数字经济和数字博弈双重背景下人工智能的国际法治理

沈伟*　赵尔雅**

内容摘要:人工智能的国际法治理问题首先出现于数字经济兴起的背景下,随着数字经济背景下的竞争实质上转变为技术霸权之争,人工智能也从各国技术治理之争的对象演化为技术霸权之争的工具。运用国际法进行人工智能治理并克服系统性风险是可能且必要的路径。现有的人工智能国际法治理呈现出四个主要特点:内容上以伦理规则为主;形式上以非政府主体制定的软法为主;直接规制规则空缺,间接规制规则趋完善;部分法域的域内法发展显著。数字经济背景下人工智能对国际法的挑战总体上表现为排他性主权与统一数字空间的张力,具体在国际经贸规则中体现为人工智能的性质认定与规制路径不明。为实现人工智能治理的全球合作,首先应将其与数字经济规则密切结合,以数据治理为根本;其次应打造多元主体参与的协同共治模式;最后应防范地域与南北隔阂,营造全球普遍的法律环境。

关键词:数字经济　数字博弈　人工智能　数据治理

人工智能作为一项根植于数据的技术,正在成为各国在数字经济时代相互竞争的核心领域。随着大国之间数字博弈的展开,人工智能的治理图景也在相应地变化。

一、人工智能国际法治理的背景:从数字经济到数字博弈

人工智能的国际法治理问题首先出现于数字经济兴起的背景下,随着数字经济背景下竞争的实质转变为技术霸权之争,人工智能也从各国技术治理之争的对象演化为技术霸权之争的工具。

(一)数字经济与人工智能

数字经济将数据作为一种经济资源,不仅利用数据,亦创造数据作为新的价

*　上海交通大学凯原法学院教授、博士生导师。

**　上海交通大学凯原法学院欧盟法研究中心研究助理。

本文系国家社科基金重大项目“美国全球单边经济制裁中涉华制裁案例分析与对策研究”(21&ZD208)的阶段性成果。

值。人工智能在数字经济中的重要性在于,人工智能是数字经济的核心特点,因为它作为一种计算统计技术有能力从海量数据中找出隐藏的模式和规律,[①]根据现存数据创造更多的数据信息知识,[②]而更广泛的信息又可反作用于人工智能的研发与训练。数字经济的领跑者可以通过控制数据和以人工智能为代表的相关技术来获取经济和战略优势。[③]例如,国际主流的人工智能框架由Google、Meta等科技巨头主导,形成了以Google-TensorFlow和Meta-PyTorch为代表的双寡头格局,[④]此外,这类巨头通过其服务平台所掌握的全世界用户的数据,进一步加固它们的领先地位。

(二)数字经济发展的新维度:数字博弈

人工智能的核心技术特征使其具备了国家安全属性,从而对国家安全体系产生深刻影响。比如,在军事领域,利用人工智能技术将有可能发展出致命性自主武器系统,动摇现存的战争伦理和国际人道主义规范。在经济领域,人工智能有可能颠覆和重构全球价值链和分配格局,导致结构性失业,加剧贫富分化以及资本、数据甚至算法垄断。[⑤]在金融领域,人工智能在金融决策中的应用加大了消费者隐私权的保护难度,但也可能有助于减少消费者歧视和融资成本。[⑥]在政治领域,人工智能有可能通过社交媒体,改变政治体系的逻辑和运转。人工智能的技术属性使其既是安全风险的源头,又是克服安全风险的工具。[⑦]

科技作为人类社会发展的动力之源,自然成为国际政治中权力内核的重要内容。[⑧]人工智能是下一波科技浪潮的核心,且已经对主权国家和其他国际行为体产生安全风险。以人工智能为代表的技术革命正在动摇国际竞争格局,引发国际规则和标准领域的话语权之争和技术竞赛秩序主导权之争,这总称为数字博弈。从数字

---

① 参见郑戈:《数字社会的法治构型》,《浙江社会科学》2022年第1期,第151页。

② See Shin-yi Peng, *et al.*, Artificial Intelligence and International Economic Law: A Research and Policy Agenda, in Shin-Yi Peng, *et al.*(eds.), Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration 8 (Cambridge University Press 2021).

③ See SUNCTAD, Cross-border Data Flows and Development: For Whom the Data Flow, https://unctad.org/system/files/official-document/der2021_en.pdf, visited on 31 May 2023.

④ 参见中国信通院:《AI框架发展白皮书(2022年)》,http://www.caict.ac.cn/kxyj/qwfb/bps/202202/P020220226369908606520.pdf, 2023年5月31日访问。

⑤ 参见殷继国:《人工智能时代算法垄断行为的反垄断法规制》,《比较法研究》2022年第5期,第185页。

⑥ See SNikita Aggarwal, AI, Fintech and the Evolving Regulation of Consumer Financial Privacy, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=4235395, visited on 31 May 2023.

⑦ 参见封帅:《国家安全视域下的人工智能安全研究:议题网络建构的初步尝试》,《国际安全研究》2023年第1期,第26-49页。

⑧ 参见郑华、聂正楠:《科技革命与国际秩序变迁的逻辑探析》,《国际观察》2021年第5期,第127-156页。

经济到数字博弈的话语转向表明,当今技术层面的国际竞争虽依然表现为技术治理之争,但实质上已转向为技术霸权之争。

1.数字博弈的表现:数字经济背景下的技术治理之争

各国在技术法规制定层面的竞争是数字博弈在法律层面的表现。例如,在人工智能领域,除促进人工智能发展以掌握技术上的先发优势外,在治理规则制定上占据先发优势也是各国的竞争目标。各个国家和区域立法的最新进展体现了数字经济时代以规则之争为表现的人工智能治理之争。

由于规则制定者内部对于人工智能的规制强度本身就存在争议,这一治理的推进过程必然是缓慢的。例如,在《人工智能法案》草案于2023年4月经欧洲议会表决的前夕,欧洲议会议员尚未就如何平衡数据隐私保护与避免扼杀人工智能创新和投资达成一致,分歧的核心在于哪些人工智能系统应被认定为"高风险"。欧盟一方面不愿在公民保护上妥协,另一方面又面临着人工智能技术竞争的地缘政治压力,[①]这种困难体现了博弈国家在人工智能治理中试图平衡维持规制与促进发展之双重目标的内部矛盾。

更为激烈的冲突体现在规则制定者之间,表现为国家间针对人工智能的立法竞争。以美欧为首的发达国家对中国技术发展的遏制是一个典例。2022年2月,欧盟委员会公布了《欧洲芯片法案》。2022年8月,美国《2022芯片与科学法案》(CHIPS and Science Act of 2022)也正式生效。美欧的芯片法案均旨在补贴与支持芯片和科技研发,具体途径包括资金支持、税收减免、半导体生态系统建设以及人才培训等。通过发布芯片法案,美欧不仅对芯片研发进行扶持,而且重视芯片的生产制造,希望借此解决供应链安全问题,[②]同时实现对抗中国的目的。[③]

2.数字博弈的实质:地缘政治背景下的技术霸权之争

人工智能是各国必争的科技创新高地,已经成为国际关系中的"战略性资产",[④]而保障战略资产供给的稳定是各国强化经济安全保障能力的重要一环。美国学界和政界都将人工智能硬件界定为中美科技竞争中的战略资产。美国在人工智能的

① See Hadrien Pouget, The EU's AI Act Is Barreling Toward AI Standards That Do Not Exist, https://www.lawfareblog.com/eus-ai-act-barreling-toward-ai-standards-do-not-exist, visited on 31 May 2023.

② 参见李万强、张嘉兴:《美欧芯片补贴立法的最新动向及对我国的启示》,《国际贸易》2023年第4期,第63页。

③ See The White House, Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/, visited on 31 May 2023.

④ See Jeffrey Ding & Allan Defoe, The Logic of Strategic Assets: From Oil to AI, 30 Security Studies 182-212 (2021).

科研现状、产业发展、人才支撑、硬件基础、市场应用、数据规模等指标上，依然保持着世界总体领先地位，尤其在研发、人才、人工智能芯片、融资环境等方面具有相当大的优势。[①]美国国家人工智能安全委员会建议美国政府继续通过出口管制维持美国在人工智能硬件、尤其是半导体制造设备领域的优势。[②]

数字博弈背景下的治理难题不仅反映了技术法规的设计之难，更体现了各治理主体在政治层面的博弈。上述欧盟的内部分歧实则体现了欧盟在国际数字博弈策略上的分歧。地缘政治的竞争场域已经蔓延至技术领域，这在中美两国的技术竞争中体现得尤为明显。美国在2022年《国家安全战略报告》（以下称《报告》）中指出，技术是当今地缘政治竞争的核心，并把中国定位为“地缘政治的最大挑战者”。一方面，美国力求在竞争中寻得盟友。《报告》指出，美国将通过美国—欧盟贸易和技术委员会开展工作，以促进跨大西洋在半导体和关键矿产供应链、可信赖的人工智能等方面的协调，加强美国和盟国的技术领导地位。[③]现实中，美国欲借助所谓“民主科技联盟”深化与盟友和伙伴国的多边协同，在情报、执法、出口管制、投资审查和风险防范等方面逐步实现一致化，达到“小院相通、高墙相连”的目标。[④]另一方面，美国针对中国展开了一系列的竞争与压制。在中美两国间就人工智能的技术博弈中，美国意在打压中国大型企业、实现科技断链，围绕短视频应用TikTok的争议即为一例。早在2019年11月，特朗普政府就称将对TikTok母公司字节跳动在2017年收购美国社交媒体应用musical.ly展开国家安全审查。尽管有关禁令随后在2021年被撤销，但2023年3月，新一轮针对TikTok的限制继续展开：美国政府要求字节跳动出售TikTok资产以实现剥离（divesture），否则考虑禁止其在美国的运营。无独有偶，美国商务部于2022年12月15日宣布将35家中国企业和研究机构加入实体清单，主要涉及人工智能芯片、半导体装备、航空航天等行业。安徽寒武纪信息科技有限公司等21个人工智能芯片研发、制造和销售实体被以“获取或者试图获取美国原产物项以

① 参见贾夏利、刘小平：《中美人工智能竞争现状对比分析及启示》，《世界科技研究与发展》2022年第4期，第531-542页。

② See Jeffrey Ding & Allan Defoe, The Logic of Strategic Assets: From Oil to AI, 30 Security Studies 182-212 (2021).

③ See National Security Strategy, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, visited on 31 May 2023.

④ 参见赵明昊：《统合性压制：美国对华科技竞争新态势论析》，《太平洋学报》2021年第9期，第12页。

支持中国的军事现代化”的理由列入清单,并适用推定拒绝的许可审查政策。[①]

(三)数字博弈背景下的人工智能治理新图景

1.以技术规范与国家安全规范为核心内容

地缘政治因素使得技术问题始终与国家安全紧密相关,也使国家安全规范的塑造成为人工智能治理的重要一环。不同主体对于技术规范和国家安全规范间的侧重选择有所不同。例如,欧盟当前采取以技术规范为主导的竞争策略,美国则以国家安全规范为重。美国的人工智能规制提案虽然在数量上相对较少,但在基本政策导向上十分重视国家安全的维护。美国人工智能国家安全委员会(National Security Commission on Artificial Intelligence, NSCAI)指出,美国的技术优势自“二战”以来首次面临威胁,人工智能加深了中国等国“渗透美国社会、窃取数据,并干涉美国民主”的威胁,并提出“重组政府、重新定位国家并召集最亲密的盟友和合作伙伴”的核心战略,以“保卫美国并赢取人工智能竞争”。[②]除了专门针对人工智能的政策,美国其他法规也有适用于人工智能的可能。例如,美国《外国投资风险审查现代化法》(Foreign Investment Risk Review Modernization Act, FIRRMA)中,“涉及特别关注国家的敏感交易(sensitive transactions involving countries of special concern)”的定义涵盖了可能导致数据获取的交易,具体包括“可能导致美国公民的敏感个人数据被以威胁国家安全的方式利用的交易”,以及可能导致相应实质性决策权的交易。[③]该定义还包括了可能导致获得对关键技术使用、开发、获取或发布的实质性决策权的交易。对于人工智能而言,此处的相关“数据”可能涵盖人工智能训练所需的数据,“关键技术”则可能涵盖人工智能所依托的算法。此外,美国的重要游说团体也在强调人工智能带来的国家安全风险,如美国商会(US Chamber of Commerce)在其《人工智能委员会报告》中呼吁尽快制定人工智能法律监管框架以规避国家安全风险。[④]

2.以单边性措施和区域性治理为主要形式

在技术中立的理想图景下,对人工智能的全球合作治理本应具有可能性。然

---

① See Additions and Revisions to the Entity List and Conforming Removal from the Unverified List, Federal Register Vol.87, No.242, 19 December 2022, https://www.govinfo.gov/content/pkg/FR-2022-12-19/pdf/2022-27151.pdf, visited on 31 May 2023.

② See National Security Commission on Artificial Intelligence's (NSCAI), The Final Report, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf,visited on 31 May 2023.

③ See Foreign Investment Risk Review Modernization Act of 2018, SEC. 201. Definitions (C)(II).

④ See US Chamber of Commerce, Artificial Intelligence Commission Report, https://www.uschamber.com/assets/documents/CTEC_AICommission2023_Report_v6.pdf, visited on 31 May 2023.

而，随着技术领先性成为大国间数字博弈的重要目标，各国难以在人工智能领域寻得短期内的共同利益，这使得人工智能及其治理成为竞争国家间依凭国家安全缘由而相互掣肘的工具。因此，现实中的人工智能治理形式往往具有单边性和区域性的特征。其一，在数字博弈中，由于有约束力规则的缺乏以及对国家安全的考虑，单边措施将在一定阶段内成为主流。这种广义上的单边措施既包括单边的立法与政策，如美国单边发布的《关于负责任地在军事上使用人工智能和自主权的政治宣言》；[①]也包括单边的一次性行为，如美国针对中国科技公司实施的大规模制裁和出口管制限制措施。其二，在人工智能的跨国与跨区域治理上，主要主体的利益团体划分明显。例如，欧盟和美国在技术层面存在一定程度合作：2023年3月，欧盟和美国代表在华盛顿举行了第三次欧盟—美国联合技术竞争政策对话（technology competition policy dialogue, TCPD），旨在进一步巩固合作成果，确保和促进数字领域的公平竞争。然而，区域性的治理规则本身难以推广。有分析指出，受制于现有市场、国际标准机构和外国政府的影响，欧盟人工智能法案将产生的布鲁塞尔效应有限。[②]相应的后果是，国际性的人工智能治理合作难以实现，但区域性治理的整合度在不断提升。例如，欧盟的《数字服务法案》和《数字市场法案》在执法机制上授予欧盟委员会广泛的市场监督和执法权力，加强欧盟在数字经济中的协调和直接执法，[③]体现了区域性治理的强化。

二、运用国际法进行人工智能治理的可能性与必要性

运用国际法进行人工智能治理首先是具有可能性的，这主要源于主权国家治理的有效性。同时，在诸多人工智能治理途径中，运用国际法加以治理又是具有必要性的，这主要源于人工智能技术对于有约束力国际准则的需求。

（一）运用国际法进行人工智能治理的可能性

自2018年首次公布自己的人工智能原则（AI at Google: Our Principles）以来，

① See U.S. Department of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/, visited on 31 May 2023.

② See Alex Engler, The EU AI Act will Have Global Impact, but a Limited Brussels Effect, https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/, visited on 31 May 2023.

③ See Pieter Van Cleynenbreugel, The Commission's Digital Services and Markets Act Proposals: First Step towards Tougher and More Directly Enforced EU Rules?, 28 Maastricht Journal of European and Comparative Law 667-686 (2021).

Google每年更新其人工智能原则,就人工智能标准与政策的全球对话总结成果并提出建议。[①]2022年11月,美国人工智能公司OpenAI研发的ChatGPT(chat generative pre-trained transformer)发布,这款能够以自然语言与使用者进行交互的聊天机器人程序引发了全球对于生成式人工智能(generative AI)的关注,这在法律层面表现为对于生成式人工智能所创作作品之知识产权归属的讨论。[②]

人工智能的可治理性源于主权国家治理的有效性。尽管大型私人公司具有丰厚的人工智能技术和社会资源,但它们仍根本受制于政府管控。哈佛大学国际关系教授Stephen Walt认为"科技巨头不会重塑全球秩序":科技巨头无法拥有类似主权的权力或忠诚度,它们在数字世界中的地位会随着主权在数字世界中的扩散行使而削弱。[③]在陈述对人工智能的治理方式时,有学者采用了宽泛的政策(policy)一词,但同时认可了法律的可能性(possibility)和终局性(finality)。[④]人工智能的发展需要法学界探索法律和人工智能融合的法学理论,需要立法者制定人工智能的运行和使用规则,还需要监管部门规制算法偏见和不可解释性问题。[⑤]数据的跨境流动和技术的全球扩散还意味着人工智能治理需要国际法的回应。

(二)运用国际法进行人工智能治理的必要性

通过国际法对人工智能进行治理的必要性首先源于这一技术本身的工具性,由于人工智能的应用必然是多领域和全球性的,只有国际准则可以提供统一指引。其次,人工智能已经在数据层、算法层和应用层分别对现行有约束力的国际法规则造成冲击。仅是人工智能在商业领域的广泛应用,就足以对现有国际经贸规则造成全方位影响。人工智能对现有国际法的冲击无法被忽视,需要塑造有约束力的国际规则。

由于人工智能与数字资源的必然联系,对人工智能国际法治理的讨论无法脱离

---

① See Google AI, Our Principles, https://ai.google/static/documents/ai-principles-2021-progress-update.pdf, visited on 31 May 2023.

② See for example, Giorgio Franceschelli & Micro Musolesi, Copyright in Generative Deep Learning, 4 Data and Policy 17 (2022); Michael D. Murray, Generative and AI Authored Artworks and Copyright Law, 45 Hastings Communications and Entertainment Law Journal 27 (2023).

③ See Stephen M. Walt, Big Tech Won't Remake the Global Order, https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order, visited on 31 May 2023.

④ See Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 UCD Law Review 399, 409-410 (2017).

⑤ 参见魏斌:《法律人工智能:科学内涵、演化逻辑与趋势前瞻》,《浙江大学学报(人文社会科学版)》2022年第7期,第49-67页。

国际法对于数字经济的总体治理框架。

三、现有人工智能国际法治理的主要特点

人工智能作为一种数据驱动的技术，容易被大型集团和机构等数据所有者操纵，导致风险外溢和危机。人工智能治理在个人权利、数据保护、道德和公平等方面都面临重大挑战，而这些挑战无法仅停留在人类和机器的二分法框架中。人工智能的风险治理具有技术、政治经济和社会文化的多面性和复杂性，需要一种更为系统的框架。就人工智能国际治理的现状来看，一方面，人工智能治理规则在内容与形式上均处于较为原始的形态，即以伦理规则为主要内容、以非政府主体制定的软法为主要载体。另一方面，尽管当前缺乏直接规制人工智能的有约束力的国际规则，但数据流动治理规则、消费者保护规则等为人工智能的间接治理提供了丰富的资源。

（一）内容上以伦理规则为主

由于法律不可避免的滞后性，在当前人工智能国际法规则尚未确立的情况下，仍需依靠不具有强制约束力的伦理准则进行治理，这也符合法律工具主义的限度理论。[①]伦理规则虽然不具有国际法层面抑或国内法层面的强制约束力，但其相较法律更具道德上的普适性，因而更易获得国际认可。目前，全世界在政府层面所达成的最广泛的人工智能共识是2021年联合国教科文组织大会通过的《人工智能伦理问题建议书》。[②]这是目前政府层面最广泛的人工智能伦理共识，也是最广泛的人工智能多边共识，它将为进一步形成人工智能国际标准和国际法等提供参考。

2018年，欧盟发布的第一份人工智能战略文件任命了人工智能高级别专家小组。该小组在2019年发布了人工智能道德标准——《可信赖人工智能的伦理指南》（Ethics Guidelines for Trustworthy AI），将算法的透明度与可解释性列为人工智能的基本伦理规则和实现可信赖人工智能的关键要素之一，强调算法的可解释性对于人类建立对算法信任的关键作用。[③]欧洲议会未来与科学和技术小组发布的《算法责任与透明度治理框架》（A Governance Framework for Algorithmic Accountability

① 参见蒋超：《法律算法化的可能与限度》，《现代法学》2022年第2期，第22-35页。

② See UNESCO, UNESCO Member States Adopt the First Ever Global Agreement on the Ethics of Artificial Intelligence, https://www.unesco.org/en/articles/unesco-member-states-adopt-first-ever-global-agreement-ethics-artificial-intelligence, visited on 31 May 2023.

③ See Ethics Guidelines for Trustworthy AI, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419, visited on 31 May 2023.

and Transparency),亦将算法透明度与可解释性视为解决算法公平、实现算法治理的基础工具。[①]

(二)形式上以非政府主体制定的软法为主

人工智能治理所依托的软法首先包括国际法中的软法,即由传统国际法主体参与制定的不具有约束力的国际规则。2019年5月,OECD理事会通过了《人工智能建议书》,它是第一个关于对可靠人工智能进行负责任管理的政府间标准。[②]2019年6月,G20部长级会议表决通过《G20贸易和数字经济部长声明》,[③]该声明在附件部分提出了"G20人工智能原则",并明确该原则不具有约束力。

人工智能治理所依托的软法不仅限于国际法意义上的软法,还包括其他主体主导和制定的规范。有学者把这类自律性行业规范文件称为一种"超级软法"(super-soft law)——它们不具有正式约束力,同时由于国际法的传统主体或组织并不参与其制定,亦不会成为国际软法。它们出现在国际法的空白领域,凭借自身的优点产生强大的合规吸引力。[④]当前,许多发生在传统的国际立法场域之外的人工智能国际标准制定进程正在进行。例如,电气与电子工程师协会(Institute of Electrical and Electronics Engineers, IEEE)于2016年发起的"IEEE关于自治和智能系统伦理的全球倡议"是较为全面的人工智能软法倡议,旨在确保参与自动化和智能系统设计和开发的每一个利益相关者都受到教育、培训,并被授权在设计和使用中优先考虑道德因素,从而使这些技术为人类的利益而进步。[⑤]

(三)直接规制规则空缺,但间接规制规则渐趋完善

虽然直接以人工智能为规制对象的国际法尚未成型,但与人工智能治理间接相关的治理规则并不稀缺,部分领域已经渐趋全面与成熟,其中典型的是以数据治理规则为代表的数字经济规则。

当前,与人工智能直接或间接规制相关的国际协定渐次出现。国际层面的数字

---

① See A Governance Framework for Algorithmic Accountability and Transparency, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf, visited on 31 May 2023.

② See OECD, Digital Economy, https://www.oecd.org/digital/ieconomy/, visited on 31 May 2023.

③ See G20 Ministerial Statement on Trade and Digital Economy, https://www.mofa.go.jp/files/000486596.pdf, visited on 31 May 2023.

④ See Thomas Burri, International Law and Artificial Intelligence, 60 German Yearbook of International Law 91-108, 106 (2017).

⑤ See The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, https://standards.ieee.org/industry-connections/ec/autonomous-systems.html, visited on 31 May 2023.

经济规则主要有两种形式:一是纳入自由贸易协定中的数字贸易协议内容,如《全面与进步跨太平洋伙伴关系协定》(Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP)第14章"电子商务"(electronic commerce)、《区域全面经济伙伴关系协定》(Regional Comprehensive Economic Partnership, RCEP)第12章"电子商务"、《美墨加协定》(United States-Mexico-Canada Agreement,USMCA)第19章"数字贸易"(digital trade)等均包含数字贸易相关政策。二是专门的数字贸易协定或电子商务协定,如东盟各国于2018年11月签署的《东盟电子商务协定》(ASEAN Agreement on Electronic Commerce),美国和日本于2019年10月签署的《美日数字贸易协定》(U.S.-Japan Digital Trade Agreement),2020年6月智利、新西兰和新加坡签署且中国加入的《数字经济伙伴关系协定》(Digital Economy Partnership Agreement, DEPA),2020年8月澳大利亚和新加坡签署的《数字经济协定》(Singapore-Australia Digital Economy Agreement,SADEA)等。SADEA第31条[①]和DEPA第8.2条[②]均直接以"人工智能"为标题,不过二者并未为缔约国规定具体权利义务,而是仅确认了各方对人工智能治理合作的共同认识。此外,2019年启动的WTO框架下的电子商务谈判仍在进行中,[③]但各成员在跨境数据流动、数据本地化、源代码保护、电子传输免关税永久化等方面分歧较大。[④]

① SADEA第31条"人工智能"规定:(1)双方认识到,人工智能技术的使用和采用在数字经济中变得越来越重要,可为自然人和企业带来重大的社会和经济效益。双方应根据各自的相关政策,通过以下方式进行合作:①分享与人工智能技术及其治理相关的研究和行业实践;②促进和维持企业和整个社区负责任地使用和采用人工智能技术;和③鼓励研究人员、学术界和工业界之间的商业化机会和合作。(2)双方还认识到制定有助于实现人工智能的益处的伦理治理框架对于可信、安全和负责任地使用人工智能技术的重要性。鉴于数字经济的跨境性质,双方进一步认可确保此类框架尽可能与国际接轨的好处。(3)为此,双方应努力:①通过相关的区域和国际论坛,合作并促进框架的开发和接受,以支持可信、安全和负责任地使用人工智能技术("人工智能治理框架");和②在制定此类人工智能治理框架时,考虑国际公认的原则或指导方针。

② DEPA第8章"新兴趋势和技术"之第8.2条"人工智能"规定:(1)缔约方认识到,在数字经济中人工智能技术的使用和采用日益广泛。(2)缔约方认识到为可信、安全和负责任使用人工智能技术而制定道德和治理框架具有经济和社会重要性。考虑到数字经济的跨境性质,缔约方进一步承认不断增进共同谅解并最终保证此类框架的国际一致性的益处,从而尽可能便利在缔约方各自管辖范围之间接受和使用人工智能技术。(3)为此,缔约方应努力促进采用支持可信、安全和负责任使用人工智能技术的道德和治理框架(人工智能治理框架)。(4)在采用人工智能治理框架时,缔约方应努力考虑国际公认原则或指导方针,包括可解释性、透明度、公平性和以人为本的价值观。

③ See E-commerce Negotiators Seek to Find Common Ground, Revisit Text Proposals, https://www.wto.org/english/news_e/news22_e/jsec_23feb22_e.htm, visited on 31 May 2023.

④ 参见李墨丝:《WTO电子商务规则谈判:进展、分歧与进路》,《武大国际法评论》2020年第6期,第64页。

目前,在经贸协定和其他与数字经济有关的协定中出现了两处有代表性的关于人工智能的共识:DEPA第8.2条“人工智能”和SADEA第31条“人工智能”。二者的结构与内容颇为相似:首先,二者都重申了人工智能在数字经济中日益广泛的作用;其次,都指出实现人工智能益处的伦理治理框架对于可信、安全和负责任地使用人工智能技术的重要性,并强调鉴于数字经济的跨境性质,双方进一步认可确保此类框架尽可能与国际接轨的好处;最后,都强调成员方的人工智能合作与对国际共识的考量。以DEPA第8.2条为例,其重要性在于,此前国际贸易协定从未涉及过与人工智能等支撑数字经济之具体技术相关的问题。[①]不过,由于该条是用非强制意义的语言“尽力而为”(best endeavor)表达的,[②]它并不能被视为对开发人工智能治理框架的约束性承诺,而更像是一种宣示工具(signaling tool)。[③]

此外,虽然在当前国际法中尚不存在以人工智能为直接规制对象的多边国际条约,但双边层面的共识渐次出现。2020年10月,印度外交部表示,印度与日本已确定一项协议,将促进关键信息基础设施、5G技术、物联网、人工智能和网络空间等关键领域的合作。[④]2023年1月,美国国务院和欧盟委员会通信网络、内容和技术总局在白宫和布鲁塞尔总部同时举行线上仪式,签署了《人工智能促进公共利益行政协议》。根据该协议,美欧将会联手开发人工智能的社会应用,将有前途的人工智能研究成果运用在气候变化、自然灾害、健康和医学、电网优化、农业等领域。[⑤]在人工智能快速发展的阶段,人工智能的国际合作有利于应对全球治理的挑战。

---

① See Marta Soprana, The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block, 13 Trade, Law and Development 143, 161 (2021).

② 例如,第8.2条第3款表述为缔约方应努力(endeavor to)促进采用支持可信、安全和负责任使用人工智能技术的道德和治理框架(人工智能治理框架)。

③ See Marta Soprana, The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block, 13 Trade, Law and Development 143, 161 (2021).

④ See Dipanjan Roy Chaudhury, India, Japan Finalise Pact for Cooperation in 5G, AI, Critical Information Infrastructure, https://economictimes.indiatimes.com/news/defence/india-japan-finalise-pact-for-cooperation-in-5g-ai-critical-information-infrastructure/articleshow/78534833.cms. FE Online, India, Japan Finalise Landmark Pact to Enhance Cooperation on 5G Tech, AI, https://www.financialexpress.com/defence/india-japan-finalise-landmark-pact-to-enhance-cooperation-on-5g-tech-ai/2100387/#:~:text=India%20and%20Japan%20have%20finalised%20a%20landmark%20cyber-security,efforts%20in%20ensuring%20a%20free%20and%20open%20Indo-Pacific, visited on 31 May 2023.

⑤ See Under Secretary Fernandez Signs Administrative Arrangement with European Commission's Directorate General for Communications Networks, Content, and Technology (DG-CNECT) on Artificial Intelligence, https://www.state.gov/under-secretary-fernandez-signs-administrative-arrangement-with-european-commissions-directorate-general-for-communications-networks-content-and-technology-dg-cnect-on-artificial-intellig/, visited on 31 May 2023.

（四）部分法域的域内法发展显著

1.欧盟

和国际层面的人工智能治理规则相比，部分国家或地区的数字经济治理规则具有突出优势，尤以欧盟为典型。尽管欧盟的人工智能发展在全球范围并非领先，但欧盟围绕人工智能治理的规则体系相对成熟。欧盟有关人工智能的规则可分为直接规则与间接规则两类：前者是以人工智能为专题的战略政策与立法，后者则涵盖以数据为规制对象的配套规则。因此，欧盟的人工智能规则同时具备针对性强和配套规则全面的特点。欧盟的人工智能治理直接规则主要包括：（1）2019年4月发布的《可信赖的人工智能伦理准则》（European Commission Ethics Guidelines for Trustworthy AI）。[①]该准则提出了对可信任人工智能的七大核心要求：人类控制和监督，技术健全性和安全性，隐私性和数据管控，透明性，多样性、非歧视和公平性，社会和环境福祉，可追责性。（2）2020年2月发布的《人工智能白皮书——通往卓越和信任的欧洲路径》（White Paper on AI: A European Approach to Excellence and Trust）[②]。该白皮书主要围绕“卓越生态系统”（ecosystem of excellence）和“信任生态系统”（ecosystem of trust）两个方面的建设展开：前者意味着在私营部门和公共部门之间建立伙伴关系，以实现在整个价值链上调动资源；后者旨在让公民有信心采用人工智能应用，并为公司和公共组织提供使用人工智能进行创新的法律确定性。（3）自2021年4月《关于制定人工智能的统一规则（人工智能）并修正某些联合立法行为》的提案[③]首次提出以来，各个版本的《人工智能法案》（AI Act）草案。相关草案提出了人工智能应用场景风险评定制度，将人工智能应用场景分为“低、有限、高、不可接受”四个风险等级；在草案中以附件形式列举出了属于人工智能范围内的技术清

① See Ethics Guidelines for Trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, visited on 31 May 2023.

② See White Paper on AI: A European Approach to Excellence and Trust, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, visited on 31 May 2023.

③ See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF, visited on 31 May 2023.

单,以提供必要的法律确定性。捷克于2022年7月接任欧盟轮值主席国后,根据各代表团的反馈编写了《人工智能法案》折中草案第二、三、四版,并在此基础上于2022年12月提交。折中草案对人工智能系统下定义时引入技术概念,在分类上采取宽松的态度,避免高风险人工智能覆盖范围过宽;在降低高风险人工智能系统要求、增设通用人工智能系统编、调整法案适用范围和支持创新等方面扩大了对执法机关的授权和对中小企业的支持;加大了支持创新的力度,明确指出人工智能监管应在国家主管部门监督指导下建立受控环境,同时允许在现实世界中测试创新性系统。2023年5月,欧洲议会内部市场委员会和公民自由委员会通过了《人工智能法案》的谈判授权草案,这一草案将于6月提交欧洲议会全会表决。(4)2022年9月,欧盟委员会更新了《产品责任指令》(Product Liability Directive)提案,[①]并针对人工智能可能造成的具体损害提出了《人工智能责任指令》(Artificial Intelligence Liability Directive, AILD)提案。修订后的《产品责任指令》将所有规则扩展到配有人工智能的产品,但只要求制造商对物质损害负责,包括死亡、人身伤害以及医学上公认的心理伤害、财产损失或数据丢失。《人工智能责任指令》则专门确定了针对人工智能产品所致损害的适用规则,引入了"因果关系推定"原则,减轻受害者的举证责任和负担;同时,还规制人工智能的滥用,允许就侵犯基本权利的行为进行索赔。

欧盟的人工智能治理间接规则主要指其一系列的数据法案,具体包括:(1)2016年4月的《通用数据保护条例》(The European General Data Protection Regulation, GDPR)[②],该条例规定了个人数据自由流动的原则,引入了被遗忘权和数据可携带权,从个人对数据的自决权出发建构个人数据权利体系。[③](2)2018年11月通过的《非个人数据自由流动条例》(Regulation on the Free Flow of Non-Personal Data)。[④]该条例只适用于"欧盟境内个人数据之外的电子数据"。(3)2020年至2022年

① See New Product Liability Directive, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf, visited on 31 May 2023.

② See Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data ProtectionRegulation),https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, visited on 31 May 2023.

③ 参见汪庆华:《人工智能的法律规制路径:一个框架性讨论》,《现代法学》2019年第2期,第54-63页。

④ See Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN, visited on 31 May 2023.

间先后通过的三大数据法案之草案:《数据治理法案》(Data Governance Act)[①]《数字服务法案》(Digital Services Act)[②]和《数字市场法案》(Digital Markets Act)草案[③]。三者与之前生效实施的GDPR共同构成了欧盟最新的数字经济法律体系框架,为构建欧盟单一数字市场奠定制度基础。(4)2022年2月通过的《数据法案》(Data Act)草案[④]。作为对《数据治理法案》的补充,该法案为数据共享制定了一系列新规则,赋予消费者和企业对其所拥有数据更多的控制权。

在上述所有规则中,欧盟的《人工智能法案》最受关注。《人工智能法案》进一步缩小人工智能系统的定义为"机器学习或基于逻辑和知识的系统",以区别于传统系统。《人工智能法案》限制了人工智能的运用场景。比如,将禁止使用人工智能进行社会评分的范围扩大到私主体、将禁止利用特定群体脆弱性的规定增加适用于因其社会或经济状况而处于弱势地位的人、禁止执法机关在公共场所使用"实时"远程生物识别系统。此外,《人工智能法案》只用于研发目的和非专业目的的人工智能系统,不适用于国家安全与防御和军事目的的人工智能系统。在实施层面,《人工智能法案》限制了欧盟委员会的自由裁量权,为高风险人工智能系统和通用人工智能系统制定了共同的技术规范,简化了法案的合规框架。欧盟委员会可以指定欧盟测试机构提供独立的技术建议,同时,还有义务创建一个专家库。人工智能系统的用户也有义务在欧盟数据库中登记高风险的人工智能系统,以提高系统使用的透明度。

2.美国

美国也是较早对人工智能进行立法和监管的国家。美国国会在2012年通过了《联邦航空管理局现代化和改革法》,以消除无人机兴起和美国空域监管的冲突,重点是对产品系统进行监管。2015年,国会将人工智能的表述加入《修复美国地面交通法》,对自动驾驶车辆进行立法规制。2018年,联邦航空管理局在《再授权法》中嵌入对人工智能的规定。《2019财年国家授权法令》第238节规定了对国防领域的人工

① See Proposal for a Regulation on European Data Governance (Data Governance Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN, visited on 31 May 2023.

② Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and Amending Directive, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=EN, visited on 31 May 2023.

③ See Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842, visited on 31 May 2023.

④ See Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), https://ec.europa.eu/newsroom/dae/redirection/document/83521, visited on 31 May 2023.

智能进行主动监管的相关措施。联邦政府在2018年颁布了《关于美国工业领域人工智能峰会的概要》,评价了人工智能在工业领域运用的监管政策规定。2019年,白宫科学和技术政策办公室发布了《美国人工智能倡议》,优先调配更多联邦资金转向人工智能研究。美国州政府的监管反应更加迅速,加利福尼亚州、内华达州早就发布了自动驾驶汽车的监管规定。

美国商务部的非监管机构——国家标准与技术研究院于2023年1月26日正式公布《人工智能风险管理框架》,旨在指导机构组织在开发和部署人工智能系统时降低安全风险,避免产生偏见和其他负面后果,提高人工智能可信度,保护公民的公平自由权利。该报告分析了人工智能安全风险的独特性,指出其风险和收益可能受到来自技术方法、使用方式、系统交互、操作人员、社会环境等诸多社会因素的影响。该报告也强调人工智能的部署和利用可能会扩大、延续或者加剧个人和群体的不公平待遇。该报告是非强制性的指导文件,仅供机构组织自愿使用,但也为算法合规和人工智能风险管理提供了有益的参考。

3.英国

英国在2021年制定了《国家人工智能战略》和《数据保护和数字信息法案》,提出"用于人工智能监管的支持创新方法"。英国拟采取的监管方法侧重于高风险应用程序,这样就可以为风险小的技术提供创新空间。英国通信监管局、竞争与市场管理局、信息专员办公室、金融行为管理局和医疗保健产品监督管理局都参与到对人工智能的监管中,但是这些部门的监管不会转化为强制性义务。

综上,不同法域对人工智能的规制已经呈现出差异化。以欧美为代表的发达国家对人工智能的规制已呈现出两种不同的路径:欧盟的硬监管是为了规范外国技术,保护本土人工智能的发展;而美国的软治理是为了强化技术优势,力图消除人工智能技术发展的障碍。欧盟的硬监管主要体现在风险分级制度上,对风险小的人工智能系统采取轻度监管,对高风险系统采取强制性监管,对不可接受风险的系统采取禁用措施。被认定为高风险人工智能系统的公司必须遵循数据管理、信息提供与透明度、风险管理、人为监管等规定。这些企业在进入市场之前必须经过影响评估、治理机构合格评定、注册入录欧盟高风险数据库、签署合规声明等步骤。尽管欧盟在技术上落后于美国,但是其欲通过加强市场监管的方式强化数字主权,成为世界数字经济监管引领者,达到布鲁塞尔效应。不过,美国软治理的路径也在发生变化。美国联邦立法机关提出了130多项人工智能法规,显示出积极和进取的态度。美国还开始针对不同行业采取精细监管,联邦贸易委员会、金融监管部门都开始提出政策措施。

四、数字经济背景下人工智能对国际法的挑战

人工智能对于当前国际法的挑战主要在于,现有规则如何适应人工智能。直接规制人工智能的有约束力的国际规则缺位,这种缺位在国际法原则与具体规则领域均可被识别。本文选取主权原则和具体国际经贸规则两个方面加以讨论。

(一)排他性主权与统一数字空间之间存在张力

1.主权概念的扩张

人工智能对传统国际法的挑战首先在于在对传统威斯特伐利亚主权概念的挑战上。在通信与网络技术发展过程中,出现了数据主权(data sovereignty)概念。数据主权是指国家对数据和与数据相关的技术、设备、服务商等的管辖权及控制权。[①]在2020年欧洲议会的《欧洲的数字主权》(Digital Sovereign for Europe)报告中,欧盟将数字主权定义为"欧洲在数字世界中独立行动的能力",这包括促进数字创新的保护机制(protective mechanisms)和进攻工具(offensive tools)两个方面,并重点关注数据安全和人工智能问题。[②]但是,数据主权概念也并不足以涵盖人工智能对于主权的影响:由于人工智能已经构成了数字经济的基础,与人工智能有关的主权问题不仅关涉以数据安全、规制权等为表现的传统主权,还渗透到了国际活动的各个方面——如经贸规则中,从而与作为国际法律机制基本价值的发展权有关。[③]在这一背景下,出现了"人工智能主权"的概念,它在对内层面意味着主权国家对人工智能技术与实体的管辖权;在对外层面指国家享有自主决定和保护本国人工智能产业发展与规划而不受其他国家干扰之权利。[④]人工智能的综合性决定了人工智能主权虽然是最新出现的概念,但它比数据主权的内涵更为复杂,因其涉及人工智能在基础层、技术层、应用层三个层面的问题,而数据主权的问题仅是人工智能在基础层面临的问题。

---

① 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。

② See Digital Sovereignty for Europe, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf, visited on 31 May 2023.

③ 参见李蕾:《发展权与主权的互动是实现发展权的基本要求》,《政治与法律》2007年第4期,第22页。

④ 参见赵骏、李婉贞:《人工智能对国际法的挑战及其应对》,《浙江大学学报(人文社会科学版)》2020年第2期,第10-25页。

2.主权体系下的困境:不均衡的人工智能发展与数字割据

如果说不均衡的人工智能发展水平现状是致使人工智能国际规则缺位的现实原因,那么人工智能技术背后数据的天然流动性特征同主权治理的排他性特征间的冲突,则是造成人工智能国际治理困境的根本原因——有学者称之为数据隐私的"巴尔干化/割据"(balkanization)现象。[①]UNCTAD 2021年《数字经济报告》指出,目前世界范围内的技术竞争,尤其是人工智能技术的竞争,可能会导致数字空间和互联网出现碎片化,出现一种各自为政的数据驱动的数字经济,而违背了互联网自由、去中心化和开放的初衷。[②]不均衡的人工智能发展加剧数字割据,而数字鸿沟的扩大又加剧了人工智能水平的差异,这和数字经济对于开源的本质要求是相悖的。数字经济运行在开源基础上,未来可能需要包括公司、政府组织和个人贡献者在内的多方努力来确保开源软件生态系统的安全性和活力。[③]在人工智能时代,尽管政策制定者、评论方和消费者权益倡导者将透明度和问责制放在首位,包容性也是他们应该更加关注的设计特征之一。[④]

(二)人工智能在国际经贸规则中的性质认定与规制路径不明

对人工智能的主体性的讨论已屡见不鲜,但人工智能在国际法中的定性问题远不限于人工智能实体之主体性的讨论。仅是在以人工智能作为研发与应用客体为前提的讨论中,人工智能在现存国际经贸规制中的具体性质已足以引发争议,从而影响当前国际规则的适用。

1.人工智能在应用层——人工智能产品是货物还是服务?

人工智能在应用层面临的一个问题是,在现有国际贸易规则中,人工智能究竟属于货物还是服务。CPTPP在数字产品的定义条款中注释:"数字产品的定义不得被理解为反映一缔约方对通过电子传输的数字产品贸易应被归入服务贸易或货物

① See Fernanda G. Nicola & Oreste Pollicino, The Balkanization of Data Privacy Regulation, 123 West Virginia Law Review 61 (2020).

② See UNCTAD Digital Economy Report 2021, https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf, visited on 31 May 2023.

③ See Hila Lifshitz-Assaf & Frank Nagle, The Digital Economy Runs on Open Source. Here's How to Protect It, https://hbr.org/2021/09/the-digital-economy-runs-on-open-source-heres-how-to-protect-it, visited on 31 May 2023.

④ See Peter K. Yu, Beyond Transparency and Accountability: Three Additional Features Algorithm Designers Should Build into Intelligent Platforms, 13 Northeastern University Law Review 263 (2021).

贸易的观点”,从而直接回避了数字产品贸易归属于服务贸易还是货物贸易的争论。[①]

其次,不仅是广义的数字产品面临这一困境,即使相对成熟领域的产品定位亦如此,其中一个重要原因是人工智能技术服务与产品通常聚合为一体而打包流通。以自动驾驶系统(Automated Driving Systems, ADSs)为例,它是人工智能应用相对成熟的领域之一,但供应链上的各个国家尚无法就这种货物和服务的集成体究竟属于二者中哪一类达成共识,而这决定着WTO法律体系中仅适用于货物贸易的《技术性贸易壁垒协议》能否适用。[②]

此外,即使人工智能产品得以受到规则保护与规制,其所基于的数据却并不一定能享有类似待遇。例如,在数据被用以训练服务产品的情况下,仅产品受保护而数据不受保护。只有当数据本身是终端服务产品且成员在减让表中具体承诺时,《服务贸易总协定》规则方可适用。[③]

2.人工智能在数据层——数据可否作为投资?

人工智能的研发需要数据,这表明了数据的价值。然而,能否将数据投入人工智能训练的过程按照金融资本投资同样处理,仍存在疑问。换言之,数据可否作为一种资本,用于人工智能训练的数据投入是否为国际投资法意义上的“投资”(investment),仍存在疑问,这是人工智能在数据层面临的问题。

在规则层面上,这一问题是由自由贸易协定中的电子商务与投资章节二分所造成的。作为投资的数据应当按照哪种标准进行规制,在两种语境下是不一样的。例如,TPP是第一个将跨境数据流动约束力条款纳入电子商务章节的自由贸易协定,CPTPP作为其承继者也基本保留相关条款,但是,CPTPP对数据自由流动的要求只出现在第14章电子商务中,[④]而不在第9章投资中。而根据投资章节第9.19条,投资者只能就投资章节下的义务、投资授权、投资协议提出仲裁请求。[⑤]因此,

---

① See Footnote 3 to Chapter 14 Electronic Commerce, CPTPP: “The definition of digital product should not be understood to reflect a Party's view on whether trade in digital products through electronic transmission should be categorised as trade in services or trade in goods.”

② See Shin-yi Peng, Autonomous Vehicle Standards under the Technical Barriers to Trade Agreement: Disrupting the Boundaries?, in Shin-Yi Peng, *et al.,* Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration 127 (Cambridge University Press 2021).

③ See Thomas Streinz, International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy, in Shin-Yi Peng, *et al.,* Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration 184-185 (Cambridge University Press 2021).

④ CPTPP第14.11.2条规定:“当以电子方式进行跨境信息传输的活动是为了涵盖人的商业行为时,每一缔约方应当允许以电子方式进行跨境信息传输,包括个人信息。”

⑤ CPTPP第9.19条规定:(1)如一投资争端未能在被申请人收到根据第9.18.2条(磋商和谈判)提出的一书面磋商请求后6个月内得到解决,则:①申请人,可以自身名义,根据本节将下列请求提交仲裁:(i) 被申请人已经违反:(A) A节下一义务;(B) 一投资授权;或(C) 一投资协议;以及(ii) 由于此项违反或源于此项违反导致申请人遭受损失或损害……

投资者无法直接就投资过程中的数据流动限制向东道国主张权利。不过,由于电子商务章节第14.2.5条亦规定了对第9章的合规要求,[①]投资者可以限制数据流动构成对投资义务的违反为由向东道国主张权利。[②]类似地,通过对USMCA、RCEP的投资章节考察可知它们中均存在此问题。USMCA在第14.3条与其他章节的关系(relation to other chapters)中未提及第19章数字贸易与本章的关系,[③]RCEP投资章节的范围条款亦并未纳入该协定的"电子商务"章节。[④]

可见,对于数据自由流动的规定并不一定能很好地作用于投资领域中。其一,数据流动规则由于需要在传统投资实体待遇的框架下适用,可能受制于后者而遭克减。其二,在以数据为主要资源的投资活动中,甚至可能由于数据在程序上不构成投资而使得投资者由于法律意义上的投资不存在而无法主张权利。根本的解决方法还是应确立数据作为投资要素的性质。具体而言,这一判定需要结合数据在人工智能研发过程中的作用。若按照对管理的有效控制权(effective influence of management)标准,[⑤]数据投入无法比拟于股权投入,但按照更为广泛的Salini案所确立的经典四要件标准(实质承诺、特定时间段、风险承担以及有利于东道国发展),[⑥]数据可能根据其在特定项目中发挥作用的重要程度而构成"投资",典型的项目如人工智能的研发训练。

3.人工智能在算法层——源代码如何开放?

人工智能算法的代码蕴含着具体项目的技术特性,还可能内嵌算法偏差甚至

---

① "For greater certainty, the obligations contained in Article 14.4 (Non-Discriminatory Treatment of Digital Products), Article 14.11 (Cross-Border Transfer of Information by Electronic Means), Article 14.13 (Location of Computing Facilities) and Article 14.17 (Source Code) are: (a) subject to the relevant provisions, exceptions and non-conforming measures of Chapter 9 (Investment)..."

② See Andrew D. Mitchell & Jarrod Hepburn, Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer, 19 Yale Journal of Law & Technology 182, 229-230 (2017).

③ USMCA第14.2条规定:(1)本章适用于缔约方采取或维持的与下列有关的措施:①另一方的投资者;②涵盖的投资;和③关于第14.10条(性能要求)和第14.16条(投资和环境、健康、安全和其他监管目标),在该缔约方境内的所有投资……

④ RCEP第2条规定:(1)本章应当适用于每一缔约方采取或维持的、与下列有关的措施:①另一缔约方的投资者;以及②涵盖投资。(2)本章不得适用于:①政府采购;②一缔约方提供的补贴或补助;③一缔约方相关机构或主管机关行使政府职权时提供的服务……④一缔约方采取或维持的措施属于第8章(服务贸易)所涵盖的范围;以及⑤一缔约方采取或维持的措施属于第9章(自然人临时流动)所涵盖的范围……

⑤ See Free Trade Agreement between the EFTA States and the United Mexican States, http://secretariat.efta.int, visited on 31 May 2023.

⑥ See Salini Costruttori S.p.A. and Italstrade S.p.A. v. Kingdom of Morocco [I], ICSID Case No. ARB/00/4, para. 56.

歧视，这在浅层上意味着人工智能在同人类的交互中对自身身份的披露，深层上则意味着源代码的开放。人工智能算法的源代码开放本质上是一个透明度问题，算法公平（algorithmic fairness）被用以保证透明度，[①]因此，人工智能之算法应如何受到保护并适度开放，是人工智能在技术层面临的问题。

当前，诸多经贸协定章节对数字产品源代码作了规定。有的明确将源代码作为规制对象：例如，CPTPP第14.17条“源代码”，[②]USMCA第19.16条“源代码”[③]以及《美日数字贸易协定》第17条“源代码”[④]，均直接规定禁止对源代码的强制技术转让，同时亦保留披露算法的空间。有的虽未明确提及源代码，但对人工智能的可解释性、透明度提出原则性要求。如DEPA中的“人工智能”条款第4项规定，“在采用人工智能治理框架时，缔约方应努力考虑国际公认原则或指导方针，包括可解释性、透明度、公平性和以人为本的价值观”。RCEP则没有明确的透明度要求，仅将源代码问题加入有关电子商务的对话议程。[⑤]综上可见，目前的通常做法是谨慎限制源代码的披露情形，将其限缩于商业合同约定或当事国监管要求两类情况。事实上，欧盟在WTO电子商务谈判中曾主张引入“禁止成员国用国内法采取要求获取、传递软件源代码”的贸易条款，但这一主张遭到了欧洲学者的批判，认为其会限制欧盟对人工

① See Grazia Cecere, *et al.*, Fair or Unbiased Algorithmic Decision-Making? A Review of the Literature on Digital Economics, https://ssrn.com/abstract=3943389, visited on 31 May 2023.

② CPTPP第14.17条规定：(1)任何缔约方不得将要求转移或获得另一缔约方的人所拥有的软件源代码作为在其领土内进口、分销、销售或使用该软件或含有该软件的产品的条件。(2)就本条而言，需遵守第1款的软件限于大众市场软件或含有该软件的产品，不包括用于关键基础设施的软件。(3)本条中任何内容不得阻止：①在商业谈判合同中包含或实施与源代码的提供相关的条款和条件；或②一缔约方要求对软件源代码作出使该软件符合与本协定不相抵触的法律或法规所必需的修改。(4)本条不得理解为影响与专利申请或已授予专利相关的要求，包括司法机关对专利争端发布的任何命令，但需防范未经一缔约方法律或实践授权的披露行为。

③ USMCA第19.16条规定：(1)任何一方均不得要求转让或访问另一方主体拥有的软件源代码或该源代码中表达的算法，作为在其领土内进口、分发、销售或使用该软件或包含该软件的产品的条件。(2)在符合防止未经授权披露的保障措施的前提下，本条不排除一方的监管机构或司法当局要求另一方的人员为特定目的向监管机构保存和提供软件源代码或该源代码中表达的算法，以完成调查、检查、审查、执法行动或司法程序。

④ 《美日数字贸易协定》第17条规定：(1)任何一方均不得要求转让或访问另一方人员拥有的软件的源代码，或者转让或访问该源代码中表达的算法，作为进口或在其境内分发、销售或使用该软件或包含该软件的产品的条件。(2)在符合防止未经授权披露的保障措施的前提下，本条不排除一方监管机构或司法机关要求另一方人员保存和提供软件源代码或该源代码中表达的算法，以进行具体调查、检查、审查、执法行动或司法程序。

⑤ RCEP第12.16条规定：(1)双方认识到对话的价值，包括酌情与利益相关者对话，以促进电子商务的发展和使用。在进行此类对话时，双方应考虑以下事项：①根据第12.4条（合作）进行合作；②当前和新出现的问题，例如处理数字产品、源代码和跨境数据流以及金融服务中计算设施的位置；和……

智能的治理。[①]

“黑盒人工智能”(black box AI)程序如何得出结论是不可知的,而“白盒人工智能(white box AI)”如何得出结论是透明的。[②]相应地,有两类对于算法的监管模式:审计源代码的“白盒”方法,以及通过接口审计人工智能系统的输入和输出的“黑盒”方法。[③]目前经贸协定中的源代码规则仅规定单一的源代码披露,而未区分对于不同类型人工智能的不同监管方式,可能使得更需要监管的“黑盒人工智能”不受有效约束。此外,虽然对于源代码的监控是控制算法影响的重要途径,但人们企图避免的算法偏差依然很大程度上源自数据本身的偏差。因此,需要从源头监管数据的获取来源与筛选过程,并落实从伦理规则到技术规则的转化。

五、人工智能治理全球合作路径设计

在数字经济背景下,人工智能治理的全球合作首先是一个技术准则问题;而在数字博弈背景下,人工智能治理的全球合作也是一个国际政治问题。因此,人工智能治理的全球合作路径设计既需要关切数字经济治理本身的需求,也需要注重对于多元主体的覆盖以及对普遍法律环境的塑造。

(一)与数字经济规则密切结合,以数据治理为根本

数据治理与人工智能治理密切关联。其一,大数据是人工智能发展的基石之一,人工智能开发主体需要借助数据完成其工作。《在英国发展人工智能产业》报告对大数据和人工智能的关系进行了简要概括:“数据是为了开发人工智能,人工智能是为了管理数据”(data for developing AI, Al for managing data)。该报告指出,正是数据的快速增长催生了人工智能,获取大量数据和特定数据是成功训练机器学习算法的关键。[④]人工智能涉及三层空间——现实层、数据层和知识层中,数据层是人

---

① See Kristina Irion , AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code? , Study Commission by the German Federation of Consumer Protection Organizations (vzbv), Institute for Information Law. doi: 10.2139/ssrn.3786567.

② See The Difference Between White Box and Black Box AI, https://bigcloud.global/the-difference-between-white-box-and-black-box-ai/, visited on 31 May 2023.

③ See Kristina Irion , AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code? , Study Commission by the German Federation of Consumer Protection Organizations (vzbv), Institute for Information Law. doi: 10.2139/ssrn.3786567.

④ See Growing the Artificial Intelligence Industry in the UK, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf#:~:text=Growing% 20the% 20Artificial% 20Intelligence% 20Industry% 20in% 20the% 20UK,in% 20different% 20application% 20areas% 2C% 20and% 20coordinating% 20research%20capabilities, visited on 31 May 2023.

类复杂现实世界和经过人工建模或机器学习得到的结构化知识之间的连接层面。其二,人工智能的应用可能干扰用户的数据权利。例如,有学者指出机器与人类不同的遗忘特性会导致被遗忘权在人工智能领域适用的困境。[①]

虽然直接规制人工智能的国际规则十分有限,但国际社会已表现出对以人工智能为生产力来源之一的数字经济的高度关注。在人工智能助力数字经济发展的同时,人工智能产业有机会随数字经济国际治理框架的完善而得到规范。当前,全球数据治理框架的可能性与路径抉择未知,而大型私人公司主导的人工智能发展预示着私人治理时代的到来。为了维护人工智能领域的公共声音,需要从治理数据入手,而不只是治理算法输出的结果。[②]

(二)打造多元主体参与的协同共治模式

人工智能的要素有四个层面:人类主体、数据与算法、硬件设施与软件平台。其中,人类主体为人工智能的全球治理主体,其他为治理客体。人工智能全球治理的关键因素在于人类主体,除了政府主导进行行业规范设计外,国际行业协会和跨国数字巨头公司也是行业规范生成的参与者甚至主导者,诸多非政府主体已经推出了人工智能伦理倡议:除经典的IEEE关于自治和智能系统伦理的全球倡议外,2022年2月,我国商汤科技亦发布《2021企业社会责任报告》,将人工智能伦理与治理放在关键位置。[③]这些行业自治规则具有更强的时效性,且形式更加灵活,可为强制性的行业规范确立起到先导作用。

观察当前人工智能治理在国际层面的规则进化可知,人工智能的国际框架正在从两方面被构建:一方面,这一过程受益于非政府主体参与拟定的"超级软法",[④]其中典型的如IEEE等行业协会制定的准则。同时,其他有影响力的个体也积极参与规则形成的过程,如人工智能企业商汤科技与上海交通大学清源研究院联合发布的《AI可持续发展白皮书》入选联合国"人工智能战略资源指南"。另一方面,人工智能的国际规则也有向传统国际软法规制方式演化的趋势,这主要体现为正式与非正式国际组织(如UNESCO、OECD、G20)日益增长的参与和引导。

---

① 参见翟凯:《论人工智能领域被遗忘权的保护:困局与破壁》,《法学论坛》2021年第5期,第142-151页。作者指出,"由于现行法律并未充分考虑人类和机器在记忆与遗忘中的异同,故在现有的人工智能背景下,被遗忘权的实施面临技术瓶颈和规制障碍,无法实现其法律目的"。

② See Alicia Solow-Niederman, Administering Artificial Intelligence, 93 Southern California Law Review 633 (2020).

③ 参见《商汤科技首次发布企业社会责任报告 做有温度的人工智能》,https://www.sensetime.com/cn/news-detail/41164728?categoryId=72,2023年5月31日访问。

④ See Burri Thomas, International Law and Artificial Intelligence, 60 German Yearbook of International Law 91-108 (2017).

(三)防范地域与南北隔阂,营造全球普遍的法律环境

有观点警示,由于在人工智能时代,具有更强技术实力和更大数据掌控规模的国家很可能占据主导权,一种新的南北隔阂或将由此产生。[①]单一霸权主导的体系虽然是相对稳定的,但是人工智能的无国界性对全球治理提出了更高的要求,需要兼顾人工智能研发的推动和普惠性治理体系的构建。这一需求的背后是全球价值链的转型:全球优化的价值链(globally optimized value chain)将是数字技术与旧的低成本技术相结合的价值链,允许产品和服务之间的更大整合,并利用独立全球平台的商品和服务的交换。[②]

人工智能的全球治理要求多极化主体的主导,这既意味着对人工智能技术霸权的防范,还意味着多方参与治理模式(multi-stakeholder model)的必要性:科技公司等非政府主体的积极参与将有助于弥合技术人员和政策制定者之间的信息不对称。在国内层面,政策制定者应关注如何通过市场和规范等替代监管模式过滤公众意见并传递公共价值观,而不只是试图通过法律直接控制人工智能的算法技术。[③]而在国际层面,人工智能全球治理面临的更大挑战在于避免进一步分散的治理措施,而致力于实现全球普遍接受的法律环境。这需要一种新的思维方式——抛开传统的主权考虑,转向新的知识概念。[④]这时,软法由于其本身适用的国际化特点将发挥关键作用。[⑤]

六、结论

人工智能给现有国际法原则与国际经贸规则带来了综合性的挑战。当前,直接规制人工智能的有约束力的国际规则暂付阙如,但以主权国家治理的有效性为出发点,国际法在适应人工智能发展,这是国际法推动与适应数字经济转型的子议题。

---

① See Han-Wei Liu & Ching-Fu Lin, Artificial Intelligence and Global Trade Governance: A Pluralist Agenda, 61 Harvard International Law Journal 407 (2020).

② See Daniel Wagner, AI & Global Governance: How AI is Changing the Global Economy, https://cpr.unu.edu/publications/articles/ai-global-governance-how-ai-is-changing-the-global-economy.html, visited on 31 May 2023.

③ See Alicia Solow-Niederman, Administering Artificial Intelligence, 93 Southern California Law Review 633 (2020).

④ See Rolf H. Weber, Global Law in the Face of Datafication and Artificial Intelligence, in Shin-Yi Peng, *et al.,* Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration 69 (Cambridge University Press 2021).

⑤ See Carlos Ignacio Gutierrez, *et al.,* Lessons for Artificial Intelligence from Historical Uses of Soft Law Governance, 61 Jurimetrics 133-149 (2020).

具体而言，人工智能的出现加剧了主权概念的分化，而主权与人工智能背后的数据流动限制和技术发展不均衡加剧了数字经济层面的割据和不平衡现象。在国际经贸规则彰显数字经济时代要求的同时，人工智能在应用层、数据层和算法层仍对现有规则带来诸多挑战。人工智能在这三个层面的法律成熟度不尽相同：传统的国内法和国际法继续作用于人工智能的应用层，但已显示出落后与不足；正在初步形成过程中的全球数据治理的框架将成为人工智能数据层治理的重要依托；而在人工智能的算法层，现存的源代码披露条款对算法透明度做出了一定要求，但缺乏对于黑盒人工智能的针对性监管。

为应对这些挑战，需要打造人工智能国际法治理的全球合作路径。首先，人工智能在数字经济中的技术作用决定了数字经济规则、尤其是数据治理规则在人工智能治理中的决定性地位。其次，私营领域的人工智能发展意味着可依托其行业规则与标准生成“超级软法”。最后，亦应关注人工智能国际规则生成中的南北隔阂与话语权不对称，将人工智能的普惠性纳入规则制定的考量中，而这需要更广泛的政策支持和多方对话。

对于我国而言，首先需要关注国际经贸规则中的数字经济规则，依托区域经贸协定参与规则制定与治理。我国陆续发布了《关于规范人工智能军事应用的立场文件》和《中国关于加强人工智能伦理治理的立场文件》，在发出中国声音的同时，也为国际新规则的成型提供了方案。其次，在支持鼓励国内私人和公共主体算力建设的同时，积极参与人工智能治理国际软法形成中的伦理规则讨论与制定。目前，国家是人工智能产业规划和政策的主导者。我国于2015年就发布了人工智能的国家级政策文件——《中国制造2025》和《关于积极推进“互联网+”行动的指导意见》。国家新一代人工智能治理专业委员会发布的《新一代人工智能伦理规范》和中央网信办发布的《互联网信息服务算法推荐管理规定》都包含了透明度、可解释性、可理解性等伦理规范。此外，完善国内传统部门法制度以应对人工智能应用已经导致的问题是当务之急。例如，上海市人大于2022年9月发布了《上海市促进人工智能产业发展条例》，推动人工智能与经济、生活、城市治理等领域深度融合，打造人工智能世界级产业集群。针对生成式人工智能，国家互联网信息办公室于2023年4月发布《关于〈生成式人工智能服务管理办法（征求意见稿）〉公开征求意见的通知》，该办法将是我国首个针对生成式人工智能产业发布的规范性政策文件，对利用生成式人工智能产品提供聊天和文本、图像、声音生成等服务的组织和个人的责任进行了规定。提供者承担对产品生成内容的责任和个人信息保护义务，且在向公众提供服务前需向国家网信部门申报安全评估等。随着人工智能治理制度的完善，发布一部人工智能的基本法将是我国在下一阶段人工智能治理中的核心任务。

International Law Regulation of Artificial Intelligence in the Dual Context of the Digital Economy and the Digital Competition

Abstract: The issue of international legal governance of artificial intelligence first appeared in the context of the rise of the digital economy. As the competition under the background of the digital economy has essentially transformed into a competition for technological hegemony, artificial intelligence has also evolved from an object of technological governance among states to a tool in the competition for technological hegemony. It is possible and necessary to apply international law to artificial intelligence governance and overcome the system risks. The existing international governance of artificial intelligence presents four main characteristics: the content is mainly ethical rules; the form is mainly soft laws formulated by non-government entities; although direct regulatory rules are scarce, indirect regulatory rules are gradually improving; the development of domestic laws in certain jurisdictions is remarkable. In the context of the digital economy, the challenge of artificial intelligence to international law is generally manifested in the tension between exclusive sovereignty and unified digital space. Specifically, in the field of international economic and trade rules, it is reflected in the difficulty in the identification of the nature of artificial intelligence, as well as the unclear regulatory path of artificial intelligence. In order to achieve global cooperation in artificial intelligence governance, first of all, it should be closely combined with the rules of the digital economy, with data governance as the foundation; second, a governance model should be created with the participation of multiple stakeholders and collaborative governance; finally, regional and north-south barriers should be prevented in the process of creating a universal legal environment.

Key words: digital economy; digital competition; artificial intelligence; international law

（责任编辑:肖军）