财说法
BUSINESS & ECONOMIC INSIGHTS

AI时代下 OPC需防范哪些法律风险？

中经记者 赵毅 广州报道

2026年《政府工作报告》提出“打造智能经济新形态”、深化拓展“人工智能+”行动，推动AI与经济社会深度融合。人工智能OPC（One Person Company，一人公司）作为“一人+AI工具”的新型创业范式，以“碳基智慧+硅基执行”协同，实现一人全链路业务闭环，成为“超级个体”“一人军团”的新质生产力代表。

当前，全国多地政策加持、产业加速、人才涌入。但AI赋能下OPC天然法律风险也被放大：法人人格混同、AI行为责任、数据合规、知识产权、算法伦理等问题突出，国家层面专项立法空白、监管规则不统一、合规体系不健全，成为制约OPC健康发展的核心瓶颈。

为此，《中国经营报》“财说法”栏目邀请到中国人民大学法学院院长、交叉科学学术委员会主任杨东，中国社会科学院法学研究所教授、博士生导师姚佳，广东省人工智能法律应用重点实验室主任、小包公·法律AI创始人王燕玲，共同解答“OPC在经营中需重点防范哪些法律风险？”助力创业者厘清合规边界、政府明确监管方向、产业构建法治生态。

杨东

中国人民大学法学院院长、交叉科学学术委员会主任

姚佳

中国社会科学院法学研究所教授、博士生导师

王燕玲

广东省人工智能法律应用重点实验室主任、小包公·法律AI创始人

以“共票机制”实现利益共享

个人创意通过AI高效转化，打破传统一人公司的个人能力边界，释放更大发展潜力。

《中国经营报》：目前我国AI处于怎样的发展阶段？您如何看待AI时代下OPC的发展趋势？

杨东：当前，我国AI依托新型举国体制，凭借海量数据与丰富应用场景优势，已进入产业爆发、法治同步推进的高速发展阶段，在数字资产、智能体及多个领域实现突破，整体发展水平位居全球前列，硅基与碳基革命实现深度融合。

AI时代下，OPC迎来颠覆性发展，彻底突破传统一人公司的应用局限，成为AI与市场主体创新融合的核心载体。传统一人公司在工业时代应用价值有限，难以落地推广，而AI技术为其赋予全流程运营能力，可承接经营、管理、营销等各类事务，从个人辅助工具升级为融合个人、组织与社会的新型主体，实现颠覆性创造。

传统公司制度存在代理成本高、数字时代适配性不足的短板，AI赋能的OPC是对传统法人制度的革新，个体可依托其成为具备完整经营能力的超级智能体，中小微企业也可通过智能体实现高效运营。这一变革虽会优化部分岗位，但能推动个人自主搭建OPC创业，实现就业结构升级。

未来需跳出传统确权思维，以“共票机制”（Coken）构建共创共建、利益共享的数字资产治理规则，融合算力、数据、算法等核心要素完善法治体系，为AI与OPC产业高质量发展筑牢制度根基。

《中国经营报》：与传统一人公司相比，OPC在运营模式、法律关系上的核心区别是什么？

姚佳：当前，国内人工智能OPC发展已进入关键转折点，从政策、概念探索阶段迈向良性发展生态构建期，属于现象级发展态势。

从政策维度看，OPC先是创业圈自发兴起，2025年起纳入政策体系，全国20多个城市出台专项政策，培育生态社区与标杆企业；从基础设施维度看，各地高新区加速落地，在算力、产业、社区方面实现技术与人的高效对接；从经济效能维度看，AI实现人机协同工作，大幅降低人力成本、提升产出效率，已形成系统性竞争力，整体处于政策扶持、落地推进、即将迎来快速发展的关键阶段。

与传统一人公司相比，OPC法律定性不变，仍属于一人公司，股东以出资为限承担有限责任，AI仅为工具，不具备法律主体地位，法律责任承担逻辑未变。

核心差异体现在运营模式与生产力结构上，传统一人公司依赖创始人个人时间、精力投入，以人力换取收益，需持续承担人力管理成本；而OPC是“人+AI智能体”模式，通过AI嵌入实现个体能力杠杆化，借助AI完成流程再造、营销策划及大量工作，重构生产力结构。

同时OPC发展内驱力更优，AI赋能推动运营成本持续走低，能将个人创意通过AI高效转化，打破传统一人公司的个人能力边界，释放更大发展潜力。

《中国经营报》：目前，国家层面针对AI的专项立法尚处空白，您认为未来监管规则的完善方向是什么？如何平衡“创新激励”与“风险防范”？

杨东：目前，我国AI治理仍处于由分散规范逐步走向体系化建构的阶段。短期内，AI监管规则的完善方向，不宜简单理解为制定一部“人工智能法”，而应当聚焦于AI基于“平台—数据—算法”多维层面产生的综合影响，因此应当是在既有《网络安全法》《数据安全法》《个人信息保护法》以及算法、深度合成、生成式AI等规范基础上，围绕重点问题持续补强，逐步形成分层分类、衔接协调的系统性《人工智能法》。

具体制度建设需聚焦三方面：一是健全高风险AI活动前端治理，强化伦理审查、风险评估、备案监测等机制，对人身安全、公共利益及其他高敏感场景实施严格合规管理；二是完善数据治理规则，厘清训练数据来源合法性、个人信息保护、生成内容归属等核心问题，规范数据利用秩序；三是明晰平台及模型提供者责任，推动责任从事后处置向事前预防、持续合规转变，明确内容治理、算法歧视防范、虚假生成识别和系统性风险控制等方面形成更清晰的规范框架。

在平衡“创新激励”与“风险防范”的关系上，应构建多维互补的治理体系。首先，推广“监管沙盒”作为压力测试场。其次，实施精准的风险分类分级规制。根据AI的应用场景、技术属性及潜在损害程度设定差异化监管规则，避免因“一刀切”式监管压制行业活力。最后，发挥“共票机制”在价值分配中的枢纽作用。让各方主体公平地分享AI发展的制度红利，从而从根本上激活内容生态的创新动力。

《中国经营报》：您深度参与《网络安全法》《数据安全法》《个人信息保护法》及AI相关立法，在立法层面，如何与国际接轨的同时又体现中国特色？

杨东：我国立法应当立足于数据红利、场景优势及举国体制的组织效能，进行治理范式的自主创新。我国平台经济规模大、技术落地快、应用场景复杂，这意味着立法不仅要关注抽象的技术伦理问题，还要特别回应平台治理、数据利用秩序、公共安全、产业发展和社会稳定等现实议题。

在坚持自主性的同时，应以开放姿态吸收国际成熟经验，推动治理规则的全球兼容。针对算法风险规制、伦理标准及各项全球性命题，应结合我国国情进行制度转化。通过构建既保障国家安全又符合国际通行的跨境数据治理体系，为跨国企业提供透明、可预期的法治环境，降低制度摩擦成本。

应以大国担当积极参与全球AI治理，在世界数据组织（WDO）及各类多边对话平台的基础上，加强与各主权国家及国际组织的双边或多边合作，力促AI安全标准与监管规则的互认对接。在保障技术安全与主权底线的基础上，通过规则共建与风险共担，共同应对AI带来的全球性挑战，促进全球AI产业的互联互通与协同创新，在国际法治舞台上贡献中国方案。

创新不能逾越个人信息保护边界

OPC在运营中借助AI处理用户个人信息，必须严守个人信息保护相关法律底线。

《中国经营报》：当下OPC创业模式高度依赖生成式AI，生成式AI给网络信息治理带来哪些核心挑战？如何解决AI生成内容的版权与数据利益分配难题？

杨东：当下OPC创业模式高度依赖生成式AI，也给网络信息治理带来多重核心挑战。一是内容识别困难，AI降低虚假信息制作门槛，内容高度拟真，难以辨别，加之生成式AI的预训练模型往往存在不可解释性，使得训练数据中潜藏的偏见可能通过AI大规模扩散，形成难以穿透和监管的“算法黑箱”。

二是平台规则缺位，生成式AI的规模化与瞬时性特征使传统的“通知—删除”规则陷入失灵。特别是AIGC内容的非重复性，使得避风港原则中预设的“红旗标准”难以捕捉，导致事后救济的速度远滞后于侵权扩散的速度。若过度苛责平台的注意义务，则可能引发风险厌恶下的“过度拦截”，进而扼杀合规的内容创新。

三是责任分配模糊，AI生成内容侵权涉及多主体，责任边界难以界定，追责难度大。同时，新《公司法》放开OPC设立限制，助力AI时代创业，一人公司制度的股东证明财产独立倒置举证规则，叠加人机混同新形态，进一步加剧了责任认定的不确定性。

针对AI生成内容版权与数据利益分配难题，需从“绝对排他”转向“利益共享”。可引入“共票理论”，依托区块链、智能合约技术，为创作者、平台、用户等主体颁发可追溯、可流通的价值凭证，将内容收益实时回流至各贡献方，实现价值共创共享。

《中国经营报》：AI生成内容知识产权归属、训练数据版权合规是OPC创业者极易触碰的合规红线，目前司法实践中对这类纠纷的裁判倾向如何？创业者在前期应如何规避？

姚佳：在AI生成内容知识产权归属上，我国司法裁判核心看是否有人类智力实质性贡献。因为《著作权法》保护的是人类独创性智力成果，AI本身不具备法律主体资格，无法享有著作权。

法院审理相关纠纷时，不会单纯看内容是否由AI生成，而是判断使用者在提示词设计、参数调整、后期修改中，是否融入独特审美与个性化表达，有充分人类智力投入的生成内容，会被认定为受保护作品。当然，能否被认定为作品，仍然需要在个案中判断。

针对训练数据版权合规，按照相关管理规定，AI训练不得侵害他人知识产权，我国《著作权法》合理使用条款是封闭式列举，无法直接作为数据训练的版权豁免依据。司法实践中，未经授权使用他人作品、爬取受版权保护数据开展模型训练，生成内容与原有作品高度相似的，都会被认定侵犯复制权、改编权，这也是创业者最易踩坑的地方。

对此，OPC创业者前期要做好全方位合规规避，生成内容时全程留存提示词优化、参数调整、后期修改的完整证据链，以此证明自身智力投入；选用训练数据优先采用开源合规数据集，使用他人作品务必提前取得合法授权，网络爬取数据严守相关协议，远离知名IP及各类高风险素材；若是提供AI服务，还要完善用户协议，明确双方权利义务，对AI生成内容风险做好事前提示，严守法律红线，才能保障创业合规稳步推进。

《中国经营报》：若OPC利用AI工具处理用户个人信息，需遵守哪些核心规则？数据泄露、过度采集可能面临哪些法律后果？

姚佳：OPC在运营中借助AI处理用户个人信息，必须严守个人信息保护相关法律底线，AI创新边界不能逾越个人信息保护边界。

在核心规则上，首先要具备合法处理依据，严格遵循《个人信息保护法》规定的合法性基础，不得随意处理用户信息；其次坚持最小必要原则，只采集与业务相关的信息，杜绝过度收集；同时落实告知同意规则，通过清晰的隐私政策向用户说明信息用途、AI处理方式及用户权利；还要履行安全保障义务，采取加密、去标识化及各种技术措施保护数据安全。

数据泄露、过度采集的行为后果十分严重，将面临行政、民事乃至刑事三重责任。行政上会被监管部门处罚、责令整改；民事上需对用户承担侵权赔偿；情节严重的还可能构成侵犯公民个人信息罪，承担刑事责任。

对此，OPC创业者应做好合规安排：根据自身业务定制隐私政策，不盲目照搬模板；与AI工具提供方明确约定数据使用规则，防止数据被擅自用于模型训练；坚持数据最小化，对敏感信息脱敏处理，完善留存、删除机制并保留操作日志；设置便捷的用户权利行使渠道，建立数据泄露应急机制，及时通知用户并上报监管。

合同需注明涉法律风险核心条款

OPC因股东单一、决策集中，易出现所有者与公司边界不清的问题。

《中国经营报》：OPC在经营中存在哪些法律风险？创业者应从哪几个方面采取相应防范措施？

王燕玲：OPC的法律风险与其制度优势紧密相关，因股东单一、决策集中，易出现所有者与公司边界不清的问题，主要集中在四大方面。

一是股东有限责任被突破的风险，这是最核心的风险。若股东无法证明公司财产独立于个人财产，将对公司债务承担连带责任，常见于财务、业务、场所人员混同等情形；二是公司治理与合规运营风险，表现为重大决策无书面记录、年报公示不及时、劳动用工不规范等；三是合同签署与表见代理风险，多因授权不清、印章管理不严，引发越权担保、合同纠纷及其他问题；四是税务合规风险，包括虚开发票、个人账户收款隐瞒收入、虚假申报等，严重可涉刑。

对此，创业者需针对性防范：在财产独立上，设立独立对公账户，规范资金往来，完整留存财务凭证；在公司治理上，重大事项出具书面股东决定，按时公示年报，规范劳动合同与社保缴纳；在合同管理上，明确授权权限，严格印章保管与使用登记；在税务合规上，坚持公款公收，确保账票款一致，依法申报纳税，必要时借助专业财税力量。

《中国经营报》：OPC架构下的财产混同与法人人格否认是风险所在，股东应通过哪些财务与治理手段，有效隔离个人与公司财产？审计报告在其中的关键作用是什么？

王燕玲：新《公司法》规定，只有一个股东的公司，股东不能证明公司财产独立于股东自己的财产的，应当对公司债务承担连带责任。这意味着，在OPC场景下，法律对股东提出了更高的自证要求，实际上体现的是一种更严格的风险分配逻辑。

财务隔离是核心防线，严格做到公私账户分离。公司经营收支全部通过对公账户，杜绝个人账户代收代付；建立完整连贯的会计资料，留存合同、发票、流水等完整证据链；规范股东与公司资金往来，所有款项往来明确性质并留存书面凭证；杜绝账外经营、资产无偿占用行为，保证财务真实完整。

治理上需保障公司独立性，重大经营事项出具书面股东决定并完整留痕；保持公司办公场所、人员、资产及印章管理独立，避免与股东个人混用；建立基础内控机制，规范审批、报销、合同管理流程，彰显公司独立运营意志。

审计报告是证明财产独立的核心证据，既是法定合规要求，也是司法裁判中股东完成举证的关键材料，法院常将年度审计报告作为判断财产是否独立的重要依据，缺失会导致股东举证陷入被动。

此外，开展跨境业务的OPC，还需规范跨境资金流转与税务申报，避免财产混同引发跨境税务合规风险。唯有做到财务分户分账、治理决策留痕、备好审计报告，才能守住有限责任，有效隔离个人与公司财产风险。

《中国经营报》：与AI服务商、合作方签订合同时，需重点明确哪些条款才能规避知识产权、数据合规、责任承担等风险？

王燕玲：企业在和AI服务商、算法公司、数据合作方签订合同时，最大的误区就是只谈“功能、价格和交付”，却没有把真正决定法律风险的核心条款写清楚。

和AI服务商签合同，真正要锁定的，不仅是服务本身，而且是成果归谁、数据能不能用、出了问题谁来承担责任。

知识产权条款需清晰划分权属，明确双方原有知识产权归属，约定训练数据、模型成果、生成内容的权利归属，同时禁止服务商将委托方数据、定制化成果用于其他客户或自身模型训练，严防权利滥用与泄露。

数据合规条款要严格依法约定，要求服务商承诺数据来源合法，规范个人信息处理范围，严禁超范围使用与擅自留存；明确数据存储地点，未经许可不得跨境传输；落实加密、脱敏及其他安全措施，并约定数据泄露后的及时通知与处置义务。

责任承担条款需具备实操性，服务商应担保不侵犯第三方知识产权，若因侵权、数据违规导致委托方遭受罚款、索赔及维权费用，由服务商全额承担。

同时要设置审计监督与退出条款，赋予委托方审计权限，要求服务商留存操作日志；合同终止后，服务商须按期删除或返还全部数据，杜绝后续风险。通过明确上述条款，才能有效隔离风险，保障OPC合规使用AI服务。