人工智能时代网络空间的本体重构与治理转型

蔡翠红

【内容提要】随着大模型与生成式人工智能的广泛应用，全球网络空间正经历深层次结构性转型。网络空间不再是仅以人类为主体的信息交互环境，而是日益演变为由人类与人工智能共同参与、由算法驱动并持续生成行动的“全球智能行动域”。这一转型从存在性、时间性与权力性三个层面重构网络空间的本体结构：行动由外部输入转为系统内生，时间由可回溯事件序列转为持续演化过程，权力由入口控制转为嵌入模型与技术生态的生成机制。这些变化使以主体可识别、行为可归责、规则可预期为前提的全球网络空间治理体系面临系统性挑战，在管辖权适用、规则供给与治理执行等方面遭受结构性冲击。生成式治理强调治理应从事后规制转向事前塑形，从规制已经发生的行为转向引导行动生成机制，并重构多节点参与、协同生成的治理结构。生成式治理为理解和推动人工智能时代网络空间治理转型提供了新视角。

【关键词】人工智能　网络空间治理　生成式治理　智能行动域

近年来，全球网络空间治理呈现整体平稳但局部失序状态。深度伪造技术模糊了真实与虚假的界限，自主智能体的跨国行动时常产生非预期后果，由人工智能模型自动生成的恶意行为愈发难以防范，而生成式技术的广泛应用则对舆论生态与社会信任构成严峻挑战。[1] 这些现象均呈现出跨域性、非主体性与不可归责性。行动链条天然跨越地理疆界，关键环节缺乏明确的人类主导者，导致责任在模型、算力、数据与平台之间呈现断裂与漂移状态，致使既有治理体系陷入系统性不适，难以形成有效回应。究其根源，并非某项技术本身具有特殊危险性，而在于人工智能正在深层重构网络空间本体结构。[2]

自互联网诞生以来，全球网络空间长期被视为一个以人类主体为中心的“信息交互空间”，其治理体系建立在主体可识别、行为可归责、规则可预期等基础预设之上。然而，随着大模型、智能代理与自治系统的普及，网络空间已从被动的信息流通环境逐渐转变成由人类与人工智能共同构成、由算法驱动并持续生成行动的“全球智能行动域”。当下治理困境的本质，正是治理范式与网络空间运行方式之间出现了本体性断裂。

人工智能时代网络空间的本体改变

人工智能深度嵌入网络空间，推动其从以人类信息交互为核心的“信息交互空间”转向人机共同参与的“全球智能行动域”。“全球智能行动域”是由人类、人工智能系统、自主代理与基础设施共同构成的动态行动生成结构。[3] 在此结构中，行动具备生成性、扩散性与演化性，系统状态实时流变，难以被静态记录或回溯预测，权力关系深嵌于模型架构、接口标准与生态机制之中。网络空间从信息传递的被动通道，逐步转变为行动自主生成与衍生的土壤。人工智能时代网络空间的本体转变可从存在性、时间性与权力性三个维度加以解析，分别对应行动的内生来源、行动链条的非线性演化与行动环境的权力嵌入式分布。

一、存在性重构：从信息承载空间到行动自主生成空间

在传统互联网范式中，网络空间的存在性被理解为一种“管道式结构”，其功能是在主体之间传递信息、指令、内容或执行有明确定义的操作。网络本身并不产生

中国知网　https://www.cnki.net

（中新社供图）

2025年11月7日，2025年世界互联网大会乌镇峰会在浙江省桐乡市乌镇开幕。图为全球移动通信系统协会首席执行官洪曜庄（John Hoffman）在开幕式上发言。

行动，它只是行动的载体。然而，随着人工智能模型与自主演化代理深度嵌入网络层、平台层与应用层，它们在网络空间中执行决策、生成内容并塑造交互关系，从而成为新型的网络空间施动者。网络空间因此从以人为中心的领域，转变为人机共生的复杂生态，其本体边界被重新定义。

这种存在性重构最突出的表现是行动生成的自主化。大语言模型能在无人提示的情况下生成内容、代码、策略，甚至构建和执行完整的操作序列。自主智能体可以依据目标设定、环境反馈与状态变化持续调整自身行为。这些行动不再是外部指令的机械执行，而是呈现出明显的涌现特性，其来源难以完全追溯到特定的主体或意图。与此同时，人工智能所产生的行动往往具备跨系统传播的能力，可以从一个模型触发另一个平台的决策，继而影响舆论传播、供应链调度或安全预警机制，最终形成多层级、多节点、多后果的复杂行动链。

在这一结构中，行动的主体性显著弱化。行动不再能够归因于某个独立的个体或组织，而是在数据分布、模型参数、算力调度与系统交互模式等多重因素叠加作用下形成。换言之，行动成为一种“系统产物”而非“主体产物”。网络空间的存在性因而从“可归属”转向“可生成”，从被动承载转向主动催生，成为行动发生的内在环境。这种转变意味着网络空间不再是行为的外部舞台，而是行动自身的重要来源。

二、时间性重构：从可回溯事件序列到持续演化的行动流

传统治理体系基于一个基本的时间预设，即系统状态可被记录、冻结和回溯，行为具有明确的发生时点，其后果可在事后追溯、审查与判定。因此，法律体系多倚重事后追责，治理节奏建立在行为事件可定位的基础上。

然而，智能行动域中的时间结构发生根本性转变。

中国知网 https://www.cnki.net

借助持续微调、在线学习、检索增强与自动参数更新，人工智能系统始终处于动态演化状态。同一模型会因新数据输入、交互差异或算法自我调整而不断变化，从而在功能层面呈现“多时态主体性”，即模型在不同时刻已不再是同一行为体。[4] 与此同时，智能行动链以毫秒级速度运行，跨越多个服务商、平台节点与基础设施层级，使行为发生时间趋于流动而非固定，因果关系呈多重交织的复杂结构。

更具挑战的是，智能行动域中的状态变化具有不可逆性。许多由人工智能引发的后果难以复原，例如极端内容的扩散、模型内部参数的改变、算法排序逻辑的偏移，以及市场预期的扭曲等。即便技术上能够回退至某一模型版本，其引发的社会反应、舆论变动或经济行为也无法逆转。网络空间因此从一个“可冻结、可追溯”的存档系统，转变为持续流动、不断重构的“时间性流变体”，其本质不再是静态结果的集合，而是连续过程的展开。在这种时间结构下，治理对象不再局限于稳定的行为事件，而是延伸至不断生成中的行动过程。

三、权力性重构：从守门式控制到嵌入式生态权

在传统互联网秩序中，权力的核心体现在对“入口”的控制上，例如数据跨境关口、信息流接口分配、平台规则制定以及网络接入点管理等准入标准、授权与审核。国家、平台与各类组织围绕此类控制权展开博弈。在这种格局下，权力主要表现为“守门人权力”。[5]

然而，在智能行动域中，权力结构发生三重深刻变迁。首先，权力重心从数据“入口”上移至模型层面。模型架构、训练语料、对齐机制与系统接口共同塑造人工智能的行动逻辑与行为倾向，进而决定整个行动域中哪些行动能够生成、可见并被认可。可以说，掌握模型即掌握网络空间智能主体行动逻辑的定义权。其次，权力逐渐以“生态权”的形式被企业、平台与技术社群共同掌握。“生态权”涵盖应用程序编程接口（API）的开放或封闭、模型间互操作性的界定、数据集与训练流程的控制、代理部署规则的设定，以及监测与透明度机制的决策等。相较于传统的“守门权”，“生态权”是一种更深层的权力形态，它能够确定行动域的基本规则、边界范围、结构特征及未来演变方向。能够定义生态便意味着能够界定系统中可能出现的行动范畴。最后，智能行动域中的权力结构呈分布式、碎片化趋势。算力提供者、平台运营方、模型开发者、开源技术社区以及国家监管机构等分别掌握部分关键节点，整体权力分布呈现网络化格局，难以由任意单一主体全面掌控。这种结构导致国家、政府等法定治理者与平台企业、模型开发者、技术社群等事实治理者之间出现明显错位。因此，智能行动域中的权力不再体现为对信息“入口”的控制，而是转向对生成机制与生态结构的嵌入式塑造。

2025年10月25日，《联合国打击网络犯罪公约》开放签署仪式暨高级别会议在越南河内国家会议中心举行，60多个联合国成员国签署了这一公约。

智能行动域对全球网络空间治理的结构性冲击

人工智能引发的网络空间本体变革，直接冲击以行为可定位、可追溯、可预测为基本预设的全球网络空间治理体系。当网络空间演化为智能行动域，这些预设被逐一瓦解，并在管辖权、规则供给与治理行动效能三个维度形成结构性张力。

一、存在性转变、行动链条与管辖权适用

在管辖权分配上，全球网络空间治理长期依赖行为发生地、服务提供地和受害结果地等相对可辨识的要素。各国通过刑法的域外适用、网络犯罪公约中的合作条款，并结合域名 /IP 的地理信息与服务器位置，构建起一套针对跨国网络行为的执法分工体系。在以“信息交互空间”为特征的阶段，这套体系虽不完美但基本可行，因

中国知网 https://www.cnki.net

为大多数行为最终可追溯至明确的人类主体，关键基础设施节点也具有较为清晰的属地归属。[6]

然而，智能行动域的出现彻底打破了这种责任可追溯性的成立前提。人工智能驱动的网络行为具有高度的生成性与链条化特征。例如，一个位于甲国云平台的模型被调用，利用乙国的数据，通过丙国的代理，向丁国用户发起自动化钓鱼攻击，最终在戊国的交易所触发异常交易。整个行动链条穿越多个技术平台与司法辖区，其中关键环节由智能体生成。这使行为发生地不再是单一的地理坐标，而是一条持续流变的技术路径；行为主体也不再是特定的自然人或法人，而是由人类与非人组件共同构成的混合生成机制。

在此情形下，传统的管辖权原则面临严峻挑战。若依照属地管辖可能难以锁定稳定的连接点，依照属人管辖又无法在高度分散的责任链中识别关键主体，而保护性管辖与普遍管辖则常因各国主张重叠而引发冲突。这可能导致多国针对同一网络事件同时主张管辖权的“执法叠加”，或大量由人工智能生成的攻击、扩散事件陷入“无人管辖”的真空地带，没有国家愿意或能够承担全部责任。全球网络空间治理在最根本的权责分配问题上陷入结构性困境。更为关键的是，这一困境源于网络空间本体的深刻变化，无法通过签署合作备忘录或调整法律条文得到根本解决。当网络空间从被动的信息通道转变为行动自主生成的来源时，行为、主体与空间之间原有的线性对应关系便开始瓦解。管辖权赖以建立的坐标系本身已经动摇，管辖权的失灵由此构成智能行动域对全球网络空间治理体系的第一重结构性冲击。

二、时间性转变、行为迭代与规则供给

传统的全球网络空间治理规则体系主要依赖三类机制：一是在联合国等国际组织中达成的宣言与相关文件，如关于负责任国家行为规范的共识；二是区域层面的网络犯罪条约、数据保护规则及跨境执法安排；三是技术社群与平台自主制定的技术协议、社区准则与自律规范。上述机制共同构成现有规则基础，其背后隐含一个共同前提，即网络行为模式在可预见的时间内保持相对稳定。在此背景下，即使规则制定滞后，总体上也能对行为构成约束。[7]

然而，智能行动域带来的时间性重构使这一关键前提难以维系。人工智能系统通过持续微调、在线学习、人类反馈和用户交互不断调整其输出模式，攻击手段在开源社区中高频迭代，平台内部的推荐与过滤算法也随实时数据流持续优化。[8] 行为模式因此呈现出持续演化、随技术迭代而连续更新的特征。针对上一代攻击方式或虚假信息传播模式制定的治理规则，在其正式生效时往往已落后于现实发展。

这一问题在平台治理与内容规范领域尤为突出。随着生成式人工智能模型大规模进入内容生产环节，虚假账号、深度伪造、合成舆论与自动评论等现象可在极短时间内形成规模效应。当各国监管机构与平台企业试图围绕“合成内容标识”“算法透明度”或“自动生成内容责任认定”等议题制定规则时，其不仅难以跟上行为模式的演变速度，甚至常常难以对规范对象本身作出清晰界定。比如是应针对深度伪造，还是应涵盖更广泛的人工智能生成内容？是要求公开模型基本信息，还是必须追溯其训练数据来源？在模型能力与行为模式尚未定型的背景下，规则制定失去稳定的参照依据。

因此，规则供给的困境不仅体现在形式上规则滞

中国知网 https://www.cnki.net

后，更表现为内容上规则失焦。无论是政府间谈判还是多利益相关方论坛，都难以在高度动态、可重构的行为谱系中找到可持续的规范对象。规则体系极易陷入危机出现—被动响应—再次滞后的恶性循环，使全球网络空间治理在规则供给层面面临疲于追赶的结构性困境。

三、权力性转变、行为节点与治理执行

第三重冲击体现在治理的执行层面，对治理规范由谁执行、如何执行以及能否有效等根本性问题的回答变得愈发困难。在“信息交互空间”时代，尽管平台与技术社群已具备显著影响力，但国家仍能通过行政许可、内容审查、访问封锁、经济处罚等手段对关键网络行为施加实质性管控，整体治理结构呈现出国际规则—国家主权—平台执行这一层级传导形态。[9]

智能行动域带来的权力性重构彻底改变了这一格局。决定行为生成方式的关键节点，已从传统的接入控制转向模型与生态定义。大模型提供者通过训练数据选择、模型架构设计、对齐策略与接口规范设定行为边界与倾向。开源社区通过主流模型与框架的推广，影响攻击工具和防御机制的普及面，也影响隐私保护与合规实践。[10] 算力与云服务商则通过资源调配与接入策略，间接调控全球范围内的网络空间行为生成与分布。这些关键权力节点多数由跨国企业与分布式技术社群掌握，任一主权国家均难以对其完全支配。

由此，全球网络空间治理行动效能遭遇双重削弱。一方面，国家在形式上仍被赋予维护网络安全、数据保护与平台秩序的责任，但在面对高度分散的行动链条与深嵌于模型层的行为逻辑时，其传统治理工具效力日益有限；另一方面，真正掌握生态定义权的行为主体，如模型开发商与开源社区，在国际法层面并非传统意义上的治理者，其缺乏明确的责任框架、问责机制与强制协调平台，导致有责者无权、有权者无责的权责错配局面。这种错配进一步诱发单边化与碎片化趋势。[11] 在缺乏有效国际协调背景下，各国纷纷转向以本国利益优先的技术管控、数据主权与平台监管策略，例如强制数据本地化、算法备案、模型出口审查与数据流动限制等。短期来看，这些措施或许能增强单一国家的管控感知，但从全球整体看，却加剧技术生态割裂，削弱国际社会共同应对网络威胁、协调平台行为与共建安全机制的能力。智能行动域中的权力结构演变，正将全球网络空间治理推向资源和政策投入不断增加但治理效能持续下降的执行困境。

面向智能行动域的生成式治理范式

全球网络空间治理困境的根源在于其范式仍停留在“信息交互空间”时代，与智能行动域的生成性、演化性及生态性逻辑发生本体性错位。固守静态规则、属地管辖与中心化权威，必然导致治理系统性失效。在此背景下，亟须构建一种能够有效响应行动生成机制、系统演化节奏与权力生态特征的治理范式，即“生成式治理”。生成式治理的核心并非在既有框架上叠加新的规制手段，而是要从根本上跟随网络空间的本体演变重构治理的对象、路径与条件：一是要将治理焦点从行为主体和孤立事件转向行动生成机制本身，二是要将治理方式从事后纠偏转向事前塑形，三是要将治理条件从单一权威主导转向多节点生态协同。生成式治理的根本目标，不在于对已发生异常的行为进行事后补救，而是通过塑造模型结构、系统接口与生态边界，促使智能行动域倾向于生成可治理、可审计、可协调的行为。

一、治理哲学的转向：从规制行为到塑造生成机制

生成式治理的哲学基础在于不再将治理视为外部力量对既有行为的限制，而是将其理解为在系统内部创造条件，引导行动生成过程朝着可治理的方向演化。智能行动域中的行为本质上是生成性的，依赖数据、模型、反馈循环、算法参数等多层次结构性因素的相互作用而不断涌现。如果治理仍然将行为视为主体意图的直接表现，并基于此来制定规则，就必然会面临主体模糊、意图难以追溯、行动链条分布式展开等难题。

生成式治理要求从根本上摒弃行为归因式的治理哲学，转向结构生成式的治理哲学。在这一哲学框架下，治理的核心任务不再是简单划分合法与非法的边界，而是要界定哪些生成机制可以被允许存在，哪些必须受到限制，哪些需要被嵌入特定的外部约束。例如，一个

中国知网 https://www.cnki.net

（中新社图片）

2025年9月15日，国家网络安全宣传周开幕式在云南昆明举行。昆明市同时举办网络安全博览会暨网络安全产品和服务国际推介会，机器人与机器狗表演受到广泛关注。

模型是否具备可解释性、是否设计了审计接口、能否支持实时监测，这些已不再是纯粹的技术细节，而是治理哲学的具体体现，即治理的基石从事后追责转向事前指导。[12]

此外，生成式治理哲学承认治理主体的多元性。智能行动域的行为生成逻辑分布在模型、平台、算力等诸多技术节点上，治理无法依赖任何单一主体或权威来完成。国家、平台企业、模型开发者、算力供应商、开源社区等多元主体共同塑造着行动域，因此治理必须正视这种多主体共同参与的结构性现实。[13]

二、治理逻辑的重构：从规则约束到条件共塑

治理逻辑重构的关键在于明确治理应以何种路径与方式介入行为生成过程，而非仅关注由谁实施治理或权力如何分配。在传统网络治理框架下，治理逻辑呈现出明显的线性特征，即依次进行规则制定、行为识别、执法干预和事后追责。这一逻辑建立在行为可识别、行为链条相对稳定、行为后果可明确分割的前提下，允许在行为发生后进行单点纠正。

然而，在智能行动域中，行为是生成式的。一个行动链条可能由模型内部触发，在平台上被放大，进而在另一生态中引发后果，整个过程难以叫停、复现或清晰分割。在此环境下，若继续沿用线性的、末端化的治理逻辑，就会始终处于被动补救的状态。

生成式治理要求治理逻辑实现根本转向，从聚焦行为本身转向探究行为如何形成，从单点管制转向对生成条件的共同塑造。其核心要义在于通过调整行为生成的前提条件与演化路径等变量和相关参数，系统性引导或抑制行动发生。这意味着治理需要前移，尽可能介入行

中国知网 https://www.cnki.net

动链条早期环节。模型开发阶段的数据选择、参数调节、对齐策略与接口开放程度，平台运营阶段的信息流动逻辑、内容标记机制与算法透明度，乃至生态层面的互操作性框架、共识协议与开源社区治理规范，所有这些都构成行动生成逻辑的内在部分，因而也成为治理逻辑的关键介入点。[14]

同时，这种治理逻辑必须具备动态性与迭代性。行为生成机制持续演变，治理逻辑也必须通过评估、反馈和再设计不断调整其介入方式。治理不再是一次性的规则颁布，而是一个围绕生成条件进行持续校准的过程，力求使治理介入的“节奏”和“位置”与智能行动域的演化进程相契合。最终，治理的目标也从纠正错误转变为维持系统合规平稳运行，只要系统能够持续生成可治理的行为模式，治理的根本目的即告达成。

三、治理结构的再造：从层级传导到生成式多节点协同

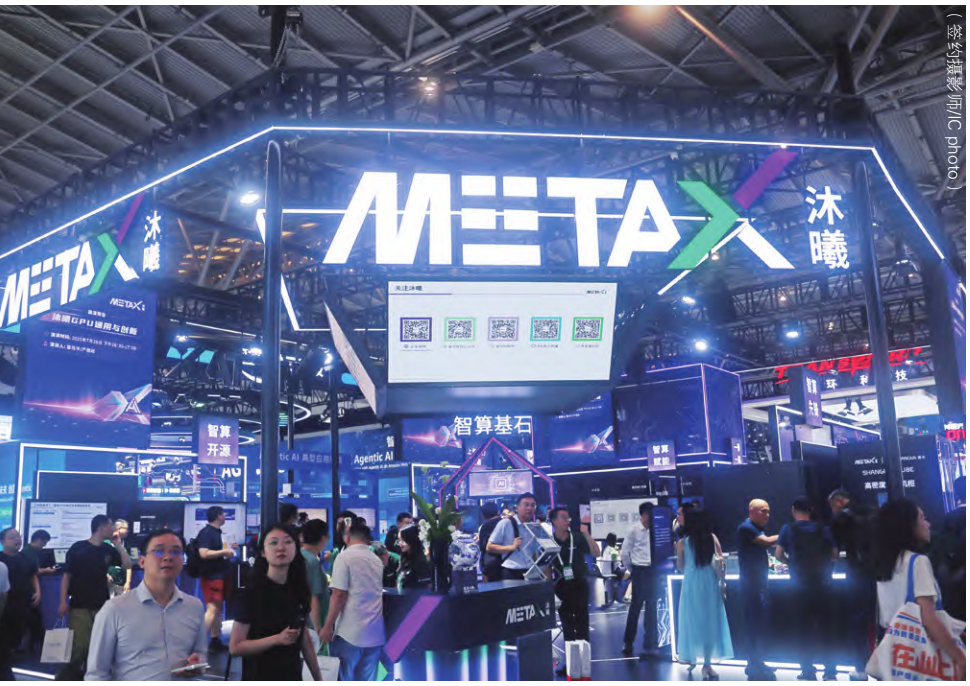
治理结构关注的关键问题是由谁治理、权力如何分配以及制度如何设计，这与前述侧重介入方式的治理逻辑有所不同。生成式治理在哲学与逻辑上的转向，最终需要落实到治理结构重塑上。

传统全球网络空间治理虽在形式上包含多利益相关方参与，并承认技术社群与私营部门的作用，但其底层权力结构仍呈现出以国家权威为顶点的层级化特征。国际组织与多边框架主导原则性共识，各国政府在此基础上制定具有强制力的规则并行使执法权，平台与技术社群则在既定法律与政策框架内发挥作用，整体上仍未脱离主权优先且规则自上而下传导的秩序逻辑。[15]

然而，在智能行动域中，权力生成与作用的逻辑发生根本变化。决定行为生成模式的关键节点，如模型架构定义、算法逻辑嵌入、生态接口控制等，实质上已经转移至全球化的科技企业、模型研发机构、开源社区与基础设施运营商手中。这些节点所行使的权力是生成性的、系统内置的，常常先于或独立于国家的立法与执法过程。

因此，治理结构必须从仍带有层级色彩的传导模型，转向真正多节点、生态化、生成式的协同架构。新治理结构以一组必须深度协同的关键主体作为治理基础。国家侧重于捍卫价值底线、设定合法性框架与维护全局性公共利益，平台需在操作层面建立可信、可控的信息流动边界，模型开发者需将可审计性、可解释性与价值对齐内嵌至系统底层，算力供应者需确保基础架构可靠与安全，技术社群则应持续推动开放、透明、可验证的机制创新。每类主体都既是治理的参与者，也受到其他主体治理行动约束。[16]这一结构的核心在于权力作用方式的转变，即治理有效性不再依靠层级命令，关键主体在机制设计上的耦合度与动态制衡才是决定性变量。只要核心主体在生成逻辑上保持基本同步，系统就更趋于自然涌现出可治理的行为模式。

此外，生成式治理边界也会随之发生变化。治理的有效单元不再主要依据领土疆界划分，而是以技术栈、



（签约摄影师/IC photo）

2025年7月28日，上海，沐曦集成电路股份有限公司参展世界人工智能大会，展示首款全国产通用GPU芯片——曦云C600。

中国知网 https://www.cnki.net

模型族群、协议标准与平台生态等功能性、技术性边界为标尺。治理结构能否生效，关键在于生态内在的规则与机制是否一致。只要生态内部治理逻辑贯通，即便参与主体分属不同主权辖区，协同仍可成立。从这个意义上说，治理结构的再造是从以主权疆域为参照系的治理，转向以技术生态为参照系的治理。

结 语

人工智能的深层效应，并非在既有网络空间上简单叠加新风险，而是通过存在性、时间性与权力性的系统重构，将网络空间从以连接为核心的全球信息交互空间转变为以生成为核心的全球智能行动域。在这一新的本体结构中，人类与人工智能共同构成行动主体。人工智能时代的网络空间行动具备内在的生成性、演化性与生态性，系统处于持续流变之中，权力广泛散布于平台、模型、算力与技术社群等多元节点之间。当前全球网络空间治理在管辖、规则与效能层面呈现的结构性张力，并非源于某项具体技术的突破，而是技术跃迁所引致的网络空间本体深刻重构。为适应这种转变，网络空间治理需要在治理哲学、逻辑与结构等方面及时调整，与网络空间的新本体特征与模式相衔接，以提升网络空间治理效能。生成式治理即为回应上述转型的理论尝试，强调治理应从事后规制转向事前塑形，通过介入模型结构、系统接口与生态边界，使智能行动域倾向于生成可解释、可审计、可协调的行为模式。生成式治理为“全球智能行动域”提供了一种能够随系统共同演进的治理框架。随着人工智能技术的持续发展，网络空间的生成属性将不断增强。唯有在生成机制层面建立有效约束，才能在动态演化中维持治理秩序的稳定与韧性。生成式治理不仅是对当前治理失序的回应，更是通往下一代全球网络空间治理体系的逻辑起点。

本文是国家社会科学基金重大项目“科技革命、产业革命对世界格局的影响塑造和前瞻性应对研究”（项目批准号：25&ZD277）的阶段性成果

作者系复旦大学美国研究中心教授

[1] Zverev Volodymyr, et al., “Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation,” *Contemporary Issues in Artificial Intelligence*, Vol.1, March 2025, https://sciformat.ca/journals/index.php/ciai/article/view/11/5.

[2] 李玥琪等：《生成式人工智能作用下网络空间舆论生态：风险表征、治理挑战及重构路径》，载《现代情报》2025 年第 11 期，第 130-140 页。

[3] Laurie Hughes, et al., “AI Agents and Agentic Systems: Redefining Global it Management,” *Journal of Global Information Technology Management*, Vol.28, No.3, June 2025, pp.175-185.

[4] MingYan Liu and Fei Ye, “Learning Diverse and Adaptive Representations for Continual Learning,” *Neurocomputing*, Vol.664, February 2026, p.112, 132.

[5] 方兴东等：《“守门人”的守门人：网络空间全球治理范式转变》，载《湖南师范大学社会科学学报》2023 年第 1 期，第 49-60 页。

[6] 李传军：《构建全球网络空间治理规则的问题与对策》，载《武汉科技大学学报（社会科学版）》2019 年第 5 期，第 520-526 页。

[7] 吴才毓：《网络空间国际治理政策法律：国际组织与规则探究》，载《政法学刊》2022 年第 6 期，第 117-125 页。

[8] 蔡翠红、管航：《算法权力影响人的安全机制分析》，载《世界经济与政治》2025 年第 8 期，第 38-68 页。

[9] Terry Flew, “Communication Futures for Internet Governance,” *SSRN Electronic Journal*, March 18, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3806967.

[10] James Jewitt, et al., “From Hugging Face to GitHub: Tracing License Drift in the Open-Source AI Ecosystem,” arXiv, September 11, 2025, https://doi.org/10.48550/ARXIV.2509.09873.

[11] 鲁传颖：《网络空间的安全困境、秩序演变与中国方案》，载《人民论坛·学术前沿》2025 年第 13 期，第 24-33 页。

[12] Amit Sheth, et al., “Civilizing and Humanizing Artificial Intelligence in the Age of Large Language Models,” *IEEE Internet Computing*, Vol.28, No.5, 2024, pp.5-10.

[13] Shalabh Kumar Singh and Shubhashis Sengupta, “Sovereign AI: Rethinking Autonomy in the Age of Global Interdependence,” arXiv, November 21, 2025, https://arxiv.org/abs/2511.15734v1.

[14] 周祥军：《论生成式人工智能的分层治理模式》，载《中国法治》2025 年第 8 期，第 106-112 页。

[15] 檀有志：《网络空间全球治理：国际情势与中国路径》，载《世界经济与政治》2013 年第 12 期，第 25-42 页。

[16] 阙天舒：《全球网络空间的竞生秩序与治理间性研究》，载《人民论坛·学术前沿》2025 年第 13 期，第 49-58 页。

中国知网 https://www.cnki.net