责任编辑 / 徐慧 编辑 / 朱非 E-mail:xuadaly@126.com

AI智能体专门立法与现行法如何互补融合

马民虎 黄道丽

- AI 智能体的法律地位是规则适用与制度构建的逻辑起点。目前，全球主要司法辖区普遍坚持“工具主义”立场，不承认 AI 智能体具有独立法律人格。在责任分担方面，归责重心正从“人工智能是否为法律主体”转向“责任应如何在关系网络中合理分配”。
- 在技术中立原则的指引下，现行法律体系能够为 AI 智能体所涉基础法律关系提供规范依据，但受制于制度设计初衷与技术适配性，难以对身份认证、动态授权与复杂责任分配等特殊问题作出有效回应，整体呈现“原则可用、规范不足”的适用格局。
- AI 智能体治理的成熟形态，并非在现行法律与专门立法之间进行单向选择，而是形成以现行法律为基础、专门立法补位、技术标准支撑的三层融合治理体系。

当前，具备自主规划、工具调用与持续执行能力的人工智能（AI）智能体，正在从技术概念走向规模化产业落地。相较于传统人工智能系统以信息输出为主要功能，AI 智能体以自主行动为核心特征。这种角色从“工具”到“自制力”的转变，对以自然人为中心构建的传统法律体系构成了系统性挑战。以 OpenClaw（俗称“小龙虾”）为代表的智能体凭借“自主性权限”所引发的广泛关注，让“监管真空”的讨论变得更趋复杂。AI 智能体的普及使法律治理面临法律身份模糊、身份认证缺失、责任链条不清等多重法律困境。面对这些挑战，全球范围内的立法热潮并非要构建法律秩序，而是在治理路径上寻求现行规则与新型立法之间递进、协同融合的法律逻辑。

AI 智能体身份、认证与责任分配的三重障碍

AI 智能体的法律地位是规则适用与制度构建的逻辑起点。目前，全球主要司法辖区普遍坚持“工具主义”立场，不承认 AI 智能体具有独立法律人格。

然而，随着 AI 智能体自主决策能力、跨平台执行能力与动态学习能力不断提升，其行为模式已显著突破传统电子代理人的功能边界。身份与认证的障碍表现在 AI 智能体在法律意义上不具备主体资格，实践中现行法律体系围绕自然人与法人构建的认证机制，难以适配多智能体交互、动态权限变更等新型场景。这导致行动主体识别、授权核验缺乏稳定规则支撑，威胁交易安全。

在责任分担方面，归责重心正从“人工智能是否为法律主体”转向“责任应如何在关系网络中合理分配”。AI 智能体嵌入在由开发者、部署者、用户等构成的复杂链条中，损害结果往往是系统设计缺陷、训练过程疏漏、部署环节失范、授权操作不当、审查机制缺失以及使用行为不规范等多重因素共同作用的结果。基于此，归责逻辑应根据各方在全生命周期中的控制力、受益程度及风险防范能力进行差异化分配，遵循“谁控制风险、谁直接受益，谁承担义务”的原则。

现行法律对 AI 智能体的覆盖与规范错位

在技术中立原则的指引下，现行法律体系能够为 AI 智能体所涉基础法律关系提供规范依据，但受制于制度设计初衷与技术适配性，难以对身份认证、动态授权与复杂责任分配等特殊问题作出有效回应，整体呈现“原则可用、规范不足”的适用格局。

首先，在代理与合同法律关系层面，传统代理制度与电子交易法律规范构成 AI 智能体合同行为的基本规范基础。现行法律承认自动化系统在获得授权前提下所缔结电子合同的法律效力，从而确立以“人”为责任兜底的基本框架。

其次，在侵权与产品责任层面，现代产品责任制度与侵权责任规范已逐步将软件及人工智能系统纳入规制范围。欧盟新版产品责任指令明确将软件纳入产品范畴，我国《民法典》侵权责任编以及网络安全法律体系亦明确规定了网络运营者与数据处理者的安全保障义务，因 AI 智能体存在设计缺陷、部署不当或滥用行为导致他人损害的，可依据现有规则追究部署者、开发者等相关主体的侵权责任。

第三，在公平交易与数据合规层面，以消费者保护法与隐私法为核心的规范体系，同样可适用于 AI 智能体应用场景。

现行法律适用于 AI 智能体的不足之处：一是统一身份标准缺位，传统账户、密钥与接口权限无法实现对 AI 智能体的唯一标识与可信识别，智能体仿冒、越权操作等风险难以通过法律途径有效防范。二是动态授权难以检验授权范围、意思表示真实性、权限等关键要素，导致以“明示授权”为核心的代理规则在动态、复杂的智能交互场景中陷入“适用失灵”。其三，AI 智能体的决策黑箱、多智能体协同部署与跨地运行等特征提高过错认定与因果关系证明的成本，容易出现责任错位与难以追责的问题。其四，AI 智能体无国界运行特性与管辖权规则的地域性存在内在冲突，跨境身份认证互认、法律适用与执法协作机制存在制度空白。

专门立法的重心：以身份认证为核心的责任分配机制

针对现行法律适用存在的问题，全球主要司法辖区正在推动人工智能专门立法。此类立法并非否定或替代现行法律体系，而是聚焦技术与法律的衔接环节，在继续关注 AI 算法、算力和数据供应链等法律问题的同时，着力构造身份定位、授权可追溯、行为可审计、责任可落实的专门规则。

专门立法的核心方向之一，是建立具有法律意义的 AI 智能体身份制度与强制性身份认证机制。通过立法明确要求为每一个具备独立行动能力的 AI 智能体分配唯一、可验证且防篡改的技术身份，并将该技术身份与背后操作者的法律主体信息进行绑定，从而形成技术身份与法律归属并行的双轨识别体系。核心方向之二，是构建具有密码支撑的加密委托授权机制。借助可验证凭证、数字签名等技术工具，将授权范围、有效时限、变更与撤销流程等关键信息予以固化与审计，实现授权全流程可核验、可追溯，从技术层面降低越权行为与意思表示争议。核心方向之三，是强化高风险 AI 智能体的审计与透明度义务。立法强制要求相关主体留存不可篡改的运行日志与决策记录，明确信息披露与数据提供义务，降低受害者举证难度，提升司法与执法认定效率。核心方向之四，是确立多层次责任分配制度。将实际控制与部署 AI 智能体的主体确定为首要责任主体，同时保留该主体向开发者、供应商、维护方等上下游主体追偿的空间，简化外部追责路径，同时维持价值链内部责任分配的合理性。

从全球实践来看，国际上多地区已呈现出协同演进的趋势。欧盟以《人工智能法案》为基础，逐步推进面向智能体的专门立法，对高自主性、高社会影响的 AI 智能体施加身份标识、授权编码、审计追踪等强制性义务，并强化操作者的严格责任。美国采取州级立法与执法联动的路径，康涅狄格州、加利福尼亚州、纽约州等通过执法备忘录与立法修订，将身份核验、客户身份识别绑定、强化电子签名要求等规则适用于金融、消费交易等高风险场景，明确排除以 AI 自主决策作为免责事由。新加坡率先发布面向人工智能智能体的治理框架，将治理重点从内容合规转向行动可信，聚焦授权边界、行动可逆性与人类监督机制建设。与此同时，ISO/IEC 42001、NIST 人工智能风险管理框架等国际标准，亦将唯一标识、最小权限、持续验证与紧急撤销机制纳入合规基线，推动技术标准与法律规则相互衔接。

现行法与专门立法应分层互补、体系融合

AI 智能体治理的成熟形态，并非在现行法律与专门立法之间进行单向选择，而是形成以现行法律为基础、专门立法补位、技术标准支撑的三层融合治理体系。二者在价值目标、规范功能与实施机制上并非替代关系，而是呈现基础与补强、原则与规则、事后救济与全程监管的协同关系。

从互补结构来看，该体系有以下三个层面交织而成：底层规范由现行法律构成，坚守代理、合同、侵权、竞争、数据保护与消费者保护的基本原则，确立 AI 智能体不具有法律人格、人类主体承担最终责任的制度底线，解决责任归属的根本问题。中层规范由专门立法提供，围绕 AI 智能体身份、授权认证、审计追溯、操作者责任等特定场景构建细化规则，解决现行规则难以直接适用的技术认定与程序核验问题。顶层规范由技术标准与技术机制支撑，通过密码、分布式身份、零信任架构等技术方案，将法律要求转化为可执行、可验证的技术规则，提升合规的在运营上的可操作性。

现行法与专门立法的张力主要集中在三个方面：一是 AI 智能体自主决策与现行意思表示理论的冲突，二是技术身份独立化与法律主体单一化之间的错位，三是现行举证责任分配与当事人举证能力之间的失衡。对此，主流立法理论倾向于采取“功能主义”化解路径，即不赋予 AI 智能体法律人格，但承认其功能性技术身份，通过技术约束实现法律目的，通过举证责任转移、强制信息披露、强制责任保险等制度设计降低维权与执法成本。

从长期发展趋势观察，AI 智能体治理将走向“代理制度现代化”与“智能体专门规则”相互融合的路径。在身份层面，实行技术可标识与法律可归属相结合的双重认定模式；在责任层面，实行操作者首责与价值链内部追偿相结合的分配机制；在监管层面，实行事前认证备案、事中动态监测与事后执法追责相结合的全周期管理模式。这种融合模式在维持现行法律体系稳定性与连续性的同时，实现了对 AI 智能体风险特征的精准治理。

综合前述分析，AI 智能体深刻影响着基础民事、行政与刑事法律关系的重构，专门立法的核心价值在于构建一个“AI 智能体身份可识别、授权可认证、行为可追溯、责任可追究”的可信法治框架。

为此，建议采取分阶段、多维度的推进策略。首先，优先夯实解释性规则。通过发布政策、技术标准以及执法指南、遴选典型案例与司法解释等方式，明确现行法在 AI 智能体场景中的具体适用规则，快速释放法律的确定性。其次，加快专门立法进程。重点推动智能体身份、授权追溯机制、审计日志规范及责任分配比例等专门立法，为技术监管提供硬性的制度支撑。第三，构建协同治理体系。形成一套跨域协同、人机协同、软硬法协同的 AI 智能体治理体系，在为技术创新预留空间的同时，确保交易安全与人格权益不受侵害。

（马民虎系西安交通大学教授、博士生导师、密码法治实践创新基地主任；黄道丽系公安部第三研究所网络安全法律研究中心主任、研究员）