处理内容时普遍剥离嵌入式版权元数据并滤除水印,造成RMI大规模削减,但将这些行为纳入“违法去除RMI”需满足两个要件:一是RMI须能“识别作品、作者或权利状态的信息”;二是行为人主观上“明知或有合理理由知道该行为将促成或掩盖侵权”(如USMCA第20.67条)。在AI场景下,上述两个要件的适用均面临挑战。一方面,AI往往“默认剥离全部外显或隐性元数据”,系出于节省存储、统一格式或隐私合规等目的进行“无差别清洗”,而非针对特定作品有选择地抹去RMI,难以在规则层面认定其主观上“意图促成侵权”。另一方面,现有协定未针对“算法性、系统性去除RMI”建立特殊推定规则或举证便利,权利人难以在跨境纠纷中证明某一AI服务提供者“明知其RMI去除行为将大规模促成侵权”。因此,AI环境下RMI条款执法效果大打折扣,数字产品来源难以追溯,导致全球数字市场出现“柠檬市场”效应,高质量、合规的原创内容无法自证,不得不与来源不明、可能是AI洗稿生成的低价内容竞争,削弱企业核心竞争优势。

(二) 纳入“元数据标识”加强规则执法效力

针对AI环境下TPM和RMI效力不足的问题,可考虑在“贸易面向型”数字知识产权执法规则中纳入“元数据标识”。当前,内容来源和真实性联盟(C2PA)建立的“内容凭证”,利用公钥密码学将可验证元数据(如AI生成标识)加密嵌入媒体文件,以实现数字内容追溯,已获OpenAI、谷歌、尼康等公司的广泛支持并被采用。另外,中国2025年颁布的《人工智能生成合成内容标识办法》确立了“显式+隐式”双标识体系。基于上述实践,可从两方面完善“贸易面向型”数字知识产权执法规则:一是将包含符合技术标准的元数据标识系统纳入有效技术措施;二是将“故意避开或破坏技术

措施”的适用范围扩展至系统性破坏元数据完整性的行为。

七、结 论

本文基于既有“贸易面向型”数字知识产权规则，剖析算法的知识产权保护、AI 大模型训练数据的侵权责任界定、AI 生成物的知识产权保护、AI 对数字知识产权执法的挑战等问题。研究发现：“贸易面向型”数字知识产权规则制约算法的监管与保护；AI 大模型训练阶段大规模复制受版权保护作品冲击“复制权”规则；AIGC 相关“贸易面向型”数字内容版权规则存在真空；AI 的使用导致“贸易面向型”数字知识产权执法规则效力不足。对此，本文认为未来“贸易面向型”数字知识产权治理将会呈现细化升级“源代码非强制转让规则”的“例外条款”、确立“技术应用导向”的算法专利标准、嵌入“TDM 例外条款”、采用“分层模式”保护 AIGC 及纳入“元数据标识”趋向。

作为全球数字贸易大国，中国应当主动参与“贸易面向型”数字知识产权规则的塑造。在国际层面，中国可考虑在 RCEP 中倡导构建符合 AI 训练特点的 TDM 例外制度。对于科研、教育等非商业场景，可适度明确例外适用边界；对于商业训练场景，则可探索建立训练数据使用摘要披露、权利人退出、合理补偿等制度安排。另外，对于正在申请加入的 DEPA，中国可主动参与推动细化“源代码非强制转让规则”的例外条款，为 AI 事前合规评估、监管审查、非司法争议解决等保留空间，提升中国在全球数字经贸规则制定中的话语权。在国内层面，可借鉴欧盟实践与中国现有《审查指南》，进一步细化算法专利保护标准，发布更多典型案例，明确不同类型 AI 算法在具体技术场景中的技术贡献判定标准，为企业专利申请提供清晰指引。在 AIGC 保护方面，中国可在既有司法实践基础上，进一步明确“人类智力投入实质性贡献”标准，并围绕提示词设计、结果筛选、后期编辑等关键因素形成更具操作性的裁判规则，为“贸易面向型”数字知识产权规则贡献中国方案。此外，可在《中华人民共和国著作权法》中将符合国家标准的元数据标识系统纳入有效技术措施，将系统性破坏元数据完整性行为纳入“故意避开或破坏技术措施”范畴。

参考文献

- [1] 蒋洁如，林鹤．生成式人工智能语料训练的知识产权监管制度：域外经验及其启示[J]．现代情报，2025，45（6）：102-111.
- [2] 李春晖．人工智能训练侵犯作品复制权吗？[J]．华东政法大学学报，2025，28（4）：46-66.
- [3] 刘一帆．生成式人工智能数据训练行为的著作权困境与出路[J]．江海学刊，2025（4）：182-189+256.
- [4] 邵永乐．欧盟人工智能大模型的知识产权保护路径及中国方案[J]．德国研究，2025，40（5）：101-123+149-150.
- [5] 宋河发，李竿影．人工智能生成物知识产权保护制度体系构建——基于激励创新与权益平衡视角[J]．科学学研究，2026，44（3）：482-490.
- [6] 孙正樑．人工智能生成内容的著作权问题探析[J]．清华法学，2019，13（6）：190-204.
- [7] 吴汉东，刘鑫．生成式人工智能的知识产权法律因应与制度创新[J]．科技与法律（中英文），2024（1）：1-10.
- [8] 徐家力．人工智能生成物的著作权归属[J]．暨南学报（哲学社会科学版），2023，45（4）：37-49.
- [9] 许中缘，郑煌杰．生成式人工智能算法专利保护的理据与进路[J]．贵州师范大学学报（社会科学版），2024（1）：135-147.
- [10] 姚志伟．人工智能生成物著作权侵权的认定及其防范——以全球首例生成式 AI 服务侵权判决为中心[J]．地方立法研究，2024，9（3）：1-17.

- [11] 张惠彬, 王怀宾. 人工智能“发明人”资格认定的国际比较与启示[J]. 国际经济法学刊, 2024(2): 65-78.
- [12] 张伟君. 论大模型训练中使用数据的著作权规制路径[J]. 东方法学, 2025(2): 79-92.
- [13] 张宪. 人工智能生成内容可版权性的认定方法研究[J]. 法学评论, 2025, 43(4): 146-160.
- [14] 张笑尘. 人工智能生成物的可版权性问题——日本经验与中国镜鉴[J]. 现代日本经济, 2025, 44(1): 81-94.
- [15] 周念利, 李玉昊. RTAs 框架下数字知识产权规则的数字贸易效应测度及异质性分析[J]. 国际经贸探索, 2021, 37(5): 35-50.
- [16] 周念利, 李玉昊. 数字知识产权保护问题上中美的矛盾分歧、升级趋向及应对策略[J]. 理论学刊, 2019(4): 58-66.
- [17] 周念利, 廖宁, 黄宁. “贸易面向型”数字技术规则的发展演进研究——基于“美式模板”及“新式模板”对比的视角[J]. 亚太经济, 2024(2): 28-39.
- [18] 周念利, 王达, 吴希贤. RTAs 框架下的数字知识产权规则能否促进数字内容贸易? [J]. 世界经济研究, 2023(10): 30-43+103+135-136.
- [19] CROUCH D. Using intellectual property to regulate artificial intelligence[J]. Missouri Law Review, 2024, 89(3): 781-845.
- [20] HE Y X, YAN R J. The differentiation and coordination pathways of intellectual property enforcement provisions in regional trade agreements: a comparative study based on CPTPP, USMCA, and RCEP[J]. Science of Law Journal, 2025, 4(1): 67-76.
- [21] IGBINENIKARO E, ADEWUSI A O. Navigating the legal complexities of artificial intelligence in global trade agreements[J]. International Journal of Applied Research in Social Sciences, 2024, 6(4): 488-505.
- [22] IRION K. Algorithms off-limits? If digital trade law restricts access to source code of software then accountability will suffer[C]//Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency. New York: ACM, 2022: 1561-1570.
- [23] JONES E, COLLINS P, GROSSE RUSE-KHAN H, et al. AI governance and the future of digital trade policy: options for the UK [R]. Oxford: University of Oxford Blavatnik School of Government, 2024.
- [24] JONES E. Digital disruption: artificial intelligence and international trade policy[J]. Oxford Review of Economic Policy, 2023, 39(1): 70-84.
- [25] MERCURIO B, YU R. Convergence, complexity and uncertainty: artificial intelligence and intellectual property protection[M]//PENG S-Y, LIN C-F, STREINZ T. Artificial intelligence and international economic law: disruption, regulation, and reconfiguration. Cambridge: Cambridge University Press, 2021: 139-154.
- [26] NEXER. Nexer and Stibo Systems launch AI solution for CBAM management[EB/OL]. (2025-02-12) [2025-12-21]. <https://www.mynewsdesk.com/nexer/pressreleases/nexer-and-stibo-systems-launch-ai-solution-for-cbam-management-3368270/>.
- [27] SALLE S, RINI W S D. Development of artificial intelligence regulations and implications for intellectual property rights protection[J]. Contemporary Issues on Indonesian Social Justice and Legal Reform, 2025, 1(1): 58-77.
- [28] SŁOK-WÓDKOWSKA M, MAZUR J. Secrecy by default: How regional trade agreements reshape protection of source code[J]. Journal of International Economic Law, 2022, 25(1): 91-109.
- [29] THONGMEENSUK S. Rethinking copyright exceptions in the era of generative AI: balancing innovation and intellectual property protection[J]. Journal of World Intellectual Property, 2024, 27(2): 278-295.
- [30] World Trade Organization. Trading with intelligence: How AI shapes and is shaped by international trade[R]. Geneva: WTO, 2024.
- [31] World Trade Organization. World trade report 2025: making trade and AI work together to the benefit of all[R]. Geneva: WTO, 2025.

Challenges and Prospects of Artificial Intelligence for “Trade-oriented” Digital Intellectual Property Rules

ZHOU Nianli LUO Yu

(University of International Business and Economics)

Abstract: As a pivotal technology of the Fourth Industrial Revolution, artificial intelligence (AI) has deeply integrated into cross-border trade while simultaneously posing severe challenges to “trade-oriented” digital intellectual property (IP) rules. Based on existing “trade-oriented” digital IP rules, this paper provides an in-depth analysis of issues, including the IP protection of algorithms, the definition of infringement liability regarding training data for large AI models, the IP protection of AI-generated content, and the challenges AI poses to digital IP enforcement. The study finds that “trade-oriented” digital IP rules constrain the regulation and protection of algorithms; the large-scale reproduction of copyrighted works during the training phase of large AI models undermines the established right of reproduction regime; there exists a regulatory vacuum in “trade-oriented” digital content copyright rules concerning AI-generated content; and the application of AI has led to the inadequacy of enforcement rules governing “trade-oriented” digital IP rights. Looking ahead, “trade-oriented” digital IP rules are expected to evolve in four main directions: the adoption of dual pathways for algorithm protection, the embedding of “text and data mining exception clauses,” the implementation of a “layered model,” and the integration of “metadata-based identification systems.” In response, as a major digital trading country, China should proactively engage in the formulation of “trade-oriented” digital IP rules.

Keywords: artificial intelligence; regional trade agreements; digital intellectual property rules; algorithms

JEL Classification: F13, O33, O34

(责任编辑: 李秀婷 王 建)