

主权 AI

一、含义

主权人工智能是指国家通过自主掌控数据、算法、算力等核心要素，建立不受外部制约的人工智能生态体系。它代表着国家对人工智能技术和相关数据的独立控制，包括部署和运营人工智能技术，构建硬件和软件基础设施，以及掌握运营和保护数据的政策和人员。

通俗来说，就是国家支持人工智能基础设施建设，用符合本国文化和思维方式等的数据训练大模型，支持本地产品形成生态系统，体现该国的文化、社会和伦理价值观，且符合本国主流价值观。

二、关联知识

与国家主权的关系：人工智能技术已成为国家认同和连续性的一部分，主权人工智能是新时代下国家主权的延伸。国家对人工智能技术和数据的控制，如同对领土、资源等方面的主权一样，关乎国家的独立自主和安全。

与经济的关系：发展主权人工智能可促进国家经济发展。一方面，它能催生国家级算力需求，强化智算中心等基础设施建设，而智算中心作为新质生产力的引擎，有望带来巨大的经济效益。另一方面，通过自主掌控人工智能技术，可支撑产业升级，确保关键领域不受制于人，增强国家在全球产业链中的竞争力，促进本土企业成长，创造就业机会。

与文化保护的关系：主权人工智能旨在反映一个国家的身份和价值观，确保人工智能应用尊重和增强该国的文化和语言遗产。各国可在国内数据上用本国语言构建大型语言模型，支持当地研究和企业生态系统，保护和传承本国文化，避免文化被外来人工智能应用所同化或忽视。

与国家安全的关系：在军事领域，人工智能可用于情报分析、作战决策等，若本国军事人工智能系统依赖国外技术，战时可能面临系统被敌方控制或数据被窃取的风险，危及国家安全。在社会治理方面，自主研发的人工智能系统可更好地服务于公共安全、交通管理等领域，维护社会稳定，保障国家安全。

与国际竞争的关系：全球数字化浪潮下，AI 在经济、军事等领域的权力属性显现，主权人工智能领域的竞争激烈。各国积极发展主权人工智能，进行大量投资，政府与科技公司合作支持相关计划。算力自主可控是国家信息安全和技术独立的重要保障，国家需在芯片设计、制造和数据管理等关键环节自主创新，以在国际竞争中占据有利地位。

与伦理规范的关系：主权人工智能的发展需要确立伦理规范，确保人工智能系统的透明度、公平性、安全性和问责制。目前存在一些伦理问题，如人工智能决策过程缺乏透明度（“黑

匣子”运行)，可能延续并放大数据集中的偏见，产出歧视性结果等。国家需要建立完善的监管框架，关注隐私、数据保护、网络安全和人工智能的道德使用等问题。