人工智能治理中的技术自主权*

赵精武

【摘　　要】当前，处于全新阶段的人工智能等信息技术构成了国家数字经济崛起的核心驱动力，国际竞争也相应日趋激烈。这一技术实践现状对网络主权内容提出了全新问题：网络主权能否延伸适用于人工智能治理领域？网络主权的具体内容是以网络空间概念为基础的，而网络主权在技术维度的内容延伸也是以构成网络空间底层支撑的信息技术为基础的。这种技术维度的内容实际上延续了从威斯特伐利亚体系下的国家主权到网络主权的延伸逻辑，即构成主权核心要素的国家安全与发展的内涵有所变化。由于人工智能等信息技术关系主权国家的网络安全和技术发展，故而网络主权在技术维度的内容延伸表现为技术自主权。技术自主权指主权国家有权独立自主决定本国的信息技术创新发展的管理活动，具体包括自主管理权、自主合作权和同等反制权，其核心目标是保障各个国家均享有独立自主的技术发展能力。

【关 键 词】网络主权　国家主权　技术自主权　人工智能国际治理

【作者简介】赵精武，法学博士，北京航空航天大学法学院副教授。

【中图分类号】D912.170.1　　【文献标识码】A

【文章编号】2097－1125（2025）01－0094－19

一、问题的提出

在数字时代，网络信息技术的创新发展极大地改变了国家主权的基本内涵，以往不被重视的网络空间转而成为“第五领土”，网络主权概念愈

* 本文系北京市社会科学基金青年学术带头人项目“人工智能综合治理体系：安全、创新与保障”（24DTR051）的阶段性成果。

发被国际社会重视。特别是在习近平总书记提出“网络空间命运共同体”这一关键性的中国方案后，网络主权开始成为各国网络合作治理的现实基础。虽然美国等西方国家仍旧奉行“对外指责他国封禁、阻断全球网络连接，对内强化网络空间政府治理”的双重标准，但这并不能阻碍网络主权在网络安全全球合作、数据跨境传输治理等重点领域发挥促进开放合作的核心功能。

然而，网络空间独有的跨地域性、非实体性等特征，也使网络空间的竞争与博弈呈现新的发展趋势：网络空间依赖的信息技术开始成为国际规则制定的重点事项。信息技术的实际范围早已不再局限于数据传输、网络通信等技术类型，而是延伸至人工智能等技术领域。以 ChatGPT、Sora 等为代表的人工智能产品实现了跨越式创新，人工智能也成为全球各国数字经济发展的核心产业之一。在国际竞争中，美国等西方国家试图通过限制芯片出口钳制算力资源生产、以国家安全名目阻断数据跨境流动等方式对全球人工智能技术创新实施在产业链和供应链层面的竞争博弈措施。这种技术竞争现象也产生了一个新问题：网络主权能否延伸适用至人工智能技术治理领域？

在主流观点中，网络主权概念往往与网络安全和数据安全密切相关，是一个国家对本国网络空间实施独立自主的治理措施最为核心的法律依据。所谓“网络空间”通常指向依托网络通信信息形成的虚拟空间，从文义理解来看，“网络空间”的概念内涵难以推导至网络空间内的信息技术，特别是一项具体的信息技术及其治理体系何以成为网络主权的组成部分更是缺乏相应的证成依据。基于此种网络空间的概念理解，网络主权与技术治理似乎属于两个不同维度的研究议题。但是，国外学者已经注意到，主权概念争议以价值观的方式转移到了数字领域，进而导致主权的领土内涵失去影响力。[①] 此时，网络主权强调的网络安全目标与技术治理强调的技术安全目标可能存在主权价值层面的归属关系。因此，为了回应这一系列争议问题，有必要从三个方面逐次建构网络主权在人工智能技术治理领域的适用理论：一是网络主权指向的网络空间范围如何划定，网络主权概念是否发生内涵和外延层面的变动，以及这种变动是否足以证成网络主权在技术治理领域的延伸适用；二是网络主权在技术治理领域的适用究竟意味着新型主权内容的产生，还是传统主权内容的扩张；三是基于“新”或“旧”的主权内容，在网络主权框架下，人工智能治理规则呈现何种体系框架形态。

① 参见 Dana Burchardt, Does Digitalization Change International Law Structurally?, *German Law Journal*, Vol. 24 (3), 2023, p. 458。

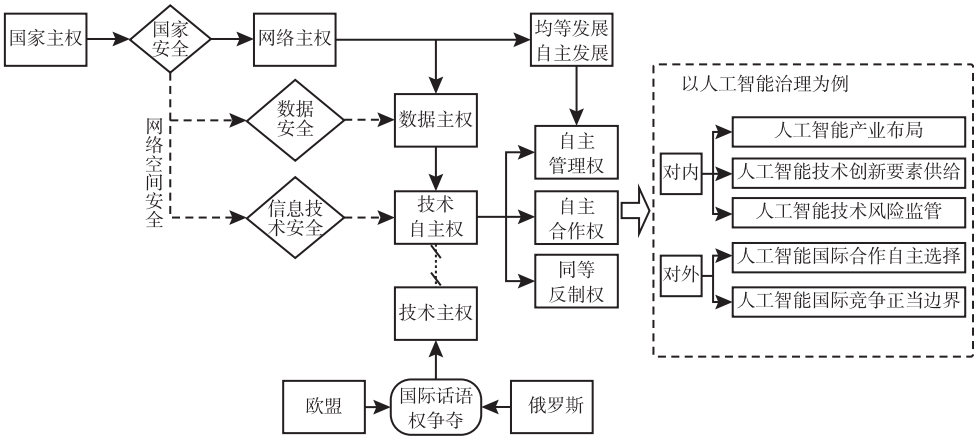

图 1　网络主权在技术领域的延伸适用路径

二、网络主权在技术治理领域的延伸适用：网络空间的概念重述

审视网络主权内容的演进历程可以发现，它始终以网络空间治理为中心。这是因为网络空间并非一个固定不变的概念，而是会随着网络通信技术、网络安全态势、底层信息技术等诸多要素的变化而发生变化，故而重新厘清网络空间概念延伸的实践趋势确有必要。

（一）网络主权的基本内涵与演进发展

网络主权概念的形成实际上是一个动态发展的过程。在互联网发展初期，网络通信技术的发展水平与当下相去甚远，故而在过去的治理模式中，网络空间大多被视为线下业务延伸至线上业务的“经营场所”或“活动空间”，网络空间安全问题也被划归为纯粹的技术安全问题。但是，在经历了从大数据、云计算到区块链、人工智能等信息技术创新浪潮之后，各国逐渐开始意识到网络空间安全对国家经济安全和社会稳定的重要意义，网络空间安全正在成为国家安全的重要内容。随之而来的是各国开始在网络空间推行各自的治理主张，网络主权、多利益攸关方治理、全球公域治理等治理主张相继被提出，网络空间国际治理规则呈现碎片化和阵营化的发展趋势。所谓的碎片化，指各国基于本国国家安全的考量，在国内法层面制定网络空间治理立法体系。这些国内法的内容存在不同程度的冲突和矛盾，彼此之间难以兼容，网络空间国际治理规则也呈现“割据”状态。所谓的阵营化，指网络空间国际治理被政治冲突主导，特别是美西方奉行的网络空间自由主义和

中俄等国坚持的网络空间主权治理方案存在较大争议，网络空间国际治理的阵营划分特征趋于显著。究其根本，围绕网络空间治理的争议焦点在于，一个国家对网络空间究竟享有何种程度的管控能力。

这个争议焦点也延伸出网络主权肯定论与网络主权否定论的对立。时至今日，网络主权概念已被国际社会普遍接受，特别是在我国提出“网络空间命运共同体”等理念后，网络主权理念已成为大部分国家制定本国网络空间立法的正当性基础之一。然而，网络主权肯定论与否定论的争论并没有完全终结，美国追求的美国占据全球技术领先地位的理念依然在以不同的方式影响网络空间国际治理的统一进程。在网络主权的概念提出之初，美国等西方国家为了巩固自身在网络空间治理的优势地位，意图通过“网络空间属于全球公共领域”“网络空间自由不应当被主权国家不当干预”等事由将网络空间排除在主权管辖范围之外。从表面上看，这种治理倾向似乎是为了贴合网络空间跨地域性等技术特征而做出的“合理”规划；实际上，基于“网络空间自由”“网络全球公域”提出的多利益攸关方治理和全球公域治理不过是为了维护美国等西方国家既有的国际经济政治秩序。因为两种治理理论背后依赖的诸如 ICANN 等非国家治理组织实质上依然受到美国的影响，更有学者直接指出，“美国政府从未真正放弃网络全球治理的主导权”。[①] 美国正是通过这些治理主张将自身的“长臂管辖”正当化，无视主权平等，将其国内的司法管辖权无限扩大。

网络主权肯定论则更加强调一个主权国家对网络空间实施各项独立自主治理活动的正当性。多数观点认为网络主权属于国家主权在网络空间中的概念延伸，相应地，网络主权内容也应当以传统主权包含的管辖权、独立权、自卫权、平等权四项内容为基础，但相关的主权内容存在不同观点。传统主权延续论在既有的四项内容的基础上解释国家对网络空间的主权内容，如管辖权指“主权国家对网络疆域内一些人、事、物以及网络疆域外的本国人实行管辖的权力”。[②] 国家管控论将网络主权界定为公权，并指出其内容是“国家主权中对信息资产和行为进行控制管辖、管理监督的部分”。[③] 对内对外主权说强调网络主权表现为“按国内法与国际认可或公认的国际法对网络实施管理与管辖”，禁止和阻断他国对本国网络治理活动的任何干涉。[④] 从

① 方菲：《网络主权研究：理论与实践》，武汉大学出版社 2023 年版，第 38 页。

② 参见陈星：《论网络空间主权的理论基础与中国方案》，《甘肃社会科学》2022 年第 3 期，第 115～116 页。

③ 林婧：《论国际法协调互联网权利与网络主权的进路反思与重构》，《中国科技论坛》2019 年第 9 期，第 86 页。

④ 参见程卫东：《网络主权否定论批判》，《欧洲研究》2018 年第 5 期，第 75 页。

我国 2016 年发布的《国家网络空间安全战略》、[①] 2017 年发布的《网络空间国际合作战略》、[②] 2020 年发布的《网络主权：理论与实践（2.0 版）》以及 2023 年发布的《构建网络空间命运共同体 更好造福世界各国人民》的内容来看，我国主张的网络主权内容主要包括两个方面：一方面，网络主权作为国家主权的自然延伸，包含独立权、平等权、管辖权和防卫权等权利；另一方面，网络主权意味着本国有权拒绝他国对本国网络空间治理活动实施任何形式的干预。

（二）网络主权的实践基础：网络空间的概念界定

无论是规范性文件提及的网络主权，还是学界探讨的网络主权，其核心内容均以网络空间的特殊性为前提，并且基于这种特殊性的不同认知，也延伸出不同的网络主权内容。以美国为代表的西方国家推崇的“多利益攸关方”等治理模式实际上是将网络空间的法律性质解释为全球公共空间。同时，美国等西方国家基于网络空间的开放性、无边界性、泛用性等技术特征，始终强调在网络空间内的各类活动应当处于国家管控范围，即所谓的“网络自由”。因此，在相当一段时间内，各类主权国家、政府间国际组织以及私营组织纷纷参与至网络空间治理活动中，[③] 这也是所谓的“多利益攸关方”治理模式。与通常讨论的多元主体治理模式不同的是，“多利益攸关方”治理模式否定了政府管理的主导地位，强调政府、私营部门、社会公众等多方主体在网络空间国际治理活动中具有平等地位。然而，这种表面的“民主治理”只不过是另一种国际话语权争夺方式。整个网络空间的基础技术架构离不开根服务器的支撑，而现实情况是，全球管理互联网主目录的大

① 《国家网络空间安全战略》提及“尊重维护网络空间主权”，并明确“网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。”

② 《网络空间国际合作战略》在主权原则部分提及：“各国政府有权依法管网，对本国境内信息通信基础设施和资源、信息通信活动拥有管辖权，有权保护本国信息系统和信息资源免受威胁、干扰、攻击和破坏，保障公民在网络空间的合法权益。各国政府有权制定本国互联网公共政策和法律法规，不受任何外来干预。各国在根据主权平等原则行使自身权利的同时，也需履行相应的义务。各国不得利用信息通信技术干涉别国内政，不得利用自身优势损害别国信息通信技术产品和服务供应链安全。”

③ 参见罗楚湘：《网络空间国际治理中国方案的形成、遵循与路径》，《广西社会科学》2024 年第 1 期，第 112 页。

多数服务器（包括主根服务器）被放置在美国，只有英国、瑞典、日本各有1台根服务器。[①] 可见，美国在技术层面拥有绝对优势，完全有能力掌控网络空间的存在与否，例如，在伊拉克战争期间，美国通过根服务器彻底关闭了伊拉克的网络。

然而，随着网络空间国际治理实践的持续深入，越来越多的国家已经意识到网络空间并不是所谓的“全球公域”或“自由空间”，美国也在持续强化国家对网络空间的管控能力，并基于国家安全等事由对网络空间的经营活动、科技创新投资等行为做出一系列限制性约束。在现有的学说中，主要存在两类认定网络空间的法律性质的学说。一类是网络领土说，该类学说主张将网络空间拟制为“领土”，[②] 或称之为“领网”“第五疆界”，[③] 其内在逻辑是将网络空间视为国家主权的自然延伸，作为有形性和无形性综合体的领网是“一国领土的重要组成部分”。[④] 另一类是新空间说，该类学说主张将网络空间解释为一个由信息技术、物理基础设施等形成的虚拟空间，最常见的解释逻辑是按照计算机网络通信分层结构对网络空间的构成要素进行划分。例如，将网络空间视为由社会域、逻辑网络域、物理域构成的多重场域，从各个场域延伸了不同的主权内容；[⑤] 或将网络空间解释为由物理层（网络基础设施）、逻辑层（代码与算法）、内容层三个层次相互重叠组成，进而推导得出网络空间具有跨越性和安全性特征，并分别对应网络空间命运共同体与总体国家安全观双重网络空间立法路径。在《网络行动国际法塔林手册2.0版》中，网络空间被细分为基础设施层、逻辑、基础资源、数据层以及社会应用五个层面，并由此延伸出网络主权的具体内容。

网络领土说与新空间说的核心差异在于网络空间究竟是否构成在传统国家主权概念中领土的延伸性概念或者类似领土的概念，而这一差异将会导致两类学说对网络主权内容的解释路径有所差别：网络领土说实际上是将网络主权视为领土主权的组成部分或者延伸内容，故而相应的主权内容也是基于领土主权进行“改造”；新空间说更加侧重网络空间的技术特征，通过对网

① 参见陈星：《论网络空间主权的理论基础与中国方案》，《甘肃社会科学》2022年第3期，第118页。

② 参见方滨兴、邹鹏、朱诗兵：《网络空间主权研究》，《中国工程科学》2016年第6期，第1~6页。

③ 参见余建川：《欧盟网络安全建设的新近发展及对我国的启示——基于〈欧盟数字十年网络安全战略〉的分析》，《情报杂志》2022年第3期，第89页。

④ 盛文楷、肖光荣：《网络空间国家主权研究的回顾与思考——兼论结构功能主义分析框架的应用》，《中国矿业大学学报》（社会科学版）2020年第2期，第148页。

⑤ 参见许开轶、俞润泽：《基于多重场域原理的网络空间主权生成逻辑》，《社会科学研究》2020年第2期，第50~52页。

络空间各类支撑要素的梳理和归类，进而得出在技术架构中各个环节对应的具体主权内容。然而，这种差异性仅属于观察视角层面，其核心目的是对宽泛意义上的网络空间做出限定。早期网络主权受到质疑的原因之一是网络空间属于一个开放式的虚拟空间，不同于传统主权观念中的领土、领海、领空等概念，其本身缺乏足够明确的空间边界。因此，网络主权质疑者认为在实践层面难以证成一个国家对开放且不具有明显边界的虚拟空间具有实质性的管控能力，这会使主权涵盖范围相当不确定。在之后的网络主权学理讨论中，学者们开始逐渐关注对网络空间的概念界定和具体边界的划定，在确保传统主权理论能够继续适用的同时，细化网络主权这一新型主权类型的具体内容。

（三）网络空间的概念延伸：新发展趋势下的技术要素

随着网络空间治理实践的不断丰富，新空间说反而更加契合网络信息技术的发展趋势，能够基于网络空间的构成要素动态性地延伸出网络主权的新内容。例如，数据主权、技术主权等概念的提出是基于数据、信息技术是支撑网络空间正常运行的技术要素的。现有的各类网络空间概念界定方式均无法将客观模糊的网络空间边界清晰化，而是结合网络空间自身的发展趋势、技术特征建构相应的主权适用范围。事实上，部分国外学者也通过数据本地化、删除请求、屏蔽外国网站等方式建构其网络空间边界与地理层面领土边界的关联性。[①] 因此，网络空间的概念应当包括组成要素、边界要素以及管控要素三个维度的基本内涵。在组成要素层面，网络空间是由网络通信关键信息基础设施、网络信息、网络通信信息技术组成的虚拟空间，故而网络主权的基本内涵也涉及网络运行安全、关键信息基础设施运行安全、数据安全以及技术安全四项内容。在边界要素层面，网络空间的边界认定并非依循领土、领海等传统概念背后的物理边界划分，而是通过网络行为主体、网络行为发生地、网络设施所在地等建构一个虚拟化的活动场所。网络主权之所以被视为国家主权的延伸，是因为这些网络空间活动直接关系国家安全和社会发展，并且行为主体、行为发生地、网络设施所在地等要素也与传统主权概念的地理边界存在一定程度的关联性。在管控要素层面，相较通常意义上的网络空间概念，网络主权意义上的网络空间直接关涉一个国家的总体安全，国家管控网络空间的目的并不是限制所谓的网络自由，而是网络空间本身完全可以成为颠覆国家主权的攻击路径。这种攻击模式具有典型的隐蔽性、匿名性，因此，网络安全攻击对国家主权安全的威胁程度远超以往。总而言之，网络空间指由各项网络通信物理设备、信息技术、数据等组成的虚拟空间，该类空间承载了一个国家数字经济发展的各项活动，一旦遭受网络攻

① 参见 Beth A. Simmons and Rachel A. Hulvey, Cyber Borders: Exercising State Sovereignty Online, *Temple Law Review*, Vol. 95 (4), 2023, pp. 627 – 638。

击、服务中断等威胁，便能够直接影响该国的国家安全和社会稳定。

这种网络空间的概念界定既延续了既有学说的物理层、软件层、应用层等层次划分特征，也为国家主权延伸至网络空间的范围和边界提供了正当性基础。网络主权的内容演进与网络空间的动态发展同步进行，信息技术是网络空间的重要组成内容，相应的信息技术创新治理和管控活动显然也成为网络主权的重要内容。事实上，欧洲部分国家已经开始推行欧洲模式的技术主权概念，例如，德国联邦教育与研究部在2021年9月发布《技术主权塑造未来》（*Technologisch souverän die Zukunft gestalten*），它推崇的技术主权概念实际上是经济、技术、安全等多重治理目标的整合，如扩大“工业4.0”计划、实施先进系统工程等，[①] 目的是在先进产业中减少对外依赖并提振德国及欧盟的技术研发和自主创新能力。这种技术主权概念反映了欧盟成员国在主权层面自主发展高新技术产业的治理主张，[②] 虽然该概念并没有局限于数字经济领域，但是也间接体现了欧盟国家认同技术自主发展对国家主权的重要性。在制度层面，虽然网络主权与信息技术治理实属两个议题，但是在网络空间层面，信息技术作为支撑网络空间安全和发展的重要工具，理应被纳入网络主权的基本内涵。只不过这种网络主权在信息技术维度的内容延伸以网络空间概念的扩张为基础：在网络主权概念兴起之初，争议焦点表现为“网络主权是否存在”；而在网络主权概念逐渐得到认可后，争议焦点则表现为“网络主权的适用范围如何认定”。这种从“存在论”到“边界论”的争议转变与从“自由公域”到“主权空间”的网络空间概念转变保持同步，但更为核心的内因在于，网络空间对一个国家的主权发展的影响方式发生了变化。时至今日，网络空间对国家安全的重要意义不仅包括网络空间安全，而且包括网络空间自主发展，这种自主发展的内涵显然包括网络空间活动的合法有序开展和网络空间技术自主创新。换言之，信息技术创新发展不仅涉及网络空间安全能力的提升，而且涉及网络空间活动能否按照一国主权意志自主进行，故而当下网络主权的基本内容存在向信息技术创新领域延伸的必要性与正当性。

三、网络主权在技术维度的内容延伸：技术自主权

在概念层面，网络空间并不局限于网络通信技术形成的虚拟空间，还包

① 参见德国联邦教育与研究部（BMBF）官网，https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/24032_Impulspapier_zur_technologischen_Souveraenitaet.html，2024年6月11日。

② 欧盟在《塑造欧洲的数字未来》《欧洲数字战略》《欧洲人工智能白皮书》中均提及“技术主权”概念。

括与网络空间组成部分相关的数据和基础信息技术。在审视网络主权、网络空间概念演进历程的基础上，以数据主权的形成与发展为比照对象，可以发现网络主权在技术维度同样延伸得出了全新的主权内容。

（一）网络主权内容延伸的逻辑审视：以数据主权为例

网络主权概念最初是为了解决国家管控网络空间以及国际网络空间治理合作的正当性基础问题而被提出的，故而网络主权的相当一部分内容是网络空间安全保障机制。随着网络空间治理活动的深入，网络空间概念的内涵从虚拟技术空间延伸至多维度的主权空间，网络主权的内容也从“管辖权、独立权、自卫权、平等权”的架构拓展至数据安全治理、技术自主发展等领域。这种内容拓展最为典型的观点便是数据主权的提出，它主张国家有权独立管辖和治理网络空间数据及其相关处理活动。数据主权的概念在本质上是将网络安全与数据安全分割，强调数据安全治理活动的特殊性，进而提出有别于网络主权内容的数据治理架构。虽然存在“大数据主权”“信息主权”“数据主权”等不同的概念指称，但这些概念实际上都是国家主权在不同阶段的“弹性延伸”，[①] 例如，“大数据主权”被解释为国家主权在数据空间的集中体现，是生存空间数字化、大数据资源化等因素的作用结果；[②] “信息主权”被解释为“主权在信息空间中的自然延伸”。[③] 这些解释路径以数据处理活动对国家安全的作用方式为基础，强调主权国家管控数据的必要性和正当性，[④] 进而推论至跨境数据传输、数据本地化存储、数字贸易活动监管等制度内容。

然而，关于网络主权与数据主权之间的逻辑关系也存在并列说和包含说的争议。并列说以数据安全的特殊性为论据，主张单独界定数据主权的基本内涵，[⑤] 而这些内涵界定往往采用与网络主权相似的界定模式；包含说主张将数据主权视为网络主权在数据治理领域的具体表现形式。[⑥] 学界多数意见

① 参见冉从敬、刘妍：《数据主权的理论谱系》，《武汉大学学报》（哲学社会科学版）2022 年第 6 期，第 22 页。

② 参见伍小乐：《论大数据主权的生成逻辑》，《湘潭大学学报》（哲学社会科学版）2022 年第 5 期，第 21 页。

③ 参见牛博文：《自由与秩序：信息主权法律规制的价值博弈》，《学术交流》2016 年第 2 期，第 80 页。

④ 参见 Neha Mishra, Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?, *World Trade Review*, Vol. 19 (3), 2020, p. 346。

⑤ 参见齐爱民、盘佳：《数据权、数据主权的确立与大数据保护的基本原则》，《苏州大学学报》（哲学社会科学版）2015 年第 1 期，第 68 页。

⑥ 参见陈斌彬、王斌楠：《数据主权视阈下我国数据出境的法律规制及完善》，《华侨大学学报》（哲学社会科学版）2024 年第 2 期，第 51～52 页。

支持包含说，因为并列说始终无法解释两种主权概念的边界究竟如何确定。而且，数据主权指向的数据处理活动在本质上属于网络空间活动范畴，在实践中，数据安全治理与网络安全治理也处于交叉重叠的关联状态，即便是学理层面的数字法学论证也将网络安全和数据安全等而视之。① 更重要的是，倘若将数据主权与网络主权视为同一维度的主权概念，可能导致产生诸如通信主权、信息技术主权等类似概念，这无疑使在威斯特伐利亚体系下的国家主权概念被异化、被肢解。虽然存在部分观点主张数据主权的适用范围还包括与数据相关的算法、信息技术、服务提供商等，② 但是这种观点无限扩大了数据主权的内涵，脱离了“主权”概念形成的法理基础。一旦将数据、技术、算法等要素统一纳入数据主权的概念范畴，将会使数据主权与网络主权存在大范围的内容重合。事实上，数据主权作为主权概念子属类别，也因“数据不具有作为国家主权客体的适格性”“导致主权概念的过度延展”等问题而受到质疑，③ 故而数据主权更适宜被视为网络主权在数据治理维度的自然延伸。

从网络主权到数据主权的演进，在本质上是一种治理对象和治理目标明确化的过程。诚然，相较狭义层面的网络安全，数据安全治理活动具有特殊性，但这种特殊性并不足以支撑数据主权成为独立的主权类型。在治理对象层面，数据主权主要针对的是跨境数据传输监管等数据安全监管活动。④ 在治理目标层面，数据主权主要实现的是对内和对外两个方面的数据治理效果，即对内确保数据安全有序流动，对外确保有独立自主决定本国数据治理的能力。因此，数据主权也常被作为反击美国“长臂管辖”、电子跨境取证等主权冲突问题的理论基础。⑤ 部分学者将现有的数据主权工具价值观点总结为“保障国家数据安全”“协调网络空间的法律冲突”“巩固国家在数字空间的权威”“维持国家在数据领域的竞争优势”⑥ 等。由此观之，数据主

① 参见赵精武、周瑞珏：《论数字法学研究范式的转向：风险体系化治理》，《求是学刊》2024 年第 4 期，第 141 页。

② 参见孙南翔、张晓君：《论数据主权——基于虚拟空间博弈与合作的考察》，《太平洋学报》2015 年第 2 期，第 65 页。

③ 参见陈曦笛：《法律视角下数据主权的理念解构与理性重构》，《中国流通经济》2022 年第 7 期，第 120 ~ 121 页。

④ 参见乔晗、徐君如：《基于 LDA 模型与政策工具的中国数据主权政策研究》，《中国科学院院刊》2024 年第 3 期，第 504 ~ 505 页。

⑤ 参见赵海乐：《论美国跨境电子取证与我国数据安全立法的冲突与对策》，《安徽大学学报》（哲社版）2024 年第 1 期，第 101 页。

⑥ 刘妍：《当我们谈论数据主权时我们在谈论什么？——从文献综述出发》，《图书情报知识》2023 年第 6 期，第 33 ~ 34 页。

权不是学界为“蹭热点”而提出的“学术热点词汇”，而是为了解决网络空间国际治理在数据领域的特殊问题，只不过部分学者误将数据主权的体系定位解释为独立主权类型。这种网络主权内容延伸的内在逻辑在本质上是以特定的治理目标和治理对象为起点，遵循一般性的网络空间安全治理逻辑，通过延伸特殊的主权内容和规则体系解决网络空间治理的特殊议题。

（二）网络主权在技术维度的内容延伸：技术自主权的证成

网络主权在数据治理维度的内容延伸同样适用于技术治理领域。域外兴起的技术主权概念便是网络主权在技术维度内容延伸的代表之一，只不过这种主权概念具有明显的国际政治博弈属性和区域特征。“技术主权”“数字主权”等概念在欧洲的兴起实际上与欧盟及其成员国追求数字领域的战略自主目标和建构欧盟数字化单一市场无不相关。① 这些概念亦是一种欧盟范围内的“整体性”主权意识，强调将欧盟网络空间治理理念和治理规则国际化，故而也有学者将欧盟的这些主权概念内涵归结为“制度层面的规范性权力”、“技术层面的自主技术能力”和“观念层面的文化软实力”三个层面。② 类似地，俄罗斯也提出了“科技主权”“技术主权”等概念，③ 其目的主要是保障本国获取影响国家安全、经济稳定的关键科技研发能力，部分学者也将其总结为“保障关键产品和服务的生产”“稳固国际技术交流与合作的谈判地位”“培育未来产业发展竞争力”等。④ 尽管在国家利益层面，欧盟和俄罗斯存在显著差异，但二者的技术主权概念均指向对内的科技创新安全和对外的科技竞争能力。这种共性不是偶然，而是因为科技创新能力和自主控制能力在国际网络空间博弈中愈发重要，加之美国近年来的科技竞争政策也延伸至数据资源和科技创新供应链的控制，欧盟和俄罗斯均选择将技术主权作为强化国际规则话语权的重要依托。

技术主权的共性特征实际上为网络主权在技术维度的内容延伸提供了国际共识层面的正当性基础。在人工智能等信息技术及其相关产业成为国家经济发展重要支柱的大背景下，技术主权概念更加侧重的是一个国家对自身科技自主创新能力的保障以及抵御外部以科技创新供应链等为目标的不当干

① 参见忻华：《“欧洲经济主权与技术主权”的战略内涵分析》，《欧洲研究》2020 年第 4 期，第 3 ~ 9 页。

② 参见蔡翠红、张若扬：《“技术主权”和“数字主权”话语下的欧盟数字化转型战略》，《国际政治研究》2022 年第 1 期，第 21 页。

③ 例如，俄罗斯 2023 年 4 月 15 日的第 6603 号决议提出，俄罗斯政府将继续努力保障技术主权，重点开展航空工业、汽车工业等 13 个重点领域的科技创新。参见俄罗斯政府官网，http：//government. ru/news/48272/，2024 年 6 月 11 日。

④ 参见高际香：《大国科技竞争背景下俄罗斯强化技术主权的实践与启示》，《俄罗斯东欧中亚研究》2024 年第 1 期，第 96 页。

预。客观而言，一国的科技创新发展治理属于典型的内政范畴，并非典型的国家主权议题。但是，由于近年来美国越来越频繁的“阵营式”科技创业政策，全球科技创新供应链处于不确定状态。例如，美国为了强化自身的全球科技实力领先地位，借由国家安全等名义，将对外投资活动、知识产权贸易活动等与科技发展相关的国际议题纳入主权框架下，先后出台《外国投资风险评估现代化法案》（Foreign Investment Risk Review Modernization Act）、[①]《2022 年芯片与科学法案》（CHIPS and Science Act 2022）、第 14083 号总统行政令等规范性文件。这些文件均强调强化美国的科技领导力、供应链韧性和安全能力，并将中国的科技创新视为最大威胁。这一点在网络空间治理中早已有所体现，部分学者认为这种阵营化治理趋势会使与网络治理相关的议题遭受连锁反应。[②] 因此，在科技创新维度增设符合国际共识的主权内容确有其正当性，这不仅有利于建构新型的国际科技合作发展秩序，而且能够有效避免网络空间治理阵营化趋势可能导致的互联网“巴尔干化”。

为了避免在概念称谓上与网络主权等概念发生冲突，并结合该类主权的功能定位来看，将宽泛意义上的“技术主权”称为“技术自主权”更适宜。诚如前文提及的，从网络主权到数据主权的延伸逻辑是以特定的治理目标和治理对象为起点，相对地，从网络主权到技术主权的延伸逻辑同样如此。在治理目标层面，各国均认同在主权框架下对本国科技创新能力的维护和对他国损害或威胁本国科技创新能力的抵御。网络空间安全的基本内涵已经不仅是针对黑客攻击、勒索攻击、信息系统瘫痪等网络安全风险的预防和控制，[③] 而且涉及网络空间底层信息技术的发展安全。在治理对象层面，网络主权的延伸内容主要是在主权范围内的信息技术创新活动管理、合作与发展。网络主权本身作为国家主权的延伸概念，在技术维度上，其延伸范畴也是以网络空间概念为基础的，它将国家主权范畴的技术主权内容特定到以人工智能、网络通信等为代表的信息基础领域。需要说明的是，这种概念逻辑并不当然意味着在各个技术领域中均存在诸如生物医疗技术主权等概念。之所以信息技术存在主权内容层面的特殊性，是因为网络主权强调的网络安全是一种多层次、体系性的安全架构，信息技术这一要素与数据要素、网络要素等均属于网络安全的重要组成部分，彼此之间呈现相互交织的逻辑关系。

---

① 该法案于 2018 年 8 月 13 日被纳入美国《2019 财年国防授权法案》。参见美国国会官网，https：//www. congress. gov/115/bills/hr5515/BILLS - 115hr5515enr. pdf，2024 年 6 月 12 日。

② 参见鲁传颖：《网络空间大国关系面临的安全困境、错误知觉和路径选择——以中欧网络合作为例》，《欧洲研究》2019 年第 2 期，第 114 页；杨晓强、李若瀚：《国际网络空间安全治理：困境、反思与对策》，《河南社会科学》2022 年第 6 期，第 103 页。

③ 参见周瑞珏：《面向网络安全风险的保险合同义务理论创新》，《学术交流》2024 年第 5 期，第 85 ~ 86 页。

（三）技术自主权的基本内容与误区澄清

主权概念在信息技术领域的延伸早已有学者关注，但彼时尚未出现 ChatGPT 这类“现象级”的技术创新应用，相应的主权概念多表述为“信息主权”，主权内涵也多为信息产业安全发展等。[①] 在网络主权概念兴起初期，有学者将信息主权概念定位为“处理国家主权与信息技术关系的核心概念”，遗憾的是，该概念的基本内涵仍被界定为“国家对信息享有保护、管理和共享的权利”，将信息技术治理一并纳入“信息治理”的概念范畴。[②] 当然，在这些主权概念的发展过程中，零星出现过“科技主权”的相关讨论，并且基于科技安全态势属于国家安全的重要组成部分这一论断，将科技主权视为国家保障科技独立性、自主性的基本能力。[③] 但是，这些论述受限于特定时代的科技发展水平而停留于主权概念层面的讨论，未能进一步解构科技主权的基本内容和制度体系。在当下的网络空间国际治理活动中，科技安全已经在既有的主权安全框架中发展出了全新的内涵：一个国家的网络空间安全依赖信息技术的独立自主发展，并与网络通信安全、网络运行安全、数据安全相互作用，能够有效抵御各类网络安全威胁。相较技术主权，技术自主权更能够反映网络主权内容在技术维度延伸的核心目标和治理对象，因为自主独立发展信息技术的能力是一个国家以实质性平等方式参与网络空间国际治理的重要保障。

具体而言，根据技术自主权内涵可以将其内容归结为自主管理权、自主合作权和同等反制权。第一，自主管理权指主权国家可以对本国网络空间内的各类信息技术创新活动进行管辖，自主决定本国信息技术的创新方向、创新路径等事项。该国以外的任何国家、组织或个人均无权以任何方式干涉、阻碍主权国家对这些事项的独立管辖。自主管理权以网络主权中的平等权和管辖权为基础，强调主权国家在信息技术创新治理活动中的自主管理能力，不仅能够自主决定有关信息技术创新的监管机制、市场激励机制、技术标准制定等事项，而且能够自主决定信息技术创新的国家战略布局。主权国家的实际管辖范围以本国网络安全为判断标准，包括在本国网络空间中的信息技术创新活动。即便在境外从事影响本国科技创新安全的活动，主权国家仍然有权独立管辖。第二，自主合作权指主权国家可以独立自主地选择信息技术

① 参见罗小玲：《从信息主权的高度认识信息产业的发展》，《情报资料工作》2002 年第 S1 期，第 13 页；彭前卫：《面向信息网络空间的国家主权探析》，《情报杂志》2002 年第 5 期，第 99 页。

② 参见刘连泰：《信息技术与主权概念》，《中外法学》2015 年第 2 期，第 505 ~ 519 页。

③ 参见刘祖云、黄文昊：《技术预见视角下的中国“科技主权”维护——以中国转基因技术及其发展为例》，《自然辩证法研究》2010 年第 5 期，第 45 页。

创新的国际合作方式、合作对象、合作领域，主权国家以外的任何国家均无权以直接或间接的方式影响主权国家参与信息技术国际合作活动。自主合作权主要针对现阶段网络空间国际治理规则的碎片化趋势，最大限度地实现非阵营化的信息技术创新合作模式。部分学者指出美国正在以“新干涉主义”“保护性原则”“人权高于主权”等新方式侵蚀他国主权，[①] 并且频繁利用自身的技术优势裹挟其他国家成为自身信息技术创新的资源提供者。在自主合作权框架下，这类行为不仅实质性干涉和妨碍主权国家自主选择信息技术创新国际合作方式，而且限制了主权国家自主确定信息技术创新的国家战略规划，从长远来看，主权国家提升信息技术创新能力的可能性也大大降低。第三，同等反制权指主权国家的信息技术创新活动遭受外部的攻击与威胁时，有权采取同等水平的反击手段保护本国的信息技术自主发展能力。同等反制权以主权概念中的防卫权为基础，明确主权国家针对外部威胁和攻击可以采取的具体反击措施。在实践中，最常见的威胁类型是以信息技术创新供应链为目标的他国干涉型监管政策，例如，美国通过限制对外科技投资的范围和对象、限制芯片和半导体材料出口等方式影响他国信息技术创新活动。此时，主权国家理应有权在维护本国信息技术自主独立发展的前提下采取同等水平的反击措施。之所以将“同等”作为反制权的限定词，是因为避免美国等国家借由长臂管辖等制度路径将反制权无限扩大，实现对内自主管辖和对外反击抵御之间的平衡状态。

四、技术自主权框架下的科技创新治理：以人工智能治理为例

技术自主权的基本架构是以网络主权的对内对外权利为基础，形成技术自主创新能力的持续保障体系。当下，人工智能技术是全球各国国际话语权争夺的重要领域，技术自主权则包含各个主权国家对内科技创新管理和对外科技创新合作与竞争两个维度的内容。

（一）人工智能技术自主权的具体内涵

技术自主权属于网络主权的延伸内容，故而其同样遵循在主权框架下的安全治理逻辑，亦即应当确保网络空间的底层信息技术处于安全可控的状态。人工智能技术是当下全球数字经济发展的关键工具，各国均纷纷加速制定推动技术创新的产业政策和监管制度。不过，面对人工智能技术可能产生的各类安全风险，即便是产业发展优先的美国也在逐渐强化对人工智能的监

① 参见熊光清、王瑞：《网络主权：互联网时代对主权观念的重塑》，《中国人民大学学报》2024 年第 1 期，第 128 页。

管，例如，美国近期公布的《犹他州人工智能政策法》在区分受监管主体和非受监管主体的基础上，明确了人工智能服务提供者负有透明度义务、问责义务等，并通过设立人工智能政策办公室确保技术研发应用的安全性。在过去，人工智能技术尚处于初步探索阶段，故而在网络主权框架下鲜有专门提及人工智能技术安全可靠性的必要性；而在当下，生成式人工智能的创新应用使这些技术成为足以影响网络空间安全有序状态的关键因素，以深度合成为代表的技术应用甚至可能威胁国家安全和社会稳定。在这样的背景下，以技术自主权确认和保障主权国家对人工智能技术创新的自主发展能力显得尤为必要。主权国家的网络安全始终是一种风险相对可控的安全状态，而风险可控的实现也是以独立自主的人工智能技术创新能力为基础的，并且这种能力也是国家参与网络空间博弈的重要保障。①

技术自主权的提出不会当然加深网络空间国际治理的碎片化程度，因为只有保障主权国家具备自主发展人工智能技术和排除外部不当干预的能力，才能够真正有效达成具有共识内容的国际法规则。现阶段，技术自主权面临的最核心质疑便是如何确认哪些行为构成对主权国家技术自主权的侵犯，这与网络主权概念面临的“领网”边界质疑相似。正如前文论及的网络空间概念扩张，技术自主权的适用范围并不包含所有的人工智能技术创新活动，应当以威胁或损害网络安全状态为一般性原则，结合对人工智能自主创新能力的影响程度进行判断。客观而言，意欲以领土、领海等边界模式划定网络空间边界并不具有可操作性，如何划定网络主权的适用范围这一问题本身也较为笼统，问题的追问方向更应当实现从笼统问题向具体问题的转变。在网络主权框架下，技术自主权的适用范围问题也延续了这一逻辑，即需要转化为“哪些人工智能技术属于影响国家安全的关键技术”“哪些人工智能技术研发创新活动属于保障主权的核心领域”“他国何种类型的人工智能产业政策超出了主权管辖范畴”等具体问题，这些问题实际上也是技术自主权从主权概念转化为具体的国内法规则和国际法规则的正当性基础。

从影响网络安全的角度来看，人工智能技术自主权实际上将技术安全可控这一治理目标解构为三个安全指标。一是功能安全，即人工智能信息系统运行稳定，并且在遭受外部网络攻击、发生系统故障等网络安全事件时，能够快速排除障碍、恢复正常功能。由此延伸至主权国家有权监管向本国境内提供信息服务的各类人工智能信息系统及其提供商，这也是当下网络信息服务跨地域性特点的必然结果。二是科技伦理安全，即人工智能技术应当以符合法律法规和科技伦理的方式创新发展，遵循信息技术服务人类社会的核心

① 参见黄颖：《新兴技术视域下的网络空间“碎片化”探究》，《国际政治研究》2022 年第 4 期，第 110 页。

原则。虽然各国在人工智能技术应用监管制度层面存在显著的立场差异，但近年来各国公布的人工智能产业政策和发展战略均在不同层面提及科技伦理对人工智能创新发展的规范作用。在技术自主权的语境下，科技伦理安全指标转变为主权国家有权按照符合人类共识性的伦理规范和本土伦理规范设定相应的科技伦理标准；而且，其他国家、组织或个人无权以任何方式将自身的伦理标准直接或间接地施加于主权国家。三是市场准入安全，即主权国家有权决定人工智能信息服务的市场准入条件和监管标准，禁止向本国公民提供存在国家安全风险的人工智能技术应用。任何国家、组织或个人不得以促进信息技术开放等事由变相要求主权国家允许具有安全隐患的算法模型等相关技术引入境内。这些安全指标与人工智能技术自主权包含的对内自主权和对外独立权共同构成了人工智能技术自主治理体系。

（二）人工智能技术自主权的对内效力

人工智能技术自主权对内效力体现为对境内网络空间人工智能技术创新应用的管理以及对境内人工智能产业布局、人工智能技术创新要素供给、人工智能技术风险监管这三类事项进行依法监管。

在人工智能产业布局方面，技术自主权表现为主权国家对本国人工智能产业发展方向和技术创新路径享有自主决定权。各国政府有权独立自主制定符合本国国情的人工智能产业政策，也有权采取必要的措施维持和提升本国在人工智能国际竞争中的自主创新能力。在此层面上，技术自主权与传统国家主权中的经济主权等内容的差异性在于，技术自主权指向的自主决定人工智能产业布局既包括人工智能产业本身，又包括与人工智能产业存在供应链关系的配套产业，如数据标注产业、公共数据集产业等。相对地，传统国家主权指向的科技产业布局是一种在经济学意义上的科技产业转型升级，更侧重主权国家通过内部管理活动实现科技创新经济效益增长。部分学者在其主张的信息主权概念中，将主权国家的管辖范围划定为“信息传播技术、信息产业、信息数据内容等事项”。[①] 可见，技术自主权的增设也是为了更好地说明当下网络主权的维护方式早已从实现狭义的网络安全延伸至实现信息技术及其相关产业的独立自主发展。而且，网络安全、数据安全以及信息技术安全三种网络空间安全状态相互交织，主权国家不仅有权自主决定人工智能产业布局，而且能够独立自主地统筹管理与人工智能产业相关的其他社会公共资源及其配套产业设施。

在人工智能技术创新要素供给方面，技术自主权表现为主权国家能够独立自主地开展有关人工智能科技创新要素供给的管理活动。与自主决定人工智能产业布局不同的是，该层面的技术自主权更侧重主权国家在国内法层面

① 参见宋知原、李毅：《总体国家安全观视阈下的中国国家主权安全与国际法规则》，《中国政法大学学报》2024 年第 2 期，第 51 页。

自主决定数据、算力、算法等创新要素的供给机制、市场激励机制以及监管机制。在数据资源供给方面，技术自主权与数据主权在内容层面存在交叉关系，均表现为主权国家可以自行决定本国境内数据流动的监管方式，并对数据跨境流动设置必要的安全审查机制，只不过技术自主权更侧重主权国家制定与人工智能创新相关的数据资源供给机制。在算法模型方面，国外不少人工智能大模型以开源代码或服务接口的方式允许他国企业使用，但客观而言，算法模型技术本身处于典型的价值中立状态，由于不同主权国家对算法模型的合法性要求存在差异，算法模型的应用行为会产生不同的法律评价结果。技术创新不能凌驾于国家主权之上，故而技术自主权表现为主权国家能够依法监管境内外算法模型的应用活动，并依据国内法的相关规定，限制或禁止部分算法模型在本国管辖范围内应用。在算力方面，技术自主权表现为主权国家对本国境内算力基础设施建设、算力供给和交易机制建构等方面的制定权和管理权。算力基础设施安全与算力资源供给安全属于网络安全的重要组成部分，因为算力供给安全问题既是人工智能产业创新的技术基础，也是网络空间关键信息基础设施运行安全、数据流动安全的重要保障。

在人工智能技术风险监管方面，技术自主权表现为主权国家有权针对不安全、不可靠的人工智能技术应用采取限制或禁止措施，制定专门面向人工智能技术研发者、服务提供者以及用户的相关法律法规。事实上，这一层面的技术自主权早已成为国际社会共识。美欧等已经开始在国内法层面设置相应的人工智能技术风险监管机制，例如，欧盟在《人工智能法》中对通用人工智能算法模型提供者设置了“采取充分的网络安全防护措施”“评估并减轻系统风险”“实施包含对抗性测试的模型评估”等法定义务。此时，技术自主权是对狭义网络安全的技术安全要素的“补强”，即在网络主权框架内，主权国家独立自主管辖网络空间的表现形式当然包括对信息技术安全风险的预防和控制。美欧主张的技术中立是难以在技术自主权概念下证成的，因为信息技术的创新发展应当以维护国家安全和社会稳定为前置性要件。

（三）人工智能技术自主权的对外效力

人工智能技术自主权的对外效力体现为主权国家有权自主决定人工智能技术的国际合作方式，平等地参与人工智能技术国际竞争活动，并在遭受不当干预和妨碍时采取同等水平的必要反击措施。在事实层面，各国信息技术的发展水平和创新能力存在差距，网络主权之所以能够在这种客观事实背景下得到国际社会的认可，是因为该主权概念反映了“均权发展”、“独立发展”和“平等发展”的网络空间国际治理新秩序。在网络空间国际竞争中，信息技术的强弱实际上决定了一个国家在国际竞争中的话语权大小，而这种网络权力也被部分学者称为治网权，网络主权强调的尊重主权平等原则是为了防止这种治网权被滥用，使主权国家均能够享有均等的

发展机会。[①] 作为网络主权子概念的技术自主权同样强调各国均享有自主独立发展人工智能等信息技术的平等机会，在尊重主权平等的基本原则下，任何国家、组织或个人均不能采取任何方式限制或妨碍这种均等的技术自主创新能力。此外，技术自主权的增设也是为了防止国家之间信息技术发展的“数字鸿沟”持续扩大，美国的网络空间国际治理话语权争夺已经延伸至人工智能技术领域，美国借由自身芯片技术的优势地位，要求芯片企业“站队”，并拉拢西方国家加入己方阵营，达成国际层面的算力资源垄断。

在人工智能技术国际合作方面，技术自主权表现为主权国家能够独立自主地决定人工智能创新合作方式，并且主权国家之间的技术创新合作不应当受到其他主权国家、组织或个人的不当干预或妨碍。相较国内法层面已经逐步建构人工智能监管体系，技术自主权更侧重人工智能治理的国际规则体系建构。中国推行的“数字丝绸之路”倡议实际上是为广大发展中国家提供网络安全能力建设援助，[②] 而这一援助活动本身除了网络通信技术能力，还包括有关网络安全保障的其他信息技术建设能力。因此，在技术自主权框架下的人工智能国际治理规则应当以尊重主权平等原则为基础，以保障各主权国家独立自主发展人工智能能力为导向。我国在《网络空间国际合作战略》中也提及“和平、主权、共治、普惠”四项原则，而技术自主权是在共治原则和普惠原则的基础上延伸至“主权国家普遍且平等地享有人工智能技术国际合作决定权”。平等且充分的人工智能国际合作是形成普适性人工智能国际治理规则的必要基础，如此方可避免因为国家之间科技创新和科技治理能力的巨大差异导致人工智能技术滥用，由技术优势地位国家流向技术弱势地位国家，形成在国际治理环节中的“灰色地带”，[③] 人工智能安全已经成为发展中国家实现国家安全的重要领域。[④]

在人工智能技术国际竞争方面，技术自主权表现为主权国家有权采取符合国际法规则的人工智能技术竞争外交策略、产业政策和法律制度，并根据自身遭受的不正当待遇采取同等水平的反击措施。面向以往的其他信息技术，各国对待这些技术风险采取了不同的监管立场和治理策略；而面向人工智能技术，各国对待人工智能技术应用的监管立场和治理策略开始呈现趋同化特征。例如，中国的分级分类监管和欧盟的四类风险级别监管机制均将人

① 参见赵宏瑞：《网络主权论》，九州出版社 2018 年版，第 87 页。

② 参见郑春荣、李岳梅：《德国参与网络空间国际治理的主张、实践与动因分析》，《同济大学学报》（社会科学版）2022 年第 6 期，第 32 页。

③ 参见 Aaron D. Kirk, Artificial Intelligence and the Fifth Domain, *Air Force Law Review*, Vol. 80, 2019, p. 235。

④ 参见 Kushal Srivastava, Artificial Intelligence and National Security: Perspective of the Global South, *International Journal of Law in Changing World*, Vol. 2 (2), 2023, pp. 84 – 85。

工智能安全风险作为设置监管机制的基本要素，只不过二者在风险级别划分、不同风险对应的监管标准等具体内容上存在差异，这种差异性恰恰是在主权平等基础上的正常国际竞争活动。无论是网络主权，还是技术自主权，均不否认主权国家基于国家利益采取必要的国际竞争策略之正当性。但是，同美国那般以间接侵犯主权的方式变相强制其他主权国家遵守其主导的人工智能国际治理规则的做法已经超出了技术自主权认可的“竞争范畴”。美国政府在 2025 年 1 月 13 日发布了《确保人工智能时代的美国国家安全和经济实力》（Ensuring U. S. Security and Economic Strength in the Age of Artificial Intelligence），该文件将高性能芯片供给活动纳入国际政治博弈的框架内，严重影响全球芯片供应链安全稳定。部分学者认为促成人工智能国际治理达成共识的要素在于“利益”、“制度”和“信念”，[①] 归根结底，这些共识性要素需要达成主权平等、国家利益保障以及国际竞争力提升三重目标的平衡，这也是技术自主权存在国际合作和国际竞争两个内容维度的理论基础。

五、结语

在信息技术国际竞争越发激烈的当下，需要从国际法和国内法两个层面建构保障信息技术自主创新能力的制度体系。时至今日，网络主权的基本内涵与网络空间、网络安全等概念保持着同步发展、同步扩充的状态：在跨境数据流动领域，网络主权延伸了数据主权等具体内涵；在信息技术自主发展领域，网络主权延伸了技术自主权等具体内涵。网络主权在数据维度、技术维度的内容延伸是网络空间国际治理深入发展的必然结果。因为一个国家的网络空间安全已经不再是狭义层面的网络空间安全，而是网络通信安全、网络数据安全、网络技术安全等安全要素的综合体，所以有必要从多个治理维度确保本国网络空间的安全可控。当下的网络空间国际竞争越发关注人工智能技术的创新能力，美欧在持续强化科技创新能力的同时，通过阻断产业供应链、限制特定企业市场准入等方式实施新型的外部干预行为。面对日益复杂的国际竞争环境，以保障本国信息技术自主创新能力为核心目标的技术自主权越发重要。该项源自网络主权的新兴主权，是主权国家平等参与人工智能国际治理、推动形成平等自主国际治理规则的国际法依据，也是集功能安全、科技伦理安全、市场准入安全等要素于一体的网络空间安全新样态。

（责任编辑：方　军）

① 参见马爱芳、胡泳：《人工智能的国际治理：理论框架、现实困境与模式探究》，《新闻与写作》2024 年第 1 期，第 77 ~ 78 页。