

【数字经济】

开源软件的合规治理与政府采购

邬展霞 张国锋 朱其罡

摘要：中国政府在“十四五”规划中明确提出支持开源发展的国家科技战略。DeepSeek、OpenClaw 一经问世迅速风靡全国，成为软件领域数字公共产品的主要供给。事实证明，开源不仅在技术层面产生了深远影响，还在政策和管理层面带来了新的挑战 and 机遇。本文从概念及特性阐述开源具有数字公共产品的特性，指出政府采购可以从推动技术创新、引导市场需求、营造公平环境、推动合规建设、提高供应链安全、促进开源软件的发展；同时剖析开源软件政府采购时可能面临的法律层面、技术层面、许可证层面、知识产权与供应链的合规风险，通过借鉴主流国家在鼓励开源公共产品发展时的风险管控经验，结合政府采购国际规则、国际政策经验对比，提出对开源软件政府采购及公共产品促进中的合规治理建议。

关键词：数字公共产品；开源合规；政府采购

作者简介：邬展霞，上海对外经贸大学教授，中国对外贸易会计学会跨境采购与国际财税专委会副主任（上海 201620）；张国锋，教授，上海对外经贸大学开源创新与数字治理研究院院长、上海开源信息技术协会创始人（上海 201620）；朱其罡，北京智源人工智能研究院开源专家、FlagOS 开源社区秘书长（上海 200336）

DOI 编码：10.19941/j.cnki.CN31-1957/F.2026.04.004

根据国际著名 ICT 研究与咨询机构 Forrester 发布于 2022 年的统计，全球 80% 以上的应用软件使用了开源组件，在能源、金融、互联网行业的比例已高达 95%^①。开源已成为全球软件产业的主要模式，在我国也颇受重视。2021 年以来，我国相继发布《关于规范金融业开源技术应用与发展的意见》《“十四五”软件和信息技术服务业发展规划》《“十四五”数字经济发展规划》等政策文件，明确开源模式作为软件技术和产业创新的主导模式。《中国开源年度报告》显示，2024 年度开源 AI 井喷式爆发，全年诞生出无数热门的开源软件应用^②。2025 年以来，我国工业和信息化部多次细化政策，进一步引导平台企业、制造企业共建开源生态，强化企业开源操作系统适配^③。研究发现，各国在开源软件引领信息技术快速发展的背后，政府采购是重要的驱动力量。开源以其低成

① 中国科协创新战略研究院，《创新研究报告》，2022 年。

② 《2024 中国开源年度报告》，<https://kaiyuanshe.github.io/2024-China-Open-Source-Report/>。

③ 《推动工业互联网平台高质量发展行动方案（2026—2028 年）》，中国政府网 2025 年 12 月 29 日，https://www.gov.cn/zhengce/zhengceku/202601/content_7054660.htm。

本已成为诸多国家政府采购可持续发展的最佳实践之一。

一、开源软件的本质是数字公共产品

（一）数字公共产品的概念与特性

2013 年美国经济学家 Shane Greenstein 首次将“公共产品”的概念拓展至数字世界。2020 年，联合国《数字合作路线图》报告中，明确数字公共产品定义是“开源软件”“开放数据、开放人工智能模型、开放标准和开放内容”。耿曼曼通过文献调查和网络调查，详细探讨了数字公共产品的概念、标准，指出，数字公共产品具有开源、开放、共享的特点^①；隆云滔等从国际经验的角度出发分析认为，数字公共产品应具有开放协作作用^②；杨旭梳理了数字公共产品的发展脉络和特征，深入探究了数字公共产品的概念和特征，指出数字公共产品同样应具有非排他性和非竞争性^③。

（二）开源软件具有数字公共产品特性

开源软件（Open Source Software, OSS）是指源代码公开，允许开发者自由查看、修改、复制、分发的软件，其核心特征是开放协作、共享创新，依托全球开发者社区实现技术迭代与功能完善^④。按照开源促进会（Open Source Initiative, OSI）的定义，开源软件具有源代码公开、可自由再发布、允许衍生作品、可分发许可证、保持技术中立等特征。源代码公开使开源软件形成近乎免费的“公共产品”创新架构，呈现出数字公共产品非竞争性、非排他性、互操作性等特质，极大降低了用户的研发成本，催生出高效的协作共享创新模式，为低成本开展更高层次的创新活动提供了技术条件^⑤。开源软件明确具有数字公共产品的属性特质。

另一方面，开源软件的成本效益优势使其成为数字公共产品的理想选择。政策研究发现，一些国家从 2004 年起就出台支持性政府采购公共政策，力争在全球开源创新中形成先发优势^⑥。2021 年 9 月欧盟发布的《开源软硬件对欧盟经济技术独立性、竞争力和创新的影响》报告显示，开源社区的贡献者数量占 2018 年欧盟 310 万计算机雇员的 8%；开源对欧盟的 GDP 贡献显著，每增加 10% 的开源软件投入，将促进欧盟 GDP 增加 0.4% 至 0.6%，并催生 600 多家计算机通信领域的初创企业^⑦。全球已有超 100 个国家已

① 耿曼曼：《数字公共产品：概念、标准及与图书馆的相关性》，《大学图书情报学刊》2024 年第 5 期，第 83—89 页。

② 隆云滔、林靖玲、刘海波等：《数字公共产品开放协作治理机制研究：基于国际经验分析的视角》，《中国软科学》2025 年第 1 期，第 65—76 页。

③ 杨旭：《数字公共产品的多维解读》，《内蒙古科技与经济》2024 年第 24 期，第 76—79 页。

④ What Is Open Source Software? <https://www.linuxfoundation.org/blog/blog/what-is-open-source-software>.

⑤ 张超、冯泽、陈凯华等：《关于健全数字公共产品制度推进开源创新生态建设的若干思考》，《中国科学院院刊》2024 年第 11 期，第 1944—1955 页。

⑥ 见下文国际政策借鉴部分详述。

⑦ The Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy, https://opencommons.org/images/c/c1/The_impact_of_open_source_software_and_hardware_on-KK0421081ENN.pdf.

将数字公共产品纳入国家数字战略或公共政策^①。健全开源数字公共产品制度已经成为各国抢占开源创新先机的关键。我国学者郭雪也从社会可持续等发展维度，论证了开源的重要价值^②。

二、政府采购促进开源软件发展的作用路径

政府采购是指使用财政性资金采购依法制定的集中采购目录以内货物、工程和服务的行为。一般而言，公共产品难以通过市场机制有效提供，需要政府通过政策引导、资金扶持、市场调控等手段，弥补市场缺陷，推动产业健康发展。开源软件具有公共物品属性，其创新过程存在投入大、周期长、风险高的特点，市场主体的创新积极性易受抑制，需要通过政府采购等方式进行干预，分担创新风险、培育市场需求，推动开源软件产业可持续发展。各国实践显示，政府采购对促进开源产业发展和开源软件进步产生了积极影响，如 Hall 报道了英国政府在新 IT 战略中已将开源软件置于核心地位，以提高政府 IT 项目的透明度和成本效益^③。政府采购对促进开源软件发展的作用主要有：

（一）推动技术创新

政府通过直接采购开源软件产品与服务，可以为企业带来稳定的收入，缓解企业的资金压力，分担研发成本与风险，激发企业的创新积极性，增强企业的创新信心。通过政府采购可以为开源项目提供资金支持，鼓励企业加大研发投入，推动开源软件的技术创新和产品升级，从而加速开源软件的发展。例如，美国国家航空航天局（National Aeronautics and Space Administration, NASA）的詹姆斯·韦伯太空望远镜地面控制系统，需要一款能够在极端环境下稳定运行的操作系统，政府采购需求引导 Linux 开发者开展定制化创新，开发出适配太空场景的定制化 Linux 系统，保障了地面控制系统的稳定运行^④。美国科技出版社 2025 年一份研究指出，政府每年巨额的技术采购不仅是工具购买，更决定了科技产品的市场格局与创新方向，开源软件能够打破技术垄断，降低政府采购成本，但若缺乏政策引导，政府采购可能固化封闭软件的市场地位，抑制开源创新^⑤。康奈尔大学通过对 16 个数字成熟国家的政策分析发现，明确的政府采购政策框架与专门的开源管理机构，能够有效推动开源软件的协同创新，提升公共部门数字化转型效能^⑥。

（二）引导市场需求

政府采购优先选择基于开源技术的软件产品和服务，可以带动市场用户采用开源软

① 中国信通院：《数字公共产品研究报告（2024 年）》，<https://www.caict.ac.cn/english/research/whitepapers/202504/P020250402569171587333.pdf>。

② 郭雪：《全球开源生态发展现状、趋势与对策建议》，《中国科学院院刊》2025 年第 3 期，第 471—476 页。

③ Hall, Kathleen. Government puts open source at the heart of its new IT strategy, in *Computer Weekly*, 2011.

④ 《Linux：开源世界的基石与创新引擎》，CSDN2025 年 5 月 5 日，https://blog.csdn.net/2502_90305547/article/details/147718677。

⑤ Mercado-Lara, E., Dosemagen, S., & Parker, A. Unlocking Innovation: Why Federal Procurement Should Embrace Open Source. Tech Policy Press, <https://www.techpolicy.press/unlocking-innovation-why-federal-procurement-should-embrace-open-source/>.

⑥ Linåker J, Carlberg A N, O’Riordan C, “Public Sector Open Source Program Offices—Archetypes for how to Grow (Common) Institutional Capabilities”, in *arXiv preprint* 2016, arXiv:2603.04891.

件,促进开源软件的推广应用。规模化应用会进一步降低开源产品和服务成本,提高整个行业的竞争力。例如,美国环境保护局在采购过程中,明确要求所有涉及开源软件开发的项目必须采用规范的开源协议,引导企业围绕环保领域需求开展开源创新,推动开源软件在环境监测、数据治理等场景的应用^①。

(三) 营造公平环境

开源软件的使用不仅降低了政府的采购成本,还通过促进跨部门合作和资源共享,提高了政府的治理能力。Bryan Kirschner 研究了平衡计分卡在开源政策和战略中的应用,提出了一个多学科、多利益相关者和社区导向的方法,强调了学习、创新和客户满意度的重要性^②。Christos Bouras 等人就提出了关于欧洲公共管理机构使用开源软件的政策建议^③。我国政府采购领域已连续出台了《政府采购领域“整顿市场秩序、建设法规体系、促进产业发展”三年行动方案(2024—2026年)》《关于促进政府采购公平竞争优化营商环境的通知》等文件,加速公平公开、透明化等建设,开源软件进入政府采购领域能够使供应商在更加公正的平台上开展竞争。

(四) 推动合规建设

政府采购通过制定明确的采购标准、技术规范与开源协议要求,能够引导开源软件企业按照统一的标准开展创新,提升创新质量与兼容性,可避免“碎片化”创新与重复投入。例如美国联邦政府采购中,通过《联邦采购条例》明确开源软件的采购标准与合规要求,引导企业遵循统一的开源协议,推动开源软件的互操作性与可复用性^④。

(五) 提高供应链安全

开源软件的透明性和可定制性使得政府能够更好地控制软件的安全性,减少对单一供应商的依赖。政府采购过程中的专家评审机制,能够对开源软件的技术水平、创新程度进行严格审核,倒逼企业提升创新质量,聚焦核心技术突破,避免低水平重复创新。此外,政府采购还能够推动开源软件的安全标准建设,引导企业加强漏洞修复与安全防护技术创新,提升开源软件的安全性与可靠性。政府采购对开源软件的采用有助于构建更加安全、可控的软件供应链,并带动相关产业链的发展,最终有助于推动开源生态的整体技术进步,以及推动整个软件产业转型升级。Krooswyk 提出,通过分析数据,联邦政府和开源软件社区可以采取有针对性的措施来降低风险并增强整体安全态势^⑤。此外,Krooswyk 还强调, AI 驱动的代码生成可以帮助开发者编写更安全和高效的代码,从而加速开发过程。

① Open-Source Software and Code., <https://www.epa.gov/developers/open-source-software-and-code-repositories>.

② Kirschner B, “Building a Balanced Scorecard for Open Source Policy and Strategy: A Case Study of the Microsoft Experience”, in *Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance*, 2008, pp.226—231.

③ Bouras C, Filopoulou A, Kokkinos V, et al., “Policy Recommendations for Public Administrators on Free and Open Source Software Usage”, in *Telematics and Informatics*, 2014, Vol.31, No.2, pp.237—252.

④ 见下文详述。

⑤ Joel Krooswyk.Strengthening open source: A roadmap to enhanced cybersecurity.Nextgov.com, 2023.<https://www.c4isrnet.com/opinion/2023/11/09/following-the-roadmap-to-open-source-software-security/>.

开源软件的数字公共产品属性及其成本效益优势，使得政府采购成为促进产业健康发展的主要政策工具。Robert Deller 和 Veronique Guilloux 通过采访法国中央和地方政府的 100 多名项目和信息技术官员，探讨了法国政府在数字化政府建设中使用开源软件的情况，发现政府采购在推动开源软件使用方面确实发挥了重要作用^①。

三、开源软件参加政府采购面临的挑战与风险

已有风险事件暴露出开源软件的风险主要是各种合规风险。政府采购政策制定需要首先考虑不同层面的合规风险。

（一）法律责任层面的合规风险

开源许可证的存在天然会带来法律责任风险。开源软件源代码的自由使用需满足许可证的规定条件。一些开发人员合规意识淡薄，未完全遵照许可规定因此违规。调研发现国内 21.4% 的开源开发者完全不懂任何许可证^②，使开源软件自带合规风险。另外，开源组件的不同许可证之间会产生兼容性合规问题。据 Black Duck Knowledge Base 统计，目前开源软件已存在 2 600 多份许可证，不同的许可证组件之间的冲突可能使整个软件产品违规。2019 年 Black Duck Software 公司审查发现，开源组件之间存在开源许可证冲突的情况占 67%^③。我国当前金融科技领域的开源软件同样涉及版权侵权问题^④。

另一方面，开源软件的创新发展使现行法律责任边界的适用性不再清晰。例如 2010 年甲骨文公司控告谷歌公司在 Android 系统中应用了甲骨文拥有版权的 JAVA，属于侵权并要求赔偿 90 亿美金。经过 8 年上诉，法院于 2018 年判定谷歌侵权，然而 2021 年最高法庭又以谷歌的代码复制属于合理使用为由，最终判定不构成侵权。

（二）技术安全层面的合规风险

源代码的开放性本身使软件安全合规面临威胁，诸如代码安全漏洞、恶意代码注入、数据泄露风险等安全风险。国产软件项目中安全风险普遍存在。有数据显示，2023 年国内企业自主开发的软件项目中，开源组件的使用率达到了 100%，平均每个项目会使用 166 个开源软件、存在 83 个开源软件漏洞，当整体缺陷密度相较于前几年有所下降^⑤，软件质量总体呈现上升态势。

开源软件攻击手段不断升级加大了安全合规风险。开源软件攻击的手段日新月异，据悉英国剑桥大学发明了一种隐蔽手段，通过 Unicode 可以构造不可见字符以躲避过人工审核^⑥。开源软件的安全风险需要网络安全人员不断追踪和分类研究。

① Deller R, Guilloux V, “Open Source Software Movement in the French Central and Local Government: A Retrospective and Prospective Exploratory Study”, in *International Journal of Electronic Democracy*, 2008, Vol.1, No.1, pp.1—13.

② 张超、冯泽、陈凯华等：《关于健全数字公共产品制度推进开源创新生态建设的若干思考》，《中国科学院院刊》2024 年第 11 期，第 1944—1955 页。

③ 王志强、伍胜、肖国强等：《开源许可证合规性研究》，《软件学报》2022 年第 8 期，第 3035—3058 页。

④ 陈江丰、王跃、孔令颖：《开源技术应用法律风险研究》，《金融科技时代》2024 年第 6 期，第 8—12 页。

⑤ 奇安信：《2024 中国软件供应链安全分析报告》，2024 年，https://www.qianxin.com/threat/reportdetail?report_id=316。

⑥ 洪晟、易哲凯：《开源软件供应链安全展望》，《工业信息安全》2024 年第 1 期，第 13—18 页。

（三）许可证层面的合规风险

开源软件的许可证种类繁多，每种许可证都有其特定的使用条件和限制。但企业在选择合适的许可证时可能会遇到困难，因为开源软件在许可证兼容性方面的问题十分复杂^①。Eremeev M.A. 和 Zakharchuk I.I 研究指出，许可证兼容性是开源软件的重要风险来源，不当的许可证组合可能导致法律纠纷，影响项目的可持续性和安全性^②。

许可证条款遵守不足会引发法律、财务和技术风险。Robin Gandhi、Matt Germonprez 和 Georg J.P. Link 分析了各种开源许可证的特点，并描述了使用开源许可证可能引发的法律争议；建议采用开放数据标准分析和评估企业的开源软件风险^③；Eremeev M.A. 和 Zakharchuk I.I. 建议采用自动化评估以确保对开源项目的风险控制^④。

项目许可证的变更也会带来风险。在 2016 年，Facebook 决定将其开源 React 框架项目的全部权利转让给自身。这一决策给百度公司带来了潜在风险。根据相关的许可协议，Facebook 实际上获得了免费使用百度在人工智能和自动驾驶领域所获得的专利的权利，使百度处于不利地位。

引入合规开源软件后还会因许可证被修改而违规的风险。数据库公司 MongoDB 在 2018 年对其开源许可证做了调整，从 AGPL V3.0 变更为 SSPL（Server Side Public License）。在变更之前，根据原的条款，云服务提供商在进行“远程网络交互”时，不需要公开他们对源代码所做的任何修改。然而，新许可证条件下，要求任何提供 MongoDB 数据库服务的云服务提供商，只要他们对外提供该程序的功能，就必须公开其源代码。这一变化旨在保护开源社区的利益，并确保所有用户都能访问到软件的改进和更新。这一变更促使该开源软件的用户不得不重新审视其对软件的使用行为。

开源许可证的法律效力不同于一般知识产权。在 2017 年，美国 Artifex Software 公司对韩国的 Hancom 公司提起诉讼，理由是 Hancom 公司销售的软件产品中使用了 Artifex 的开源软件，但未遵守相应的开源许可证条款。Hancom 公司则可能主张自己作为一家美国境外的公司，可能认为美国法院的管辖权有限。但开源许可证的遵守是一个全球性的问题，最终美国法院按照许可证的规定，判定韩国公司应该按照美国法律进行赔偿^⑤。

（四）知识产权和其他合规风险

开源软件知识产权合规的情形具有复杂性：开源贡献者作为开源软件的作者，可以依据著作权法保护自身合法权益；使用者违反开源许可证要求，可能导致版权侵权；使用开源软件名称可能又涉及商标权合规风险；开源软件所涉的技术构思、操作方法又属

① Williams van Rooij S, “Perceptions of Open Source versus Commercial Software: Is Higher Education Still on the Fence?”, in *Journal of Research on Technology in Education*, 2007, Vol.39, No.4, pp.433—453.

② Eremeev M A, Zakharchuk I I, “Risk Assessment of Using Open Source Projects: Analysis of the Existing Approaches”, in *Automatic Control and Computer Sciences*, 2023, Vol.57, No.8, pp.938—946.

③ Gandhi R, Germonprez M, Link G J P, “Open Data Standards for Open Source Software Risk Management Routines: An Examination of SPDX”, in *Proceedings of the 2018 ACM International Conference on Supporting Group Work*, 2018, pp.219—229.

④ Eremeev M A, Zakharchuk I I, “Risk Assessment of Using Open Source Projects: Analysis of the Existing Approaches”, in *Automatic Control and Computer Sciences*, 2023, Vol.57, No.8, pp.938—946.

⑤ 王志强、伍胜、肖国强等：《开源许可证合规性研究》，《软件学报》2022 年第 8 期，第 3035—3058 页。

于专利法保护的對象。

开源软件还存在知识产权之外的其他合规风险。Linux 基金会是推动开源项目成功运营的非营利组织，其注册地在美国。因此，它必须遵守美国的出口管制法规。当涉及基金会开源项目的加密技术模块时，根据美国法律，出口时需要通知美国安全部门。

开源平台或社区也会对开源项目的使用作出规定。例如 Linux 操作系统是由林纳斯·托瓦兹（Linus Torvalds）创建的，Linux 基金会是支持 Linux 操作系统发展的非营利组织。虽然该基金会下的项目可以开源使用，但 Linux 商标在未获得其创始人授权的情况下，禁止使用。

（五）供应链的合规风险

政府采购的开源软件需要持续的技术支持服务。由于开源软件通常由社区维护，可能存在技术支持不稳定或服务不及时的风险。

上游供应链管制可能会引发断供风险。很多底层基础软件如 Hadoop、Spark 等、主要的开源基金会和项目托管平台都在美国注册。根据美国现行的《出口管理条例》，公开可用的源代码通常不受出口限制。然而，随着国际开源竞争形势的变化，不能排除美国政府对开源软件的管制，导致技术服务连续性、系统稳定性受到影响^①。

使用者的并购也会带来合规风险。一些开源许可证将许可接受者及其关联方视为单一实体。以 Apache V2.0 许可证为例，任何对许可接受者的限制同样适用于其关联实体。如果许可接受者因专利诉讼导致授权终止，这种终止同样会扩展到其关联实体。同样，如果关联实体未能履行许可证义务，也可能被视为是许可接受者的侵权行为^②。这需要政府采购中对集团的开源软件风险进行合并管理。

四、国际化视角下相关政府采购政策分析

国际化视角下政府采购政策包括政府间经贸协定的相关规定，以及关于各国开源软件政府采购公共政策的国际对比。开源软件竞争力取决于一国对于开源治理政策的国际竞争力。

（一）政府采购协定中的相关规定

1. WTO 框架下 GPA 的相关规则

世界贸易组织（WTO）框架下于 1979 年推动签订了第一份《政府采购协定》（下文简称为 GPA）。GPA 与软件有关的主要讨论或规定在于：（1）电子商务联合声明倡议（E-commerce Joint Statement Initiative, JSI）。要求为电子商务提供一个公平的竞争环境，确保电子商务的透明度和可预测性；（2）电子交易框架。致力于维护与联合国国际贸易法委员会 1996 年电子商业示范法一致的电子交易法律框架，以免对电子交易施加不当的监管负担；（3）网络安全。成员国同意合作识别和减轻网络威胁，以增强对电子商务的信任；（4）数字贸易规则。成员国努力制定规则以适应数字经济的现实，包括电子商务

① 邓辉、王亚楠、黄小莉：《开源软件典型知识产权风险及应对建议》，《保密科学技术》2023 年第 3 期，第 48—54 页。

② 汪明达、刘世钰、聂大成等：《国外互联网开源信息处理研究综述》，《通信技术》2023 年第 7 期，第 807—814 页。

的共同指导原则和规则；（5）电子采购。允许电子工具的使用，如使用电子采购平台和电子文档交换；（6）技术规格：GPA 允许成员国在制定技术规格时考虑环境保护和资源节约的要求。总体来看，WTO 没有涉及开源软件的专门规定，尚未涉及开源概念的运用。只有原则（6）为采用开源软件提供了可能。

2. RCEP 协定下的政府采购

政府采购一直是多边经济贸易开放中的难点，区域全面经济伙伴关系协定（以下简称 RCEP）关于政府采购相关内容，内容较少。目前其在政府采购方面仅局限于透明度与合作两个层面的原则规定。事实上，RCEP 允许成员国在政府采购中各有所长，以支持本国产业发展和技术创新的需求。

3. CPTPP 下的政府采购

全面与进步的跨太平洋伙伴关系协定（以下简称 CPTPP）代表了国际贸易协定的最高标准。CPTPP 条款关于政府采购的内容进一步增强了政府采购的透明度。CPTPP 与软件相关的专门内容与 GPA 下大致相同，但协定引入了“可持续发展”等多元价值观评价标准，可持续发展理念与开源软件的应用紧密相关；CPTPP 特别强调为“中小企业有效参与”创造公平竞争环境，也切实有助于开源企业投标政府采购活动。

各种政府采购国际协定都没有为开源的发展提供直接指引，发展开源应该依赖于一国国内政策的专门制定。

（二）开源软件政府采购公共政策国际借鉴

美欧英等西方国家较早制定了支持开源业态发展的相关政策，以开源为手段在全技术界跑马圈地，试图主导数字世界规则及标准主导权。

1. 欧盟以政府采购法令与平台协作的开源软件治理

建立政府采购开源软件的法令。欧盟 2004 年颁布了包含开源软件的《公共采购指令》（Public Procurement Directives），并不断根据新的《欧盟开源软件策略》修订其《公共采购指令》，确立非歧视、透明、公平竞争原则，禁止排斥开源方案，确保开源软件在政府采购中的平等地位^①；明确欧盟委员会要参与开源软件社区建设并提供经费；为开发者提供适当经费支持及合规法律指导。2012 年推出《公共行政机构免费和开源软件采购指南》，包含基本软件、如何规划和定义采购方法、估算成本和效益、优先考虑互操作性和开放标准、软件供应模式和供应商选择，以及建立公平的招标过程等内容。2024 年 3 月欧盟推出的《网络弹性法案》就开源软件的文档编制和漏洞处理制定了规则。荷兰政府设立了“软界限”，要求政府部门自 2008 年 4 月开始使用开源软件。立陶宛通过绿色采购政策支持对开源采购的积极态度。法国《国家开放科学计划（2021–2024 年）》要求，受公共资金资助的源代码应向公众开放，开源开放的概念已经深入政府部门。2025 年，《迈向欧洲开放数字生态系统》，将开源纳入数字主权战略，要求政府采购优先考虑欧盟合规开源方案^②。

建立开源发展的市场秩序。2020 年欧盟相继公布《数字服务法案》（DSA）、《数

① 首次颁布于 2004 年，强调在软件采购中应支持互操作性、透明度和灵活性，以提高公共资金的经济有效性。2014 年经修订，确立开源与闭源平等采购、社区贡献、许可证合规三大核心原则。

② European Commission (2014). Open Source Software Strategy 2014–2017. European Commission Digital Strategy.

据治理法案》（DGA），旨在规范数字公共产品的交易规则，倡导数字市场的公平和开放，保障其商业创新环境以促使企业乐于参与开源建设。同年发布新的《开源软件战略（2020—2023 年）》专门强调在信息技术和其他战略领域增加开源的使用，提高欧洲的数字化建设和公共服务能力。瑞典政府建立了专门的框架协议以指导政府部门采购开源软件，并将与知识产权相关的风险转移到供应商。

建立欧盟公共部门开源协作平台 Joinup 进行统一指导。欧盟委员会主导的公共部门开源软件共享、采购指南与案例库，是政府采购开源的核心实操平台。平台开发了《开源软件政府采购指南》（Guideline on Public Procurement of Open Source Software, 2010），明确总拥有成本（TCO）评估、许可证合规、开放标准等要求。2025 年上线《欧盟开源解决方案目录》（EU OSS Catalogue），收录 640+ 合规开源方案，供成员国政府采购参考。建立 Interoperable Europe Portal（欧洲互操作性门户），发布《欧盟 ICT 采购标准目录》，推动欧盟公共部门互操作性，发布开源软件标准、合规框架与共享目录，明确政府采购软件需遵循开放标准，为开源软件准入提供技术合规依据^①。

政府提供合规指引。政府建立 Public Buyers Community（欧盟公共采购者社区），为公共采购人员提供开源采购实操指南、模板与最佳实践，如《开源软件采购知识产权策略》，明确政府采购开源软件的版权转移、再许可、开源协议兼容等合规要点^②。2026 年欧洲数字权利组织（EDRi）在《对欧盟“迈向欧洲开放数字生态系统”战略的反馈》中，直接建议将开源原则纳入政府采购强制要求，并强化合规监管^③。

2. 美国促进开源政府采购的重要制度与公共政策^④

政府采购推动开源战略实现。美国联邦政府预算与管理核心机构负责发布开源采购顶层政策。2016 年 8 月该机构出台《联邦源代码政策》，确立“开源优先、代码复用、20% 开源发布”三大原则，要求联邦机构每年必须将不少于 20% 的新开发源代码以开源形式公开发布，并且要求开源至少 3 年，以及促进联邦机构之间的创新和协作，减少重复投资。《SHARE IT 法案》（2024）将上述政策上升为法律，强制机构跨部门共享定制代码并公开清单。2025 年发布《AI 开源资产共享备忘录》，将开源框架扩展至 AI 模型、数据集，要求联邦机构优先重用开源 AI 资产^⑤。

2021 年，白宫发布《改善国家网络安全行政命令》，要求联邦采购优先使用具备 SBOM 与漏洞管理的开源软件。2022 年，针对开源软件 Apache Log4j（Log4Shell）高危漏洞爆发，美国白宫连续举办两届开源软件安全峰会，与企业界共同探讨开源安全关键问题，要求联邦采购与供应商必须遵循安全开发生命周期（SDL）、SBOM（软件物料清单）、漏洞披露等强制标准，视开源安全为执行核心，建立起政府—产业—社区联合应急响应机制。美国政府逐渐构建起开源相关安全治理战略体系。美国政府建

① European Commission (2025). EU Catalogue of ICT Standards for Procurement. Interoperable Europe Portal.

② European Commission (2023). IPR Strategy for Open Source Software Procurement. Public Buyers Community.

③ EDRi (2026). Feedback on a European Union Strategy “Towards European Open Digital Ecosystems”. European Digital Rights.

④ 庞林源：《美国开源软件治理实践路径与启示》，《软件和集成电路》2024 年第 8 期，第 44—47 页。

⑤ Office of Management and Budget (2016). M-16-21: Federal Source Code Policy. The White House.

立了包含安全理念的开源治理框架。依据《2023—2025 年 CISA 战略规划》以及《国家网络安全战略》的指导,美国政府制定的《开源软件保护法案》(Securing Open Source Software Act, SOSSA, 2022)确立联邦政府保障开源生态安全的法定职责,以及《美国开源软件安全发展蓝图》等文件,体现出对开源安全战略的系统安排。同时,政府已成为开源安全最大购买方。

提供配套技术支持提高合规水平。联邦开源门户(code.gov)发布了《联邦开源采购合规手册》《代码复用评估工具》^①,集中发布联邦机构开源项目、采购合规指南与代码目录。《联邦采购条例》(FAR)设定了开源采购专项条款,其中 1539.2 条款是专门的《开源软件采购条款》,明确禁止授予承包商独占版权,以保障政府复用与修改权^②。

联邦政府创建开源风险评估框架,提供评估准则、流程规范、指标条目、实践工具等多项应用指南;政府联合美国国家标准技术研究院形成《供应链风险管理指南》(2022)^③,联邦数字服务平台提供《开源软件政府采购实施指南》(2016)^④,专门针对政府采购提供关键软件使用的安全措施、供应商源代码测试指南等安全指引,并联合研究机构和开源企业提供相关标准、框架、最佳实践等。

支持基金会引领开源合规。美国开源基金会的管理服务与运营能力具有领先优势,并已垄断了全球大部分开源软件的代码托管服务。全球最大的基金会是美国 Apache 基金会,截至 2021 年,已为 350 多个开源项目提供支持,管理着 2254 个存储库的超过 2 亿行代码。基金会除了接受会员捐赠、活动赞助、项目支持外,还接受政府的资金支持。基金会可以发布关于开源软件的使用安全、关键性、基础设施安全漏洞处理等内容,并提供相关开源软件规范、课程和合规认证,如美国 Linux 基金会主导的《开源软件供应链规范》已被国际标准化组织(ISO)和国际电工委员会(IEC)采纳为国际标准。

软件成份标准化管理。为提高软件供应链的透明度和安全性,2021 年 7 月,美国国家电信和信息管理局(NTIA)发布了物料清单管理(Software Bill of Materials, SBOM)“最低要素”指导意见,提出了软件产品应具备的最基本“成份”,要求软件产品详细列出构成软件应用程序或系统的各个组件及其版本。这种提升透明度的要求有助于用户更好地管理和所用软件的风险。2022 年 9 月,美国出台了《通过安全的软件开发实践增强软件供应链的安全性》规定,要求政府采购供应商必须提供完整的 SBOM,目前 SBOM 已成为供应链安全的基本需求。这一举措倒逼科技企业将开源安全嵌入产品全生命周期,DevSecOps 成为行业标配。

3. 其他国家

英国政府在 2014 年出台了首部《数字服务标准》^⑤,鼓励政府部门将开发的新软件代码适时开源,同时出台了《开放代码的安全注意事项指南》提供明确的指导。2023

① General Services Administration (2016). code.gov: Federal Source Code Platform. U.S. General Services Administration.

② Office of the Federal Register (2020). Title 48: Federal Acquisition Regulations (FAR) Part 1539.2. eCFR.

③ National Institute of Standards and Technology (2022). SP 800-161 Rev.2: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST.

④ U.S. General Services Administration (2016). Guideline on Public Procurement of Open Source Software. Digital.gov.

⑤ 2019 年经修改,但对开源的支持未变。

年颁布了政府采购法案（《Procurement Act 2023》），确立“开放、公平、透明、价值优先”采购原则，明确公共部门采购需平等对待开源与闭源软件，禁止歧视性条款。2024 年发布《公共采购中的开源软件指南》（Open Source Software in Public Procurement Guidance），2025 年颁布《国家采购政策声明》（National Procurement Policy Statement）的战略性采购政策说明，要求公共部门采购优先考虑“开源复用、成本效益、数字主权”，赋予开源“经济增长、社会价值、商业能力”采购意义。同时英国政府也建立了政府采购服务平台——英国皇家商务服务局（Crown Commercial Service, CCS），通过平台发布实操指南，明确开源采购合规流程、许可证选择与合同条款模板。CCS 在 2024 年发布了《开源软件政府采购框架》（Open Source Software Procurement Framework）^①，简化了开源软件公共部门采购流程，提供标准化合同与供应商清单。

韩国科学技术信息通信部（Ministry of Science and ICT, MSIT）是韩国开源政策顶层主管部门，负责制定与实施开源软件推广战略，于 2014 年颁布了《开源软件振兴计划》（Open Source Software Invigoration Plan, 2014–2025）的长期推广计划，明确公共部门开源优先采购、代码复用、开源社区支持三大目标，设定年度开源采购比例考核指标。并通过《开源促进法案 2020 修正案》（Software Promotion Act, Amendment 2020）奠定本国开源采购核心法律，其中第 25 条款强制要求国家软件研发项目成果（含源代码）必须公开，公共部门采购优先选用开源软件。目前计划在 2026 年前让所有公共机构采用基于 Linux 研发的开源 OpenOS 系统，该项目预计需要投入 3.5 亿韩元，系统更换后预计节省 72% 软件购买成本，同时还可降低技术支持成本。韩国信息通信产业振兴院每年安排大约 1200 万财政预算用于支持开源软件能力广场（OSSCP）中的开源软件服务企业。同时，韩国国家信息技术产业振兴院（NIPA）作为开源政策执行与社区支持机构，负责开源开发者扶持、项目孵化与安全审计，通过《开源软件扶持计划（2020–2025）》（Open Source Software Support Program, 2020–2025）为公共部门开源采购提供技术支持、安全评估与维护服务，降低采购与使用门槛。

印度的开源政府应用与采购较早。电子和信息技术部是其开源政策顶层制定机构，负责电子政务与开源软件推广。印度 2012 年出台了《国家信息技术规划》（National Policy on IT）顶层战略，将开源软件纳入数字基础设施建设核心，推动电子政务系统开源化，降低对闭源软件依赖。2015 年制定了政府采购使用开源软件的专门政策《印度政府开源软件采用政策》（Policy on Adoption of Open Source Software for Government of India 2015），并于 2024 再次修订，直接确立了“开源优先”强制原则，直接规定所有电子政务项目 RFP 必须包含开源选项；如果没有包含，则供应商需提供排除开源的书面理由；政府购买开源软件后将获得永久使用权、修改权与再分发权。

政府于 2015 年发起“数字印度”计划，要求政府使用开源软件，除非该领域没有开源软件或出于战略考虑才能使用闭源软件。此外，政府还发起了名为“FOSS4GOV”的挑战赛，鼓励本土开发者为政企客户构建开源的客户关系管理（CRM）和企业资源管理（ERP）软件。旨在资助和指导本土开发者和初创企业，为政府和企业部门开发开源软件解决方案，特别是在医疗、教育、农业和城市治理等领域。同时，印度中央公共采购平台（CPPP）

① Crown Commercial Service. (2024). Open Source Software Procurement Framework. Crown Commercial Service.

是国家级电子采购平台，负责公共采购电子化与开源采购落地。通过《开源软件采购手册 2021》（Open Source Software Procurement Manual, 2021）明确了开源采购标准化流程、评标标准与合同模板，要求所有中央部门通过 CPPP 平台进行开源软件采购。

综上所述，全球各国政府都围绕开源软件产品的公共产品属性及合规风险，通过政府采购立法促进开源应用、通过采购指南规避其合规风险，依靠政府不断推动开源发展战略，支持可持续发展。

五、我国政府采购促进开源发展与合规治理的政策障碍与不足

我国政府的开源促进与应用起步略晚，近年不断推进。《中华人民共和国国民经济和社会发展规划第十四个五年规划和 2035 年远景目标纲要》是促进开源软件发展的国家级战略规划，首次明确支持开源社区发展，并完善开源相关法律体系；《“十四五”数字经济发展规划》（国发〔2021〕29 号）提出支持具有自主核心技术的开源项目发展，推动创新资源共建共享；《“十四五”软件和信息技术服务业发展规划》（工信部，2021）明确繁荣国内开源生态是核心任务，陆续建立了《网络安全法》《数据安全法》《个人信息保护法》，构建开源软件安全与数据合规的法律框架；2021 年央行等五部委联合发布《关于规范金融业开源技术应用与发展的意见》率先提出在金融业开展开源技术应用；2024 年我国出台了首个国家标准 GB/T 43698-2024《网络安全技术软件供应链安全要求》（2024 年 11 月实施），覆盖了开源组件全生命周期的风险管理。同时出台文件支持开放原子开源基金会等全国性开源组织发展，推广自主开源协议（如木兰宽松许可证）。各地地方政府的配套政策也相继出台。

政府采购领域也开始接纳开源。我国软件产品政府采购规则体系主要由《政府采购法》《政府采购法实施条例》《政府采购货物和服务招标投标管理办法》《政府机关使用正版软件管理办法》组成，2025 年 9 月我国出台了《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号），明确规定基于国产开源根技术（如 OpenEuler、OpenHarmony、国产数据库）的信创软件，符合条件即认定为本国产品，支持开源产品采购；《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（财库〔2025〕30 号）进行细化指引。进一步对比发现，我国当前开源软件参与政府采购尚存政策障碍：

（一）开源“正版化”与审计逻辑冲突

政府采购需要通过政府审计。现行知识产权审计规则尚基于传统闭源软件的管理逻辑构建，政府审计中普遍要求商业授权、发票、合同作为软件“合法身份证明”，缺乏针对开源许可证的标准化审计流程与采信机制。开源许可证因其种类繁多、条款差异较大，与闭源软件“一次性授权、明确版权归属”的模式截然不同，审计人员难以快速界定不同许可证的合规边界，也缺乏统一的审计标准来核验许可证的合法性与有效性；另一方面，开源软件的分布式开发模式、多主体贡献特性，导致其版权归属链条复杂，审计过程中难以追溯每一段代码的原始授权来源，无法像闭源软件那样通过单一授权文件完成合规验证。此外，部分审计机构对开源许可证的认知存在偏差，将“开源免费”等同于“无版权、无授权”，误将开源许可证的开放授权属性解读为“缺乏明确知识产权归属”，

进而将其归类为“来源不明”。审计人员的认知，在一定程度上阻碍了开源软件在政府与企业采购中的推广应用，加剧了开源技术进入政府采购的合规顾虑，从而使开源软件在政务、国企场景中被直接排除。

（二）开源软件的“本国产品”“信创认定”标准不明确

《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）虽明确将基于国产开源根技术的软件纳入本国产品范畴，为开源类产品的国产化认定提供了政策依据，但相关认定细则的缺失导致实践中难以有效甄别。如对于企业基于国际开源项目进行二次开发后形成的软件，是否符合本国产品“在中国境内生产、实现属性改变”的核心要求，目前无统一判定标准，既未明确二次开发需达到的技术深度、自主研发占比，也未界定境内组件成本占比的具体阈值，导致不同评审机构、不同评审人员的认定结果存在较大差异，部分评审将简单的代码修改等同于“本国产品”，部分评审则因产品源于国际开源项目而直接否定其本国产品属性，形成认定乱象。这不仅严重影响了政府采购的公平性与规范性，也制约了开源软件在信创领域的健康发展。

（三）缺乏针对开源软件的技术规格、许可证类型、风险评估的政策指引

现有的政府采购相关法规均没有关于开源软件产品的许可证类型等技术规格的规范，也未对技术规格的标准认定、风险评估提供制度保障。在缺乏明确技术规格指南情形下，开源软件进入政府采购会以各种理由被拒绝，难以参加项目投标。2024年8月23日，我国颁布了《信息技术 开源 开源许可证框架》国家标准（GB/T 44272-2024），指出了开源项目选型参考框架，同时主要针对金融业开源技术术语、评估框架、软件应用评估规范、软件测评规范作出规定。这一规定如何与政府采购全面接轨，尚需时日。

（四）供应商资质规定不符合我国开源企业发展实际

我国《政府采购法》对于供应商的资质要求做了列举式规定：要求具有独立承担民事责任的能力、良好的商业信誉和健全的财务会计制度、必要的设备和专业技术能力、税收和社保记录良好、三年内没有重大违法记录等。而《全面与进步跨太平洋伙伴关系协定》（CPTPP）中允许设置的资质限定为“履行政府采购所需的法律资格和资金能力、商务条件和技术条件”。在我国，大多数开源软件企业往往是新设创新型企业，企业规模较小，人员较少，不一定有历年税收和社保缴纳的良好记录，而且开源企业起步时期的亏损期较长，往往缺乏良好的财务表现，因此较难满足该项要求。实务中很多中小企业只能做国企或大型企业中标项目的转包。

（五）“版权”与“自主知识产权”的规定不符合开源软件数字公共产品的属性

我国于2013年8月开始实施的《政府机关使用正版软件管理办法》并未废止，该办法规定，“各级政府机关的计算机办公设备及系统必须使用正版软件”，禁止使用未经授权和未经软件产业主管部门登记备案的软件。这一规定适用于传统闭源软件。开源软件是许可证授权模式下运行的软件，不存在传统意义上的“正版”，因此无法满足《政府机关使用正版软件管理办法》的管理规定，因而在很多地区无法进入政府采购。

（六）SBOM（物料清单）与许可证合规要求执行不到位

虽要求SBOM管理，但多数采购文件仅作原则性提及，无强制提交、审查、追溯机制，开源组件风险无法闭环。采购人、评审专家普遍缺乏开源许可证知识，对Copyleft（著

佐权)、兼容性、衍生作品义务等判断能力不足。我国政府采购政策的整体“开源意识”需要明确表达,同时建立全方位政策体系^①。

六、建立全方位政府采购政策体系的建议

数字公共产品的“公共品”属性使得该类产品的生产与管理需要充分借助政府力量。从相关国际协定内容与各国实践来看,推动开源软件发展主要需依靠各国国内的政策,其中政府采购是普遍的主导政策。有鉴于欧美国家“以开源战略为引导、以合规指导为保障”的成功实践,我国支持开源发展的政策应以“政府采购为主,合规保障同步”为路径,全面引导开源企业业务合规,帮助采购实体防范风险,才能共同推动开源软件的合规发展。政策建议如下:

(一) 明确开源软件进入政府采购的配套指南

紧跟国际开源政府采购发展趋势,针对开源软件进入政府采购出台专门的政策规定,或建立明确包含开源软件的政府采购目录。鉴于开源软件的使用风险,可联合科技部门制定开源软件选购解决方案,明确开源选项的优选地位,以降低政府采购支出,提高成本效益,统筹推进开源软件采购工作。

(二) 建立全周期风险评估及应对制度指引

根据“引入、使用、退出”的软件应用全生命周期,建设对应的安全管理机制。采购之前通过代码质量、许可证兼容性、开发者社区活跃度等指标,建立软件的风险评估模型,帮助采购实体选择开源软件;通过应用场景、信息系统等指标设定开源技术的风险等级,对应制定应对策略;使用中建议采购实体借助专业力量持续评估,通过常态化测试、代码安全性分析进行持续、动态验证,确保开源软件的安全性、可靠性,制定软件漏洞处置技术规范;规范建立开源软件应用台账(邱展彦等,2023)^②,实时掌握许可证变更等情况;建立企业集团开源风险合并管理制度。

同时,借助开源社区社会力量合作建立开源信息平台,通过全社会协作共享机制,将各阶段安全测评、日常漏洞处置过程中积累的开源软件漏洞纳入知识库中并定期发布。

(三) 建立许可证合规性检测认证平台

开源软件全生命周期均需要进行开源安全评估。2024 年 8 月 23 日,我国出台了《信息技术 开源 开源许可证框架》国家标准(GB/T 44272-2024),提出开源项目选型标准,可依托该标准,通过文本解读、许可证限制条款冲突性分析,构建许可证兼容性推导模型;或基于算法建模;基于人工智能技术建立许可证风险分析工具,建设许可证安全性检测平台,提供系统化、规模化的风险分析等标准化能力,促进采购实体对开源软件。

① 国务院于 2022 年发布的《国务院关于加强数字政府建设的指导意见》对数字公共产品有所涉及,提出要“扩大数字基础设施覆盖范围,优化数字公共产品供给,加快消除区域间‘数字鸿沟’”,但其中提到的“数字公共产品”更多指代政府提供的、供公众使用的数字基础设施、数字平台、数字服务等,与联合国定义下的当前国际上广泛讨论的数字公共产品内涵存在一定差异。

② 邱展彦、潘雪苗、谭青:《金融业开源软件应用与风险研究——以广东省银行业应用情况为例》,《金融科技时代》2023 年第 12 期,第 40—43 页。

（四）出台软件物料标准

借鉴国际经验，研制并推广软件物料清单统一标准，编制可反映软件关键代码构成和开源供应链的物料清单，规范物料清单的组成和呈现方式，推进开源软件供应链标准化工作，通过在关键信息基础设施中的示范应用，将软件物料清单应用落实于软件工程生命周期中，全链条加强开源软件供应链可追溯性，有效缓释开源软件供应链风险。

（五）大力借助基金会及行业组织的技术力量

开源基金会作为非营利性组织，专门为开源项目提供资金、技术、市场、风险警示等全方位支持。一些使用基础广但亏损的项目可以托管基金会运维，基金会一般有完整的服务体系，以满足开源项目或社区在不同生命周期的需求。基金会对于开源项目的整体发展非常重要。

与国外依靠大企业借助基金会推动开源项目发展路径不同的是，我国开源企业发展起步较晚，主要是民间技术人士的自发行为，由此推动开源行业协会组织形成各地开源企业自发的业务领导机构，负责组织行业活动，为政府提供行业信息，推进行业自治，需要予以支持。

各种研究显示，开源软件已经是当今每个应用程序的基础设施，有效的开源软件合规治理对于成功的软件应用至关重要，而政府采购是其中核心的政策工具。

Compliance Governance of Open Source Software and Government Procurement

WU Zhanxia, ZHANG Guofeng, ZHU Qigan

Abstract: China's government explicitly incorporated the national science and technology strategy of supporting open source development into the 14th Five-Year Plan. Since their launch, DeepSeek and OpenClaw have gained rapid nationwide popularity and become major suppliers of digital public goods in the software industry. Facts have proven that open source has exerted profound impacts not only at the technical level, but also posed new challenges and opportunities to the government policies. Starting with the definition and inherent characteristics of open source, this paper elaborates that open source possesses the attributes of digital public goods. It points out that government procurement can drive the development of open source software by facilitating technological innovation, guiding market demand, fostering a fair competitive environment, advancing compliance development, and enhancing supply chain security. Meanwhile, it analyzes potential compliance risks in the government procurement of open source software covering legal, technical, license, intellectual property and supply chain dimensions. Drawing on the risk management experience of major countries in stimulating the development of open digital public goods, and combining comparative analysis of international government procurement rules and global policy practices, this paper puts forward suggestions on compliance governance for the government procurement of open source software .

Keywords: digital public goods, open source compliance, government procurement

（责任编辑：陈 彬）