对外经济贸易大学法学院
博士申请学位科研成果考核折算科研文献

文献形式（文献综述/读书报告）：文献综述

文献题目：人工智能训练数据跨境流动规则的国际比较研究

博士论文题目：人工智能训练数据跨境流动规则的国际比较研究

导　　师：熊光清教授

作者姓名：张素敏

专　　业：国际法

学　　号：202300540116

人工智能训练数据跨境流动规则的国际比较研究
文献综述

摘 要：生成式人工智能的训练、研发与迭代应用，均依赖大规模、多源异构且持续更新的数据资源作为基础支撑。人工智能训练数据作为新的生产要素，其全球流动性随着人工智能产业的普惠性而被深刻影响。由于全球人工智能军备竞赛，主要国家和地区开始调整数据跨境流动规则，人工智能训练数据跨境流动规则的冲突进一步加剧。本综述聚焦于人工智能数据跨境流动规制，系统梳理相关理论与实践研究，探讨现有数据跨境流动规制现状及问题。本研究梳理并讨论各国规制数据跨境流动和国际社会协调规制的理论基础，为研究人工智能训练数据跨境流动规则提供理论基础。各国在数据主权、隐私保护、国家安全与数字贸易自由化等方面的立场差异深刻影响规则冲突。本综述进一步分析全球数据跨境流动的治理框架，包括单边、双边和多边机制，并探讨其规制成效在人工智能训练数据下的失效。揭示现行国内和国际规则在保障安全与促进人工智能效能全球扩散之间的困境。中国在数据跨境流动治理中逐渐明晰立场，展现以数据安全为基础、促进新型全球化的努力。本综述为后续研究提供理论基础和实践参考，强调在人工智能训练数据流动规制中须进行国际协作与制度创新。

关键词：生成式人工智能；训练数据跨境流动；规则冲突；国际协调

围绕问题“人工智能训练数据跨境流动规则的国际比较研究”的研究，既有研究可以被分为人工智能训练数据跨境流动的理论基础、相关国内研究和国外研究。中外文献均指出，双边与多边规则在应对人工智能引发的数据治理新问题方面呈现出由碎片化博弈的特征，到逐步寻求制度协调的转变。其中多边规则中普遍存在隐私保护与国家安全二元张力，尤其在人工智能系统带来的算法黑箱、不可预见性与跨境处理不透明问题下，传统规则存在适配滞后、国际规则存在协调失灵的问题。下文将分别对三个板块的既有研究成果进行梳理并评述。

一、理论基础

（一）数据主权理论

数据主权（data sovereignty）作为一个新兴概念，近年来在国际法、国际关系和数字治理领域引起广泛关注。数据主权的理论基础主要根植于国际法中的主权原则和新兴的数字治理理论。 主权被理解为基于国内制度安排、国际机制和其他国家实践提出权威性主张的能力。[1]Polatin-Reuben 与 Wright 指出数据主权不仅是技术问题，还涉及国家安全、公民隐私和经济利益的平衡。随着云计算、大数据和人工智能的快速发展，数据主权的内涵不断扩展。[2] Anupam Chander & Uyên P. Lê首次系统提出“数据主权”概念，定义为国家对其境内生成、存储和传输的数据享有管辖权和控制权，类似于传统国际法中的领土主权。 Irion 指出数据主权是对网络主权的延伸，强调国家在数字空间的自主决策权。[3]近期研究如 Hummel et al.则指出，数据主权不仅限于国家层面，还涉及个人信息自决权和社区层面的数据控制权，呈现多维特征。[4]

当前国际法层面尚未形成明确的数据主权规则，但“数据主权”正逐步成为各国调整数据跨境流动的重要依据。在国家实践上，欧盟通过《通用数据保护条例》（General Data Protection Regulation, 以下简称 GDPR）提出“数据属地管辖”原则，美国则依靠契约管辖逻辑保护自身利益，中国强调在联合国、金砖国家、上合组织等平台推动数据治理国际规则的中国倡议，呼吁尊重各国对数据的主权。同时，数据主权通过国内立法、国际条约和多边谈判得以体现。Aaronson

---

[1] Keasner SD, *Sovereignty: A Institutional Perspective*, 21 CAMPARATIVE POLITICAL STUDIES 66, 66-94(1988).

[2] Dana Polatin-Reuben & Joss Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet, Conference: 4th USENIX Workshop on Free and Open Communications on the Internet*, https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (last visited October 10, 2026).

[3] Kristina Irion, *Government Cloud Computing and National Data Sovereignty*, 4 POLICY & INTERNET 40, 40-71(2012).

[4] Patrik Hummel, *Matthias Braun, Max Tretter and Peter Dabrock, Data sovereignty: A Review*, 1 BIG DATA & SOCIETY 1, 1-17(2021).

与Leblond分析了GDPR如何通过严格的隐私保护和数据本地化要求间接强化数据主权。[5]《中华人民共和国数据安全法》（以下简称《数据安全法》）和《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）则明确规定了数据跨境传输的限制，体现了中国的数据主权立场。国际条约方面，数据主权在《区域全面经济伙伴关系协定》（Regional Comprehensive Economic Partnership，以下简称RCEP）和《美墨加协定》（Agreement between the United States of America, the United Mexican States, and Canada，以下简称 USMCA）中有所体现。Chander指出，USMCA的电子商务章节倾向于数据自由流动，而RCEP则允许成员国保留一定的数据主权空间，反映了国家间的立场分歧。此外，联合国网络空间国际行为规范的讨论也涉及数据主权，强调网络空间的国家主权平等。有学者指出，《联合国宪章》（Charter of the United Nations）中对国家主权、互不干涉的基本原则，仍适用于数字空间。[6]因此，数据主权可以被看作是国际法“主权平等”原则在数字时代的延伸与适用。但也有观点质疑，在数据天然跨境流动的技术特性下，是否适用传统的“属地管辖”逻辑仍需进一步论证。[7]

在人工智能语境中，数据主权的理论正当性尤为突出。人工智能系统依赖大规模数据进行训练，数据主权直接关系到国家在人工智能发展上的“原材料控制权”。此外，算法歧视、技术出口、跨境数据监管等问题的复杂化，也对国家层面行使数据主权提出了更高要求。由此加剧全球数据治理规则的碎片化，以欧盟“数字单一市场”战略为代表的区域性数据主权框架成为研究热点。[8]最后，Pohle与Thiel探讨了互联网例外主义（caber exceptionalism）和互联网治理（internet governance）对传统主权的挑战，以及重新成为数字政策原则制定的基础，从而揭示了数据主权作为政治和政策领域的一种话语实践，而非作为法律或组织概念。[9]

（二）信息隐私保护理论

信息隐私保护（information privacy protection）是指个人对其个人信息在收集、存储、处理和传输过程中的控制权，以及免受未经授权访问或滥用的权利。在国际法视角下，“信息隐私”已成为数据跨境流动合法性的重要前置条件。信息隐私保护理论关注个人对其数据的控制权，强调通过法律、技术和伦理手段保

---

[5] Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 245, 245-272 (2018).

[6] 冉从敬、刘妍：《数据主权的国际博弈与我国进路》，载《图书馆论坛》2023年第9期，第8-9页。

[7] Jennifer Daskal, The Un-Territoriality of Data, 125 YALE LAW JOURNAL 326, 365-377 (2015).

[8] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 232 (David Pervin, 2020).

[9] Julia Pohle & Thorsten Thiel, *Digital Sovereignty*, 9 INTERNET POLICY REVIEW 1, 5 (2020).

护数据主体免受未经授权的处理或滥用。[10]在中国，其通常被定义为以个体对其个人信息的知情、控制、限制、删除等权能为核心的复合型人格权保障理论，[11]并嵌入于个人信息保护法体系、数据治理结构以及跨境流动规制之中。信息隐私保护的核心原则包括数据最小化、透明性、同意及数据主体权利。[12]在人工智能背景下，该理论不仅涵盖传统个人数据，还包括人工智能生成的推断数据、非个人数据及算法模型，因其可能间接揭示个体身份或敏感信息。

信息隐私保护的理论根基主要源于国际法中的人权法和数据治理理论。首先，隐私权作为基本人权，受到《世界人权宣言》（Universal Declaration of Human Rights）第 12 条[13]和《公民权利和政治权利国际公约》（International Covenant on Civil and Political Rights）第 17 条[14]的保护。这些条款确立了个人免受任意干涉私人生活的权利，为信息隐私提供了法律基础。信息自决权（informational self-determination）是信息隐私保护的核心理论。德国联邦宪法法院在 1983 年的“人口普查案”中首次提出这一概念，强调个人对其数据的控制权。此外，西方法律传统中的自由主义理论和欧洲的尊严理论也为信息隐私提供了哲学支撑。[15]DeNardis 则从从技术治理视角指出，信息隐私保护不仅是法律问题，还涉及技术设计和全球治理的互动。[16]

Warren 与 Brandeis 首次提出隐私权概念，奠定了信息隐私的理论基础，强调个人免受外界干扰的权利。[17]随着数字技术的发展，信息隐私的内涵从物理隐私扩展到数据隐私，涵盖个人数据的自主控制和保护。Solov 提出，信息隐私不仅是个人权利，还涉及社会和经济维度，尤其在大数据和人工智能时代，数据滥用可能导致歧视和权力失衡。[18]Schwartz 与 Peifer 进一步指出，信息隐私保护在全球范围内因文化、法律和技术差异而呈现多样化特征，特别是在跨境数据流动的背景下，成为国际法研究的前沿课题。[19]我国学界对信息隐私权的理解曾侧重

---

[10] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 418-420 (Michael Aronson eds., 2008).

[11] 张新宝：《论个人信息权益的构造》，载《中外法学》2021 年第 5 期，第 1144-1166 页。

[12] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 NEW YORK UNIVERSITY LAW REVIEW 771, 771-772 (2019)

[13] 《世界人权宣言》第 12 条：“任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击。人人有权享受法律保护，以免受这种干涉或攻击。”

[14] 《公民权利和政治权利国际公约》第 17 条：“一、任何人之私生活、家庭、住宅或通信，不得无理或非法侵扰，其名誉及信用，亦不得非法破坏。二、对于此种侵扰或破坏，人人有受法律保护之权利。”

[15] Julie E. Cohen, *What Privacy is For?* 126 HARVARD LAW REVIEW 1904, 1904-1933(2013).

[16] LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 23-51(William Frucht, 2020).

[17] Samuel D. Warren II, Louis Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193, 220(1980).

[18] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STANFORD LAW REVIEW 1393, 1462 (2008).

[19]Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy*, 106 GEORGETOWN LAW JOURNAL 115, 156-167 (2017).

于通讯自由和居所安宁等物理意义上的自由，但随着大数据与人工智能的发展，隐私权研究迅速转向“信息隐私”维度。《中华人民共和国民法典》第 1034 条首次承认“个人信息权益”作为独立人格权，并在《个人信息保护法》中得到全面制度化，标志着中国信息隐私保护理论从抽象伦理命题转向具有法律效力的规范体系。[20]

在国际法实践中，信息隐私保护体现在国内立法、国际条约和区域框架。GDPR 被视为全球信息隐私保护的标杆。Casey, et al.分析 GDPR 通过严格的数据处理原则、同意机制和跨境数据传输规则，显著提升了全球隐私保护标准。[21]《个人信息保护法》则结合国家安全和数据主权，规定了数据本地化和跨境流动的限制，体现了亚洲特色的隐私保护模式。国际条约方面，《欧洲人权公约》（European Convention on Human Rights,）第 8 条明确保护隐私权，相关判例[22]进一步阐释了信息隐私的法律边界。此外，亚太经合组织（Asia-Pacific Economic Cooperation，以下简称 APEC）的跨境隐私规则体系（Cross-Border Privacy Rules，以下简称 CBPR）试图在数据自由流动与隐私保护间寻求平衡。[23]2013 年，联合国大会首次通过“数字时代的隐私权”决议[24]强调了信息隐私的全球重要性。

随着人工智能模型发展涉及种群特征的预测，是否需要超越个体隐私，发展“群体信息权”成为新议题，[25]进言之“群体隐私”是否应当获得法律承认？在大模型语料训练、社交网络分析等情境中，个体隐私边界模糊，部分研究主张从个体控制权扩展至“群体隐私权”或“集体信息权益”理论，强调不仅要保护输入数据，还要对人工智能模型产生的输出推论数据进行法律规制。[26]

同时，人工智能环境下数据的再利用与自动化处理使得一次性的“知情+同意”不足以保护隐私利益，[27]传统知情同意机制面临失效困境。而越来越多学者试图将信息隐私与算法规制融合，主张建立算法透明、数据可控和隐私权利的协

---

[20] 王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》，载《当代法学》2022 年第 1 期，第 3 页。

[21] Bryan Casey, Ashkon Farhangi & Roland Vogl, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECHNOLOGY LAW JOURNAL 145, 188(2019).

[22] 如欧洲人权法院的 S. and Marper v. the United Kingdom, ECtHR, Judgement para.96-124 (2008)

[23] Greenleaf & Graham, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 17-45, 5-6(2017).

[24] The Right to Privacy in the Digital Age: Resolution/Adopted by the General Assembly, A/RES/68/167, https://digitallibrary.un.org/record/764407?v=pdf#files (last visited October 10, 2026).

[25] Dencik, L., & Sanchez-Monedero, J., *Data Justice*, 11 INTERNET POLICY REVIEW 1, 13(2022).

[26] Sandra Wachter, Brent Mittelstadt & Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 41 COMPUTER LAW & SECURITY REVIEW 1, 1-2 (2021).

[27] Brent Mittelstadt, *Principles Alone Cannot Guarantee Ethical AI*, 1 NATURE MACHINE INTELLIGENCE 501, 501-507(2019).

同治理模式。主张突破个人控制的传统思维，构建基于技术背景的信息风险评估与分级治理机制，将信息隐私置于整体国家治理与技术伦理结构之中。如“算法问责”“人工智能影响评估”等机制不断涌现，重塑传统以“知情+同意”为核心的隐私框架。[28]信息隐私强调“知情+控制”，但在人工智能自动化决策场景中，这一权利很难实际落实。例如，用户无法理解模型逻辑，或根本无法撤回使用。这一问题引发了对“解释权”“不被画像权”等新型权利的扩张性建构。

如何在信息隐私保护与国家数据主权之间找到平衡，成为数据跨境领域学界争议焦点。一种观点认为应以国家安全为优先，另一种则强调应当通过数据本地化与标准合同条款协调处理。Cohen 提出，信息隐私保护须平衡个人控制权与数据驱动的社会利益，如公共健康或科研需求。[29]学界开始展开跨境规则对接机制探索，关注信息隐私保护与“标准合同条款”“数据出境安全评估办法”的内在一致性，主张制定“信息隐私影响评估报告”作为出境备案要件之一。[30]比如，GDPR 标准的域外影响催生数据流动的适当性机制，呼唤统一的跨境隐私规则或桥梁机制。

（三）国家安全理论

国家安全理论传统上指国家通过军事、外交和经济手段维护领土完整、政治独立和公民福祉的能力，最早主要用于军事安全、政治稳定等传统领域。Wolfers 于 1952 年首次系统定义国家安全，强调保护国家免受外部威胁的核心目标。[31]冷战时期，国家安全主要聚焦于军事对抗和地缘政治竞争。全球化与技术进步推动了国家安全概念的扩展，涵盖经济安全、能源安全、网络安全和人类安全等非传统领域。Baldwin 提出国家安全是一个多维概念，需明确“对谁的安全”“何种威胁”及“通过何种手段”。[32]2015 年，《中华人民共和国国家安全法》（以下简称《国家安全法》）通过后，中国学界普遍将国家安全视为一个多维的系统性结构。在人工智能和数据跨境流动背景下，数据安全成为国家安全理论中的一个新兴维度。2021 年《数据安全法》明确提出“数据安全是国家安全的重要组成部分”，随后数据主权、数字国家安全成为研究热点。

数字时代的到来进一步重塑了国家安全概念。DeNardis 将网络安全和数据安

---

[28] Mireille Hildebrandt, *Algorithmic Accountability and the Rule of Law*, 376 PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A 2128, 2130 (2018).

[29] Julie E. Cohen, *Surveillance vs. Privacy: Effects and Implications*, in Cambridge Handbook of Surveillance Law (David Gray & Stephen E. Henderson eds., 2017).

[30] 石佳友，曾佳：《个人信息保护影响评估：制度内涵与完善路径》，载《西北工业大学学报（社会科学版）》2022 年第 4 期，第 97 页。

[31] Arnold Wolfers, “*National Security” as an Ambiguous Symbol*, 67 POLITICAL SCIENCE QUARTERLY 481, 481-502 (1952).

[32] David A. Baldwin, *The Concept of Security,* 23 REVIEW OF INTERNATIONAL STUDIES 5, 5-26 (1997).

全纳入国家安全框架，强调数字基础设施对国家生存的重要性。[33]Heng 与 McDonagh 提出“综合安全”（comprehensive security）理念，主张整合传统与非传统威胁的应对策略。[34]近年来，气候变化、公共卫生危机和人工智能的军事化进一步拓宽了国家安全的边界。国家安全理论的理论根基主要源于国际法中的主权原则、现实主义国际关系理论和新兴的全球治理理论。中国学界普遍认为，国际法框架中存在一定国家安全的例外空间，如《关税与贸易总协定》（General Agreement on Tariffs and Trade，以下简称 GATT）第 21 条、经合组织《关于隐私保护和个人数据跨境流动的指南》（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data，以下简称 OECD《隐私指南》）等都为国家以安全理由限制数据流动提供正当性基础。但也有学者指出，滥用国家安全例外可能引发数据保护主义。[35]

在国际法实践中，国家安全通过国内立法、国际条约和多边机制得以体现。尽管尚无一部统一的“全球数据安全公约”，但数据安全已逐渐成为国家间博弈的重要焦点。国内层面，各国通过立法强化国家安全。以中国为例，《国家安全法》涵盖了军事、经济、网络等多个领域，体现了综合安全理念。2001 年《美国爱国者法案》（Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act）通过扩大政府监控权限，优先保障国家安全，但引发隐私权争议。另一方面，美国则以国家安全名义强化对中国企业的投资限制与数据控制，如禁止 TikTok 和华为事件，引发数据主权与国家安全例外之间的国际法争议。[36]欧盟 GDPR 则通过“数据保护适当性决策”保障本地数据不被任意流出。国际条约方面，《联合国宪章》第 51 条规定了国家基于自卫权的合法安全措施，适用于传统和诸如网络攻击新兴威胁。Schmitt 进一步探讨了网络空间的国家安全规范，[37]提出国家可在遭受重大网络攻击时援引自卫权[38]。此外，区域性安全框架中诸如北约集体防御机制和《非洲组织统一宪章》（Charter of the Organization of African Unity）中的和平与安全条款，体现了国家安全在多边合作中的实践。

---

[33] LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 59-132 (William Frucht eds., 2020).

[34] YEE-KUANG HENG & KEN MCDONAGH, RISK, GLOBAL GOVERNANCE AND SECURITY：THE OTHER WAR ON TERROR 26-28(Aaron Karp &Regina Karp eds., 2009)

[35] 邵怿：《跨境数据流动规制的自由化与本地化之辩》，载《政法论丛》2023 年第 5 期，第 139 页。

[36] 廖丽、武子微：《国家安全例外条款在数据跨境流动中的适用研究》，载《国际贸易》2024 年第 8 期，第 87 页。

[37] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE JOURNAL OF INTERNATIONAL LAW 1, 2 (2017); Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace,* 95 TEXAS LAW REVIEW 1639, 1641(2017).

[38] 【美】迈克尔·施密特主编：《网络行动国际法塔林手册 2.0 版》，黄志雄等译，社会科学文献出版社 2017 年版，第 342-356 页。

在数字领域，国家安全与数据治理密切相关。欧的 GDPR 虽以隐私保护为核心，但其数据本地化要求也服务于国家安全目标，《数据安全法》则明确将数据安全纳入国家安全框架。在人工智能背景下，安全不再局限于数据本身，拓展至算法安全和模型安全等新领域。[39]有学者主张中国应当强化国际话语建构与规则塑造能力，通过“一带一路”数据走廊、数字自贸协定推动中国提出的数据安全规则获得国际采纳。

（四）国际协调理论

国际协调理论（international coordination theory）是国际法和国际关系领域的重要理论框架，用于分析国家在全球治理中的合作机制、规则制定及行为协调。其核心在于解释国家如何通过规则、规范和制度实现利益最大化。国际协调理论为理解国际法在全球治理中的作用提供了重要框架。从新自由制度主义的起源到建构主义和社会化理论的补充，该理论不断演进，适应了全球化背景下的新挑战。当前，国际法研究需进一步关注非国家行为体、软法机制和新兴技术领域的协调问题。

国际协调理论的根源可追溯至 20 世纪 70 年代的国际关系研究，特别是新自由制度主义的兴起。1984 年，Keohane 奠定了国际协调理论基础，提出国际协调是国家在无政府状态下通过制度化合作实现共同利益的过程。他强调国际制度通过降低交易成本、提供信息透明度和建立信任，促成国家间的协调行为。[40]Young 进一步发展了这一理论，提出制度谈判概念，认为国际协调的核心是通过谈判形成具有法律约束力的规则体系。[41]

在国际法领域，1995 年，Slaughter 将协调理论应用于全球治理，提出“跨政府网络”（transgovernmental networks）概念，强调非正式协调机制在国际法实施中的作用。她认为，国际协调不仅是国家间正式条约的结果，也包括监管机构间的非正式合作，如金融监管或环境标准协调。国际协调理论在国际法领域的应用广泛，尤其体现在多边条约、国际组织和争端解决机制中。[42]例如，Chayes 和 Chayes 于 1995 年提出“管理式合规”（managerial compliance）理论，认为国际协调依赖于持续的对话和能力建设，而非单纯的强制执行。WTO 的争端解决机制和《巴黎气候协定》（Paris Agreement）的定期审查机制均体现了这一逻

---

[39] 张龙辉：《数字社会建设中的算法安全风险及其化解策略》，载《东北师大学报（哲学社会科学版）》2024 年第 2 期，第 134-139 页。

[40] 【美】罗伯特·基欧汉：《霸权之后：世界政治经济中的合作与纷争》，苏长和、信强、何曜译，上海人民出版社 2006 年版，第 49-65 页。

[41] Iris Marion Young, *Polity and Group Difference: A Critique of the Ideal of Universal Citizenship*, 99 ETHICS 250, 274(1989).

[42] Anne-Marie Slaughter, *International Law in a World of Liberal States*, 6 EUROPEAN JOURNAL OF INTERNATIONAL LAW 503, 503-538(1995).

辑。此外，国际协调理论还推动了对全球公共品（global public goods）治理的研究。

近年来，国际协调理论在应对全球性挑战时展现出新的发展方向。技术进步和数字化治理为协调机制带来新机遇与挑战。例如，Aaronson 和 Leblond 研究了数据保护领域的国际协调，指出 GDPR 如何通过“布鲁塞尔效应”影响全球数据治理标准。[43]此外，人工智能和网络安全领域的国际协调成为新兴热点，Crootof 探讨了非国家行为体在制定技术标准中的作用，挑战了传统国家中心协调模型。[44]在国际法理论层面，近期研究强调碎片化与协调的关系。Benvenisti 和 Downs 分析了国际法体系碎片化如何削弱协调效果，提出通过元规范（meta-norms）整合不同法律体系的可能性。[45]另一方面，Pauwelyn 等探讨了国际法与非正式规范的互动，认为协调理论需适应多元化和多层次的治理结构。[46]

二、国内研究

（一）人工智能背景下完善数据跨境流动规则的必要性

全球化进入一个由数据流定义的新时代，越来越多的经济活动由数据驱动，[47]在以人工智能为代表的数字技术驱动的新一轮全球化中，数据、算法、算力是人工智能发展的三驾马车，其中算法也与数据密切相关。生成式人工智能技术耦合了跨境数据流动的产业发展进程，跨境流动数据成为数字贸易发展的生产要素和重要载体。[48]即人工智能技术训练数据和用户场景数据的跨境流动对人工智能大模型训练和人工智能企业出海发展至关重要。

数据跨境流动将加速全球创新知识的共享应用、催生跨领域技术的融合创新、助推人工智能算法技术创新和模型创新，促进科技进步与产业创新。数据是影响算法迭代优化的核心关键，数据的规模、质量和多样性直接影响模型的精度和泛化能力。推动数据跨境流动进而提升数据要素多样性和质量，发挥数据要素

---

[43] Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 245, 245-272(2018).

[44] Rebecca Crootof, *Regulating New Weapons Technology*, in THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT (Eric Talbot Jensen & Ronald T.P. Alcala, eds., 2019).

[45] Eyal Benvenisti & George W. Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STANFORD LAW REVIEW 595, 624 (2007).

[46] Joost Pauwelyn, *Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How They May Outcompete WTO Treaties*, 17 JOURNAL OF INTERNATIONAL ECONOMIC LAW 739, 739-751(2014).

[47] 洪永淼、张明、刘颖：《推动跨境数据安全有序流动引领数字经济全球化发展》，载《中国科学院院刊》2022 年第 10 期，第 1418 页。

[48] 聂新伟、卢伟：《数字经济全球化背景下中国数字贸易开放的路径选择》，载《区域经济评论》2024 年第 4 期，第 137 页。

对人工智能创新的促进作用。[49]跨境数据流动为人工智能算法提供了跨越国界的训练数据，不同国家和地区，涵盖广泛行业和应用场景的海量数据，训练人工智能模型的数据规模倍增，显著提升机器学习模型的准确性和泛化能力。[50]学者提及生成式人工智能的迭代发展必须依赖数据要素的自由流动及合理配置。[51]同时，云计算、物联网等跨境数据流动技术为生成式人工智能的发展了基础支撑，数据跨境流动对生成式人工智能发展具有关键意义。[52]

数据融合是对于消除人工智能偏见、促进社会公平具有重要意义。[53]即自由安全地跨境传输数据的能力使人工智能系统能够访问各种信息，这是消除偏见、实现人工民主化的关键要素。[54]同样，当人工智能训练的信息其收集和使用是来自有限的地理区域或人口，自然会导致训练数据的偏见，导致人工智能模型算法偏见，造成社会不平等和歧视。[55] 同时，数据跨境流动促进了跨国界、跨学科、跨行业的创新合作网络形成，通过数据集、算法模型、研究方法、专业人才的全球共享合作，助力更快攻克技术难关，提升算法性能。从而助推全球范围内人工智能技术的进步，全球技术创新和社会进步。

（二）数据跨境流动的理论基础与治理理念

数据跨境流动规则的研究首先需要明确其理论基础与治理理念。中文文献中，学者们从数据主权、数据自由流动与数据安全三个维度展开深入探讨，形成了数据主权安全理论和自由与安全并重的核心治理理念。强调在总体国家安全观下，通过数据分级分类、例外条款设计等手段实现自由流动与安全保护的动态平衡。

一是数据主权与国家安全的问题，数据主权是数据跨境流动治理的基石。早年，齐爱民从大数据时代的数据安全特点出发，提出应秉持“发展与安全并重”的原则，通过理念变革与制度创新应对数据跨境流动的动态性与综合性风险。[56]

---

[49] 周宁南：《人工智能时代数据跨境管制趋势分析》，载《中国信息安全》2024 年第 7 期，第 43 页。

[50] 陈龙江、唐静：《数据跨境流动赋能新质生产力：理论机制、关键挑战与实践路径》，载《战略决策》2024 年第 4 期，第 63 页。罗早西：《人工智能如何影响跨境数据流动规》，载《中国外资》2023 年第 19 期，第 44 页。

[51] 张亮、陈希聪：《生成式人工智能背景下的跨境数据安全规制——基于 DeepSeek、ChatGPT 等主流 AI 的思考》，载《湖北社会科学（哲学社会科学版）》2025 年第 2 期，第 120 页。

[52] 姚迁、刘晋名、盛小宝：《生成式人工智能数据跨境流动的安全风险及治理范式》，载《网络安全与数据治理》2024 年第 12 期，第 80 页。

[53] 丁晓东：《论人工智能促进型的数据制度》，载《中国法律评论》2023 第 6 期，第 176 页。

[54] Tshilidzi Marwala Eleonore Fournier-Tombs Serge Stinckwich, Regulating Cross-Border Data Flows: Harnessing Safe Data Sharing for Global and Inclusive Artificial Intelligence, UNU(26 October 2023), https://unu.edu/publication/regulating-cross-border-data-flows-harnessing-safe-data-sharing-global-and-inclusive.

[55] Israel Desmond, *Assessing the Effectiveness of Cross-Border Data Flow Regulations in the Age of Artificial Intelligence (AI),* https://ssrn.com/abstract=4448648 or http://dx.doi.org/10.2139/ssrn.4448648(last visited October 10, 2026).

[56] 冉从敬：《捍卫国家数据主权刻不容缓》，载《图书馆论坛》2023 年第 9 期，第 3 页。

孙南翔与张晓君指出，数据跨境流动对国家数据安全构成威胁，而数据主权赋予国家监管数据的合法性基础，实践中各国围绕数据安全问题开展管理和控制。[57]卜学民与马其家则提出“数据主权谦抑性”理念，认为传统主权的绝对性在数字时代需适度调整，以平衡数据自由流动与安全保护的需求。[58]在治理理念上，国内文献普遍强调“总体国家安全观”作为数据跨境流动规制的指导原则。例如，熊光清与张素敏主张在总体国家安全观下完善数据出境安全管理制度，通过细化数据分级分类、完善阻断法规等措施确保国家安全。[59]冉从敬等学者从国家数据主权角度出发，强调数据作为国家战略资源具有重要的主权发展价值与主权保护价值，认为捍卫国家数据主权是应对数据跨境流动安全风险的根本前提。

二是数据自由流动与经济效率的平衡，数据自由流动被视为数字贸易发展的基础。许可在分析《数据安全法（草案）》时指出，“数据自由流动”是基础性原则，而“数据安全流动”是限制性原则，二者共同构成中国数据跨境流动治理的审慎包容方案。[60]魏远山通过博弈论视角分析，认为在保障安全的前提下促进数据自由流动是实现数据保护与经济发展的平衡之道。[61]此外，盛斌与高疆强调，数据跨境自由流动与数据安全保护之间的平衡是决定全球数字贸易发展的关键制度因素，建议通过法律法规有效协调二者关系。[62]黄现清进一步明确，“自由流动”是数据跨境流动的基础原则，而“安全流动”是限制原则，需在国内立法中明确二者的适用标准。[63]

三是自由与安全的动态平衡问题，数据跨境流动治理的核心在于自由与安全的动态平衡。徐玉梅与杨柳从全球数字贸易规则视角出发，提出“自由”与“主权”两种模式的动态博弈，主张通过理念、规则与监管机制三个层面的完善实现平衡。[64]洪延青分析《促进和规范数据跨境流动规定》，认为其标志着中国从强监管向安全与发展“再平衡”的转变，勾勒出数据竞争战略的雏形。[65]具体而言，

---

[57] 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》，载《太平洋学报》2015 年第 2 期，第 63 页。

[58] 卜学民、马其家：《论数据主权谦抑性：法理、现实与规则构造》，载《情报杂志》2021 年第 8 期，第 62 页。

[59] 熊光清、张素敏：《总体国家安全观视角下我国数据出境安全管理制度的完善》，载《哈尔滨工业大学学报（哲学社会科学版）》2023 年第 5 期，第 32 页。

[60] 许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期，第 22 页。

[61] 魏远山：《博弈论视角下跨境数据流动的问题与对策研究》，载《西安交通大学学报（社会科学版）》2021 年第 5 期，第 114 页。

[62] 盛斌、高疆：《数字贸易：一个分析框架》，载《国际贸易问题》2021 年第 8 期，第 17-18 页。

[63] 黄现清：《数字贸易背景下我国数据跨境流动监管规则的构建路径》，载《西南金融》2021 年第 8 期，第 74 页。

[64] 徐玉梅、杨柳等：《自由”与“主权”：数据跨境流动治理模式的动态博弈——基于全球数字贸易规则视角》，载《行政论坛》2024 年第 6 期，第 157 页。

[65] 洪延青：《中国数据出境安全管理制度的“再平衡”——基于国家间数据竞争战略的视角》，载《中国法律评论》2024 年第 3 期，第 201 页。

学者们提出通过数据分级分类、例外条款设计以及国际合作等手段实现平衡。例如，孙南翔建议参考 CPTPP 规则，在商业领域以数据自由流动为原则，在非商业领域以数据安全为优先，构建兼容性规制框架。刘金瑞则主张通过厘清重要数据范围、健全跨境问责制以及明确数据访问权等方式，防范国家安全风险并促进可控的数据跨境流动。[66]

（三）国际经贸协定中的数据跨境流动规则

国际经贸协定是数据跨境流动规则的重要载体，国内文献对 RCEP、CPTPP、DEPA 等协定中的数据跨境流动规则进行深入分析，但中国现行规则在自由度与兼容性方面存在差距，学者们建议通过对接国际高标准规则、完善国内立法与探索区域合作实现规则协调。

RCEP 作为亚太地区重要的区域贸易协定，其数据跨境流动规则以“自由流动为原则，限制流动为例外”为特征。李烨指出 RCEP 以多元共治理念为核心，强调公共政策目标与基本安全例外条款，但中国现行规则过于强调“安全至上”，与 RCEP 的自由流动原则存在一定差距。[67]张晓君与刘泽杨进一步分析，RCEP 中的例外条款彰显了“发展与安全兼收并蓄”的价值追求，但其适用标准的不确定性要求中国在国内立法中进一步明确数据自由流动原则与安全标准。[68]洪治纲与霍俊先认为，RCEP 注重在尊重国家数据主权的基础上实现安全的数据跨境流动，建议中国以 RCEP 为契机扩大开放水平，形成“中式模板”的数据治理模式。[69]马忠法与苏婧怡则从中国-东盟合作视角出发，指出 RCEP 框架下数据跨境流动监管面临东盟内部治理水平不平衡与规则碎片化挑战，建议通过区域合作机制推动协同治理。[70]

CPTPP 在数据跨境流动方面提出了更高标准的要求。张子琳与彭德雷分析，CPTPP 相较于 RCEP 对中国国内规制提出更高要求，特别是在数据自由流动与本地化存储方面存在冲突，建议中国利用自贸区等制度创新载体探索监管模式。[71]孙南翔提出，中国应探索 CPTPP 数据跨境流动规则与国内数据分级分类制度的

---

[66] 刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，载《行政法学研究》2022 年第 4 期，第 73 页。

[67] 李烨：《RCEP 协定下我国数据跨境流动规则的检视与完善》，载《科技与法律（中英文）》2023 年第 1 期，第 120 页。

[68] 张晓君、刘泽杨：《RCEP 数据跨境流动基本安全例外条款与中国方案》，载《郑州大学学报（哲学社会科学版本）》2023 年第 4 期，第 36 页。

[69] 洪治刚、霍俊先：《RCEP 对数据跨境流动的规制及其重要影响》，载《西南金融》2022 年第 4 期，第 89 页。

[70] 马忠法、苏婧怡：《RCEP 框架下共建中国—东盟跨境数据流动治理合作机制的挑战及因应之道》，载《广西社会科学》2023 年第 10 期，第 77 页。

[71] 张子琳、彭德雷：《CPTPP 核心数字贸易规则与中国加入谈判因应——基于与 RCEP 的对比分析》，载《上海对外经贸大学学报》2024 年第 2 期，第 73 页。

衔接，在商业领域以自由流动为原则，在非商业领域以安全为优先。[72]王玫黎与陈雨指出，中国数据跨境规则以“数据安全”为核心，凸显“数字自由”的价值倾向，但与 CPTPP 的高标准存在一定差距，需通过完善例外条款与不符措施清单实现对接。[73]董储超进一步归纳，CPTPP 架构下的数据跨境流动规则体现包容规制的折中主义模式，中国需在安全与自由之间寻求平衡。[74]

DEPA 作为数字经济专项协定，其数据跨境流动规则以“促自由、严治理”为导向。梅傲与李淮俊分析，DEPA 围绕数据保护可信任标志、监管沙盒机制与政府数据开放等创新内容展开，中国应通过明晰安全评估范围、完善事后监管等措施对接 DEPA 规则。[75]宋晓舒指出，DEPA 在促进数字贸易便利化与可信数据跨境流动方面具有创新性，建议中国在加入 DEPA 后优化数据跨境流动规则。[76]朱雅妮强调，DEPA 的价值理念围绕激活数据与鼓励创新，同时兼顾数据安全，建议中国通过完善国内立法与国际合作对接 DEPA 的高标准规则。[77]王楚晴进一步分析，DEPA 采取“原则+例外”的规制标准，确立了自由流动与安全发展的平衡模式，中国需优化国内数据治理体系以实现相容性。[78]

最后，周念利与于美月分析了《英国-新加坡数字经济协定》（UK-Singapore Digital Economy Agreement）与《韩国-新加坡数字伙伴关系协定》（Korea-Singapore Digital Partnership Agreement），指出其在金融数据跨境流动、数字知识产权保护等方面具有创新性，建议中国借鉴其规则设计。[79]黄贵与陶如基于数字融合指数分析 RCEP 缔约国的数据跨境流动政策，指出各国在保障数据安全前提下对数据跨境流动持开放态度，建议中国完善数据分级分类管理以对接国际规则。[80]

---

[72] 孙南翔：《CPTPP 数字贸易规则：制度博弈、规范差异与中国因应》，载《学术论坛》2022 年第 5 期，第 52 页。

[73] 王玫黎、陈雨：《中国数据跨境流动规则与 CPTPP 的对接研究》，载《国际贸易》2022 年第 4 期，第 20 页。

[74] 董储超：《CPTPP 架构下数据跨境流动规则的时代表征与中国因应》，载《情报杂志》2024 第 7 期，第 179 页。

[75] 梅傲、李淮俊：《数字贸易中数据跨境流动规则的新发展——基于〈数据出境安全评估办法〉与 DEPA 的比较》，载《企业经济》2023 年第 4 期，第 160 页。

[76] 宋晓舒：《DEPA 视角下的数字贸易规则发展与应对策略》，载《商业经济研究 》2023 年第 22 期，第 134-137 页。

[77] 朱雅妮：《〈数字经济伙伴关系协定〉的治理重心、推进策略及中国的加入谈判》，载《南昌大学学报（人文社会科学版）》2023 年第 5 期，第 83-83 页。

[78] 王楚晴：《申请加入 DEPA 背景下中国数据治理的相容性审视及优化路径》，载《太平洋学报》2023 年第 3 期，第 12-13 页。

[79] 周念利、于美月：《“新式”数字贸易规则的演进趋向研究——基于 UKSDEA 和 KSDPA 的视角》，载《理论学刊》2023 年第 4 期，第 120 页。

[80] 黄贵、陶如：《RCEP 缔约国数据跨境流动政策的数字生产力基础及其影响——以数字融合指数为参照》，载《中国科学院院刊》2023 年第 8 期，第 1168 页。

（四）中国数据跨境流动的国内立法与实践

我国在数据跨境流动领域的立法与实践以“安全自由有序流动”为原则，通过《数据安全法》《个人信息保护法》等法律框架以及自贸区试点探索制度创新。然而，当前立法存在事前监管压力过大、规则适用指引不足等问题，需通过完善分级分类制度、探索监管沙盒与加强国际合作进一步优化。

中国的数据跨境流动立法以《数据安全法》《个人信息保护法》为核心，强调“安全有序流动”。王玫黎与陈雨总结，中国数据跨境规则由数据本土化制度与安全审查制度构成，凸显“数字自由”倾向但保持克制。许可分析《数据安全法（草案）》，指出其首次提出“数据安全自由流动原则”，为全球数据治理提供审慎包容的中国方案。赵精武分析了标准化合同在数据跨境传输中的作用，认为其通过私法义务细化公法责任，协调了数据安全与流动的冲突。[81]然而，学者们也指出现行立法存在不足。例如，张墨洋分析证券公司数据出境的合规困境，认为事前监管压力过大、缺乏适用指引，建议完善监管规则与探索监管沙盒。[82]马其家与李晓楠主张从完善法律法规、建立数据分类审核制度、强化技术安全建设等多个维度优化监管机制。[83]

就数据本地化义务而言，中国对数据本地化义务的正式确立始于《网络安全法》第 37 条明确规定“关键信息基础设施运营者”应在境内存储个人信息和重要数据，若确需出境，应进行安全评估。此后，《数据安全法》《个人信息保护法》进一步细化了数据分类分级和出境流程，为数据本地化义务提供了制度基础。王玥指出维纳的信息技术政治哲学思想为数据本地化立法正当性提供了哲学基础，从总体国家安全观理念出发，数据本地化有利于保障国民安全、政治安全、便利执法和经济发展。[84]不少学者主张跨境数据流动应实现自由化，田旭认为数据本地化是政府通过行政方式干预数据流出国境的一种限制性手段，从法律效果论上看其属公法，然而主流数据本地化制度的逻辑出发点是个人数据保护，其保护客体具有很强的私法性，因此对私人数据采取本地化措施涉嫌以公法干预私法，立法基础薄弱，虽然公法与私法的切分有助于提高本国数据本地化立法的可实施性和可接受性，建议中国在现有数据本地化立法中，明确数据本地化的立法目的和保护客体，加快个人数据民事权利的赋权，同时兼顾国家主权与国际融合。

---

[81] 赵精武：《数据跨境传输中标准化合同的构建基础与监管转型》，载《法律科学（西北政法大学学报）》2022 年第 2 期，第 148 页。

[82] 张墨洋：《我国证券公司数据出境的合规困境与监管应对》，载《天府新论》2024 年第 2 期，第 129 页。

[83] 马其家、李晓楠：《论我国数据跨境流动监管规则的构建》，载《法治研究》2021 年第 1 期，第 92 页。

[84] 王玥：《试论网络数据本地化立法的正当性》，载《西安交通大学学报（社会科学版）》2016 年第 1 期，第 54 页。

[85]李海英指出本地化的类型包括服务本地化、设施本地化和数据本地化。[86]

高山行、刘伟奇整理介绍了多个国家和地区的数据本地化政策，包括澳大利亚、加拿大、新加坡、德国、巴西、马来西亚和哈萨克斯坦等，建议中国政府通过对数据主体、数据持有人、存储设备拥有者、数据的分析和处理者以及对数据处理结果的使用者等民事主体进行收集、分析、占有数据的权利进行授权、分类管理、积极面对数据公开的现状、加快参与国际合作的步伐。[87]

数据分级分类是实现数据跨境流动安全与效率平衡的关键。刘金瑞从风险路径识别角度，主张通过分级管理应对重要数据跨境流动的安全挑战通过厘清重要数据范围、健全跨境问责制与明确数据访问权，防范国家安全风险并促进可控流动。[88]王玉珏等结合《数据安全法》与《中华人民共和国档案法》，建议建立符合中国实际的数据与档案分级标准，以保护数据安全。赵新潮从企业数据权利限制角度，强调企业需落实数据分类分级保护的主体责任，确保跨境流动合规。[89]

中国学界对数据最小化概念的界定，普遍以《个人信息保护法》第 6 条为基本依据，强调“目的正当、最小必要”为立法核心。制度演变方面，早期仅在部委规章如《中华人民共和国计算机信息系统安全等级保护管理办法》中零散体现，至 2021 年《个人信息保护法》实施后正式形成国家层面的原则性规范，与“知情+同意”“合法正当”共同构成数据处理基本准则。

近年来，在人工智能场景中数据滥用、泛化收集的问题日益突出，数据最小化原则开始从立法抽象原则走向治理操作性机制，引发学界对其在算法推荐、模型训练、跨境流动等领域适用边界的深入探讨。

自由贸易试验区是中国数据跨境流动制度创新的重要载体。马忠法与郑文龙分析上海自贸区对接 DEPA 规则的不足，建议拓宽数据流动互信范围、探索监管沙盒与推动政府数据开放。[90]吴玄研究海南自贸港的数据跨境规则，提出以安全、开放、可行为导向，构建目标导向的制度路径。[91]张泳与闫芊伊聚焦横琴粤澳深度合作区，指出其数据跨境流动存在立法空白与法律冲突问题，建议借鉴欧盟监

---

[85] 田旭：《数据本地化立法的兴起与反思》，载《大连海事大学学报（社会科学版）》2020 年第 1 期，第 32 页。

[86] 李海英：《数据本地化立法与数字贸易的国际规则》，载《信息安全研究》2016 年第 9 期，第 781 页码。

[87] 高山行、刘伟奇：《数据跨境流动规制及其应对——对〈网络安全法〉第三十七条的讨论》，载《西安交通大学学报（社会科学版）》2017 年第 2 期，第 87 页。

[88] 刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，《行政法学研究》2022 年第 4 期，第 73 页。

[89] 赵新潮：《个体权益·公共利益·国家安全：企业数据权利限制的三重考量》，载《湖北大学学报（哲学社会科学）》2024 年第 4 期，第 143 页。

[90] 马忠法、郑文龙：《上海自贸试验区对接 DEPA 跨境数据流动规则：动因、差距及完善路径》，载《上海财经大学学报》2024 年第 4 期，第 139 页。

[91] 吴玄：《海南自由贸易港数据跨境规则创新路径研究》，载《海南大学学报（人文社会科学版）》2025 年第 4 期，第 140 页。

管沙盒原理完善治理机制。[92]孙冉分析粤港澳大湾区数据跨境流动的逻辑构造，认为应以保障数据安全为首要原则，通过规则优化平衡发展与安全。[93]朱简则指出浙江自贸区在数据跨境安全评估、监管能力与国际包容性方面存在不足，建议健全法律体系与加强国际合作。周念利等强调自贸区应以安全为底线、发展为目标推进制度创新，聚焦模式创新与技术创新。[94]

（五）数据跨境流动的场景化治理

场景化治理研究显示，不同领域的数据跨境流动需根据其特性制定差异化规制。金融、医疗、汽车等领域因涉及国家安全与个人隐私，需严格监管与创新机制并重，沙盒监管、分类分级与国际合作是优化治理的共同路径。

金融数据跨境流动因其涉及国家金融安全与个人隐私，受到严格监管。黄琳琳总结了国际贸易法规制金融数据跨境流动的三种模式，即欧盟的隐私保护优先模式、美国的经济利益优先模式与中国的安全优先模式，建议中国在保障安全基础上明确价值取向。[95]吴一楷从金融安全观出发，提出构建以“金融数据安全”为核心的涉外金融数据法治体系。郭德香与刘畅强调，金融数据跨境流动的法律规制需以数据主权、数据安全与有限性理论为法理基础，通过多元共治与国际合作优化治理。[96]张墨洋分析证券公司数据出境困境，建议明确监管主体、完善事中事后监管与探索监管沙盒。冯泽华与刘志辉聚焦粤港澳大湾区金融数据跨境流动，提出“立法+组织+权利”的三维法治路径，平衡自由流动与本土化导向。刘妍与冉从敬主张根据金融数据安全等级划定差异化监管措施，构建互信机制以促进数据互操作。[97]

医疗数据的跨境流动涉及个人健康隐私，需严格保护。陈永怡与孟彦辰分析澳大利亚健康医疗数据跨境流动的法律规制，指出其通过专门机构与系统立法实现严格监管，建议中国借鉴其经验完善医疗数据治理。[98]何俊辉从经济法视角提出，构建数据跨境流动沙盒监管机制以平衡数据价值增值与风险控制。[99]

---

[92] 张泳、闫芊伊：《粤澳数据跨境治理困境及其纾解——以横琴深合区数据跨境流通据点为视角》，载《港澳研究》2024 年第 4 期，第 60-61 页。

[93] 孙冉：《粤港澳大湾区数据跨境流动的逻辑构造与优化进路》，载《地方立法研究》2024 年第 5 期，第 87 页。

[94] 周念利、于美月、刘春苗：《我国自贸区（港）数据跨境流动试点制度创新研究》，载《国际商务研究》2023 年第 4 期，第 86 页。

[95] 黄琳琳：《金融数据跨境流动的国际贸易法规制》，载《上海对外经贸大学学报》2023 年第 6 期，第 66 页。

[96] 郭德香、刘畅：《个人金融数据跨境流动法律规制的国际经验及中国因应》，载《征信》2023 年第 11 期，第 57 页。

[97] 刘妍、冉从敬：《金融数据跨境监管的国际策略与中国进路》，载《金融评论》2023 年第 4 期，第 109 页。

[98] 陈永怡、孟彦辰：《澳大利亚健康医疗数据跨境流动法律规制研究及其对中国的启示》，载《金融评论》2023 年第 4 期，第 109 页。

[99] 何俊辉：《不完全契约视角下的数据跨境流动沙盒监管机制研究》，载《数字图书馆论坛》2024 年

智能网联汽车数据因其全球化特性与敏感性成为研究热点。赵海乐从比较法视角分析“车联网”数据治理，建议对敏感信息最高标准保护、对非敏感信息分层共享，并通过审查机制化解国家安全风险。[100]张桁嘉与尤建新总结智能网联汽车数据风险，指出数据跨境出境需关注合作与监管的平衡，探索共性标准与关键技术。[101]

在民航数据领域，国际民航组织对旅客数据跨境流动的规制，中国应加大国际规则参与、完善安全评估与监管体系。杨彩霞与邱圣童指出，GDPR 在民航领域的域外执法需基于承诺与合作，中国应借鉴其路径优化治理。[102]在科学研究场景，王珺等分析科学数据跨境流动治理的不足，建议加强顶层设计、完善规制实施与提高国际化水平。在人工智能领域，马治国等提出人工智能基础数据的专门法保护，强调权利义务明晰与过程监管。[103]

（六）数据跨境流动的国际合作与博弈

由于中美欧三大人工智能发展区域在数据跨境流动治理中的立场分歧，中国需通过区域合作与国际规则制定增强话语权。RCEP、“一带一路”等平台为中国提供了协调规则与推动合作的重要机遇。

中美欧在数据跨境流动治理中的立场差异显著。单文华与邓娜分析欧美数据跨境流动的规则博弈，认为其表面是数据保护理念碰撞，实质是欧盟“数字主权”与美国“数字霸权”的利益冲突。[104]刘业指出，欧盟以数字宪制主义推动数据保护的域外管辖，建议中国避免陷入被动合规陷阱，构建独立自主的战略。[105]也有学者从国际政治视角分析美国全球数字战略，指出其以“自由数字秩序”为基础，强调数据跨境自由流动，旨在维护数字霸权。杨楠进一步分析美国对华数据政策的经济、军事、隐私与意识形态逻辑，建议中国警惕其战略意图。[106]陈振华等评价欧盟的充分性决定制度，认为其在保护数据安全的同时扩大了全球数据鸿沟，建议中国通过国际合作应对其影响。[107]在国际经贸协定中，如 CPTPP、DEPA 均

第 4 期，第 58 页。

[100] 赵海乐：《比较法视角下的我国“车联网”数据治理路径选择》，载《上海财经大学学报》2021 年第 5 期，第 139 页。

[101] 张桁嘉、尤建新：《智能网联汽车数据风险的研究热点与展望》，载《上海管理科学》2025 年第 1 期，第 30-31 页。

[102] 杨彩霞、邱圣童：《浅析欧盟 GDPR 对民航数据跨境之影响》，载《北京航空航天大学学报（社会科学版）》2024 年第 6 期，第 135 页。

[103] 马治国、胡明强、张磊：《我国人工智能基础数据的专门法保护研究》，《西北大学学报（哲学社会科学版）》2021 年第 6 期，第 53 页。

[104] 单文华、邓娜：《从“数据隐私框架”看欧美数据跨境流动的规则博弈》，载《太平洋学报》2024 年第 1 期，第 44 页。

[105] 刘业：《美欧数据跨境流动博弈中的欧盟技术主权战略及其实现》，载《国际法研究》2023 年第 6 期。

[106] 杨楠：《美国对华数据政策论析》，载《情报杂志》2024 年第 8 期，第 42 页。

[107] 陈振华、张伟华、王秉：《欧盟个人数据跨境流动充分性决定制度之评价分析》，载《太平洋学报》

涉数据流动与隐私最小化问题，学者建议中国通过“标准合同条款+最小化声明”提升制度对接能力。洪延青分析美欧在 WTO 电子商务谈判中的战略立场，认为中国缺乏实质性数据竞争立场，需通过立法完善治理框架。

各国跨境数据流动制度存在差异。黄宁认为各国在跨境数据流动规制的方式选择上，存在显著的差异化现象：美国主张数据自由流动，欧盟注重隐私规制，大量发展中国家则偏好数据本地化政策。[108]许多奇指出全球跨境数据流动规则主要由以欧美为首的发达国家引领，欧盟将数据权视为基本人权，美国的个人数据保护政策奉行市场导向、以行业自律为中心。弓永钦对重点国家数据跨境流动的规制进行了比较研究，其聚焦于个人隐私规则，并对网络隐私保护的法律管辖权问题及跨境隐私规则体系进行了深入论述与研究。[109]罗昕、杨仰文指出跨境数据流动治理存在“数据控制者模式”和“数据存储地模式”，二者在公民权利保护、产业发展创新与国家安全等各方面具有共识也有分歧。[110]陈少威、贾开回溯了跨境数据流动全球治理体系演进的历史，并在此基础上分析导致治理变迁的原因，各国数据规制存在显著差异的缘由是历史因素和规制传统的不同。张茉楠指出跨境数据流动受地缘政治、国家安全、隐私保护、产业发展水平等因素影响，主要经济体围绕“数字主权”，制定相应的数字治理模式，使全球跨境数据流动呈现有限性、灵活性、竞争性发展态势。

区域合作和参与国际规则制定是参与数据跨境流动治理的重要路径和提升中国数据跨境流动治理话语权的关键。茶洪旺等通过国际比较，建议中国加强数据分级分类管理、参与国际规则制定与降低本地化存储要求。[111]董京波提出细化数据分级分类、完善阻断法规与积极参与国际规则制定等建议，以应对他国长臂管辖。赵祺分析中国-东盟跨境数据治理合作，指出东盟国家规则复杂与美国拉拢等制约因素，建议通过 RCEP 与“一带一路”平台加强协同治理。[112]马忠法与苏婧怡强调 RCEP 框架下中国-东盟数据跨境流动合作的战略价值，建议通过区域机制应对规则碎片化挑战。参与国际规则制定是提升中国数据跨境流动治理话语权的关键。王彬彬与邓小婷建议通过 JSI 谈判路径与“一带一路”平台构建中

2024 年第 1 期，第 190 页。

[108] 黄宁：《数据本地化的影响与政策动因研究》，载《中国科技论坛》2017 年第 9 期，第 161 页。

[109] 许多奇：《个人数据跨境流动规制的国际格局及中国应对》，载《法学论坛》2018 年第 3 期，第 130 页。

[110] 罗昕、杨仰文：《跨境数据流动治理的制度化实践与中国进路》，载《传媒经济与管理研究》2019 年第 0 期，第 44 页。

[111] 茶洪旺、付伟、郑婷婷：《数据跨境流动政策的国际比较与反思》，载《电子政务》2019 年第 5 期，第 123 页。

[112] 赵祺：《中国—东盟跨境数据流动治理合作：现实与路径选择》，载《南洋问题研究》2024 年第 3 期，第 85 页。

国主导的数字贸易规则。[113]郭朝先分析数据跨境流动规则的国际博弈，指出中国以“安全与自由并重”的治理主张契合发展中国家需求，建议通过国际合作增强话语权。[114]王小林与兰松提出“数字丝绸之路”数据跨境流动机制，强调顶层设计、政策完善与多元交易模式培育。[115]

三、国外研究现状

（一）人工智能训练数据和用户数据跨境流动流动规则适用挑战

随着人工智能技术的迅猛发展，数据作为人工智能的“燃料”在全球范围内的跨境流动需求日益增加。数据跨境流动涉及国家主权、个人隐私、数据安全、国际贸易以及技术治理等复杂问题，在国际法领域引发了广泛关注。人工智能的训练和应用需要海量、多样化的数据，而这些数据的跨境传输受到各国不同法律框架的限制，形成了全球治理中的新挑战。

人工智能技术的核心在于大模型训练，需依赖海量、多样化的数据集。人工智能技术的快速发展使得数据跨境流动的规模和复杂性大幅增加。[116]例如，生成式人工智能需要跨国数据来提升模型的泛化能力，但各国对个人数据、非个人数据、敏感数据等数据类型的定义和监管标准不一，导致合规成本上升。[117]

隐私保护是数据跨境流动的核心挑战。GDPR 对个人数据的严格保护要求与人工智能的数据需求形成张力。Hoofnagle et al.指出人工智能系统常需处理匿名化或去标识化的数据，但匿名化技术的有效性在人工智能背景下受到质疑。[118]例如，机器学习可能通过数据推断重新识别个人身份。[119]此外，人工智能生成的内容，比如深度伪造技术下生成的文本、视频等，可能进一步模糊个人数据与非个人数据的界限，增加跨境监管难度。[120]

---

[113] 王彬彬、邓小婷：《JSI 谈判模式下中国国际数字贸易规则的建构》，载《国际贸易》2024 年第 12 期，第 41 页。

[114] 郭朝先、李婷、罗芳：《数据跨境流通规则博弈与中国应对》，《中国流通经济》2024 年第 9 期，第 27 页。

[115] 王小林、兰松：《“数字丝绸之路”数据跨境流动机制:逻辑框架与路径选择》，《人文杂志》2025 年 1 月。

[116] Morgan Lewis & Bockius LLP, *The Evolving Framework of Data Governance: A Global Perspect ive,* https://www.lexology.com/library/detAl.aspx?g=5b1189f8-00cd-4021-b860-174a24dbf961(last visited Octo ber 10, 2026).

[117] Emily M. Bender, et al*., On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?,* in FACCT '21: PROCEEDINGS OF THE 2021 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (Madeleine Clare Elish, William Isaac & Richard S. Zemel, 2021).

[118] Aaron K. Perzanowski, Chri Jay Hoofnagle & Aniket Kesari, *The Tethered Economy,* 87 GEORGE WASHINGTON LAW REVIEW 783, 821-828(2019).

[119] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye. E*stimating the Success of Re-identifications in Incomplete Datasets Using Generative Models,* 10 NAT COMMUN 3069, 3090(2019).

[120] Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Priv es: A Looming Challenge for Privacy, Democr, Democracy, and National Security*, 107 CALIFORNIA LAW REVIEW 1753, 1757(2019).

人工智能的战略重要性使得数据资源上升到国家战略资产的地位，数据跨境流动监管审查常常被视为涉及国家安全的问题。美国、欧盟和中国等均将人工智能数据视为关键基础设施的一部分。例如，2020 年，美国《国家人工智能倡议法案》（National Artificial Intelligence Initiative Act）强调数据安全，中国通过《网络安全法》加强对数据跨境流动的审查。这种通过国家安全为底线，可能造成全球人工智能技术竞争的碎片化。

人工智能技术的快速迭代与国际法的滞后性形成显著矛盾。现有国际法律框架多基于传统数据处理场景，难以应对人工智能带来的动态数据处理需求。[121]例如，人工智能系统可能在云端实时处理跨国数据，传统法律对“数据所在地”的定义已不适用。此外，人工智能的自动化决策可能引发法律责任归属问题，尤其是在跨境场景下。

（二）数据跨境流动具体规则研究

数据处理“说明-同意”义务、数据最小化原则、诸如删除权、被遗忘权、撤销-同意以及数据安全保障等权利是中、美、欧三大司法管辖权数据跨境流动监管框架之间的共性。[122]

1.“知情-同意”义务

在人工智能驱动的全球化数据经济中，数据跨境流动成为技术创新的核心动力。然而，数据跨境流动涉及复杂的隐私保护问题，其中“说明-同意”（notice and consent）义务作为隐私保护的基石，受到广泛关注。该义务最初源自欧美个人信息保护的基本机制，要求数据控制者在处理个人数据前，向数据主体提供清晰的信息并获得其明确同意。然而，人工智能技术的复杂性、数据处理规模的扩大以及跨境流动的法律差异，使得“说明-同意”义务面临更加复杂的挑战。

“说明-同意”义务起源于 20 世纪 70 年代的隐私保护理念。1980 年，OECD《隐私指南》首次提出知情同意作为隐私保护的基础。1981 年的《有关个人数据自动化处理中的个体保护公约》（Convention for the Protection of Individuals with Regard to the Processing of Personal Data）（以下简称《欧洲委员会 108 号公约》）进一步确立了该机制的法律地位。1995 年《保护个人在数据处理和自动移动中权利的指令》（Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data）（以下简称《欧盟数据保护

[121] WALTERS ROBERT, THE DIGITAL ECONOMY AND INTERNATIONAL TRADE: TRANSNATIONAL DATA FLOWS REGULATIO 139, (2022).

[122] Israel Desmond, Assessing the Effectiveness of Cross-Border Data Flow Regulations in the Age of Artificial Intelligence (AI) (April 18, 2023). Available at SSRN: https://ssrn.com/abstract=4448648 or http://dx.doi.org/10.2139/ssrn.4448648(last visited October 10, 2026).

指令》）及 GDPR 将“说明-同意”明确为隐私保护的核心原则。[123]《个人信息保护法》和印度 2023 年《数字个人数据保护法》（The Digital Personal Data Protection Act，以下简称 DPDP Act）也引入了类似要求，但因法律传统差异而在具体要求上有所不同。

“说明-同意”义务在国际法中通过多边和区域协定体现。欧盟 GDPR 第 7 条要求数据处理基于“自由、具体、知情且明确”的同意，第 13 和 14 条规定隐私通知需透明且易懂。[124]在跨境数据流动中，GDPR 的充分性决定机制要求接收国保护水平与欧盟相当，间接强化了“说明-同意”义务。[125]

《亚太经济合作组织隐私框架》（APEC Privacy Framework）的 CBPR 鼓励企业在跨境传输中遵循透明性和同意原则，但其非约束性限制了执行力度，同时其试图通过认证简化同意流程而导致参与度有限。CPTPP 虽未直接规定“说明-同意”，但其第 14.11 条的隐私保护条款为其提供了间接支持。双边协议在协调“说明-同意”义务方面取得有限进展。欧盟-日本签署数据保护协议通过统一隐私通知和同意标准促进了数据流动，但未充分考虑人工智能训练数据的复杂性。中美之间缺乏类似协议，导致人工智能企业在跨境传输中面临合规难题。

人工智能技术对“说明-同意”义务构成核心挑战。“说明-同意”义务要求数据控制者在处理个人数据前，向数据主体提供透明的隐私通知或说明，并获得其自愿、知情且明确的同意。

人工智能系统依赖海量、动态的数据集，处理流程复杂且不透明，该义务需适应复杂的数据处理场景，包括人工智能训练数据、推断数据及跨国数据共享，说明需涵盖数据处理的目的、范围、接收方及跨境传输风险，同意则需体现数据主体的主动选择，难以在通知中清晰说明数据用途。例如，人工智能的黑箱特性使得数据处理目的可能在训练后发生变化，超出原始同意范围。所以，人工智能技术的兴起促使学者们争论是否需要动态同意机制以适应人工智能的实时处理，以及该机制如何扩展至非个人数据和推断数据以应对人工智能模型的复杂处理需求。例如，印度 DPDP Act 虽引入同意机制，但对人工智能场景下的实施细则不足。以云端训练为典型代表的人工智能的动态数据处理使得通知内容难以全

[123] CHRISTOPHER KUNER, LEE A. BYGRAVE & CHRISTOPHER DOCKSEY, THE EU GENERAL DATA PROTECTION REGULATION: A COMMENTARY 39 (Laura Drechsler ed., 2020).

[124] Paul M. Schwartz, *Global Data Privacy: the EU Way*, 94 NEW YORK UNIVERSITY LAW REVIEW 771, 780-783 (2019).

[125] Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. , *The European Union General Data Protection Regulation: What it is and What it Means,* 28 INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 65, 67(2019).

面，同意的有效性受到挑战。[126]有学者主张研究通过人工智能解释性技术增强隐私通知的透明度。[127]

人工智能背景下，“说明-同意”义务的有效性备受质疑。用户面对冗长的隐私政策和频繁的同意请求，常出现“同意疲劳”（consent fatigue），倾向于不加思考地点击“同意”。[128]跨境数据流动涉及多国法规差异，进一步削弱用户的知情能力。[129]学者们争论是否应简化通知或探索替代机制，如默认保护模式。人工智能技术加剧了“说明-同意”义务的法律碎片化，导致规则冲突。[130]欧盟 GDPR 要求明确同意，中国《个人信息保护法》要求“单独同意”，标准和程序的差异增加了人工智能企业的合规成本。2018 年，美国《澄清境外数据合法利用法案》（Clarifying Lawful Overseas Use of Data Act，以下简称 CLOUD ACT）允许政府绕过用户同意访问境外数据，与 GDPR 冲突。[131]学者们争论是否需要全球统一的同意标准以简化跨境合规。[132]

2.数据最小化原则

数据最小化（data minimization）原则是隐私保护的核心原则之一，要求数据控制者仅收集和处理实现特定目的所需的最少数据。该原则最早源于 20 世纪 70 年代的隐私保护理念，强调数据主体对个人信息的控制权。数据最小化原则要求数据处理限于实现特定目的的最小范围，避免不必要的收集和存储。[133]其通常依赖匿名化技术，“数据最小化”原则已成为多数跨境数据规则的重要基准之一。欧盟 GDPR、OECD 隐私原则、亚太经合组织跨境隐私规则体系（以下简称 APEC-CBPR 体系）均强调该原则在跨境传输中的合法性与正当性基础作用。

数据最小化原则的演变与隐私保护法律的发展密切相关。最早可追溯至 1980 年 OECD《隐私指南》提出的“限制收集”原则，后在欧盟 GDPR 第 5 条中被正式确立为六项基本处理原则之一。1970 年代，OECD《隐私指南》首次提出数据最小化作为隐私保护的基础。1981 年，《欧洲委员会 108 号公约》进一

---

[126] Thomas Burri, *A Challenge for Law and Artificial Intelligence*, 5 NATURE MACHINE INTELLIGENCE 1508, 1508-1509 (2023).

[127] Lilian Edwards & Michael Veale, *Enslaving the Algorithm: From a ‘Right to an Explanation’ to a ‘Right to Better Decisions’?* , 16 EEE SECURITY & PRIVAC 46, 50-54(2018).

[128] Alessandro Acquisti, et al., *Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online*, 50 ACM COMPUTING SURVEYS 1, 20-25(2018).

[129] Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, in PRI VACY, BIG DATA, AND THE PUBLIC GOOD FRAMEWORKS FOR ENGAGEMENT (Julia Lane, Vict oria Stodden, Stefan Bender & Helen Nissenbaum eds., 2014).

[130] WOODROW HARTZOG, PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIG N OF NEW TECHNOLOGIES 276-280 (2018).

[131] Jennifer Daskal, *Borders and Bits*, 71 VANDERBILT LAW REVIEW 179, 180-183 (2018).

[132] Joshua P. Meltzer, *Governing Digital Trade*, 18 WORLD TRADE REVIEW 23, 30-43(2019).

[133] Paul M. Schwartz, *Global Data Privacy: the EU Way*, 94 NEW YORK UNIVERSITY LAW REVIEW 771, 773-780 (2019).

步明确了该原则的法律地位。数字时代，《欧盟数据保护指令》及 GDPR 将数据最小化确立为核心原则。同时，2021 年中国《个人信息保护法》和 2023 年印度 DPDP Act 也引入了数据最小化要求，但其具体定义和实施要件因文化和法律传统差异而有所不同。

同时，跨境数据流动中的法律碎片化和国际规则冲突是另一争论点。各国对数据最小化的实施差异显著。中国的《数据保护法》要求跨境数据传输需经过安全评估，确保数据收集限于最小范围，单独审查机制进一步增加了复杂性。美国缺乏统一联邦隐私法，依赖州级立法比如《加利福尼亚州消费者隐私法案》（California Consumer Privacy Act），其最小化要求较为宽松，与 GDPR 标准存在冲突，导致企业合规成本上升。印度 DPDP Act 虽提及数据最小化，但缺乏人工智能场景的具体细则。一方面，这些差异导致企业在跨境人工智能应用中面临合规挑战比如中美之间缺乏统一的数据共享协议，导致人工智能企业在跨境传输中难以平衡最小化与数据需求；另一方面，在涉及多国管辖权，导致数据跨境流动管辖权冲突和规则冲突。

近年来，随着人工智能技术的兴起，数据跨境流动的规模和复杂性急剧增加，人工智能技术对海量、多样化数据的依赖与数据最小化原则形成显著张力。数据最小化需要被重新审视以应对大规模数据处理和跨境流动的挑战。人工智能系统中数据最小化处理的数据不仅涉及个人数据，还包括匿名化数据和推断数据，因人工智能的动态处理特性而复杂化。匿名化数据的再识别风险成为争论焦点。机器学习算法可通过数据推断重新识别个人身份，挑战最小化原则的有效性。[134]以及是否应将推断数据纳入最小化监管范围，是否应将最小化原则适用于匿名化、脱敏化数据处理、群体数据分析等仍存分歧。部分学者提出区分“数据主体可识别性”是判断适用边界的关键。

人工智能数据需求与最小化原则的矛盾，人工智能技术对海量数据的依赖与数据最小化原则形成核心争论。有文献指出大模型训练需多样化数据集以提升泛化能力，而最小化可能限制数据可用性，影响人工智能性能。例如，生成式人工智能依赖跨国数据，数据最小化可能导致“数据孤岛化”。[135]学者们争论是否应调整最小化标准以适应人工智能需求，或通过如联邦学习等技术手段缓解矛盾。主张通过法律和技术的协同，探索差分隐私、联邦学习等技术以支持数据最小化。

---

[134] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models,* 23 NAT COMMUN 3069, 3074(2019).

[135] Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, https://www2.itif.org/2021-data-localization.pdf(last visited October 10, 2026).

[136]例如，联邦学习允许在本地训练模型，减少数据跨境传输。新兴研究试图将最小化原则与隐私计算、联邦学习、可解释人工智能等技术工具结合，以期构建具备自动评估功能的最小化合规机制。[137]部分学者主张最小化原则应作为强制性原则适用于所有数据处理环节，尤其是跨境流动前必须评估是否“最小必要”；另有观点认为在人工智能模型训练、数据共享等场景中应保持一定弹性，以避免过度限制创新。双边协议如“欧盟-美国数据隐私框架充分性决定”（Adequacy Decision for the EU-US Data Privacy Framework）要求企业在跨境传输中遵守 GDPR 的最小化原则，但人工智能企业常通过标准合同条款规避严格要求。

学者们争论是否需要全球统一的最小化标准，以及如何平衡主权与数据自由流动。首先，在跨境场景中，数据可能在保护水平较低的国家被重新处理，增加隐私风险，当前各国数据跨境流动规则标准不统一导致人工智能数据在重新处理时候面临保护水平参差的风险。其次，当前以生成式人工智能模型为代表的主流人工智能模型依赖大规模语料训练，如何在数据收集与部署阶段落实最小化原则，技术与法制机制严重脱节。因此，学者逐步聚焦最小化原则的“可操作性”，并提出构建基于数据生命周期的评估指标体系，包括数据采集量化边界、冗余数据剔除机制等。部分研究开始从制度层面探索数据最小化原则与数据出境安全评估、影响评估的联动机制，为跨境合规建构“前置+动态”的风险评估框架。并关注多边框架在协调最小化标准中的作用。[138]

3.数据本地化义务

数据本地化（data localization）义务要求数据在生成或收集的国家境内存储和处理，通常被视为维护国家安全的重要手段。数据本地化义务的提出，最初源于保障国家网络主权与数据安全的考量，尤其是在跨境数据流动增加、隐私泄露和国家安全风险频发的背景下，该义务被制度化为重要的监管工具。数据本地化义务的起源可追溯至 20 世纪末的网络主权理念。随着网络安全威胁增加，俄罗斯和中国等国家开始实施数据本地化政策。2010 年后，数据本地化成为全球趋势，尤其在国家安全驱动下。例如，俄罗斯《联邦数据保护法》要求公民数据存储在境内，《网络安全法》及《数据安全法》规定重要数据不得出境。

国外学界近年非常关注数据本地化（data localization）或数据留存（data retention）这一主题，并涌现出了一系列有代表性的研究，对全球主要跨境数据

---

[136] Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy*, 9 FOUNDATIONS AND TRENDS IN THEORETICAL COMPUTER SCIENCE 211, 250-301(2014).

[137] Qiang Yang, Yang Liu, Tianjian Chen, Yongxin Tong, *Federated Machine Learning: Concept and Applications*, 10 ACM TRANSACTIONS ON INTELLIGENT SYSTEMS AND TECHNOLOGY 1, 17-19(2019).

[138] Joshua P. Meltzer, *Governing Digital Trade*, 18 WORLD TRADE REVIEW 23, 23-25(2019).

流动管理制度的来源、发展以及标志性制度进行了研究。[139]Anupam Chander 和 Uyên P. Lê回顾了澳大利亚、中国、法国、德国、俄罗斯、韩国等 18 个国家或地区的数据本地化措施，包括指出全球出现了加强互联网控制的趋势，同时实行数据流入审查和提出数据存储本地化要求，相当于网络的完全控制，造成了类似商品的非关税壁垒。认为政府有权力也有责任在居民的数据跨越国界时保护其隐私和安全，可以通过工具来实现这些目标，包括要求公司遵守高安全性和隐私标准的合同条款、对外国供应商的审计和认证、东道国法律对外国供应商的保护措施、遵守国际协议和标准、声誉制裁。强制数据本地化不利于全球创新发展，必须坚持没有数据保护主义的数据保护。[140]Matthias Bauer，Martina F. Ferracane 和 Erik van der Marel 指出各国探索从实施主体、彻底程度、覆盖的数据范围、本地化存储的豁免条件入手规制数据本地化措施。[141]Bret Cohen, Britanie Hall 和 Charlie Wood 介绍了全球范围内数据本地化政策的三种类型，即（1）强制本地化要求，如俄罗斯、中国、印度尼西亚要求广泛行业的数据存储于境内服务器上；（2）特定行业数据本地化要求，如澳大利亚、德国、韩国和委内瑞拉要求将从其公民处收集的某些金融、健康和医疗信息、在线发布和电信数据存储在本地服务器上；（3）重要数据的本地化要求。如美国在内的许多国家要求将与特定政府交易或重要国家安全问题相关的数据存储在本地。[142]Bret Cohen, Britanie Hall,和 Charlie Wood 认为应对本地化政策，企业必须在开放新的数据中心、改变网络架构、使用本地云供应商中作出选择。[143]

Neha Mishra 解释了限制跨境数据流动的措施在实践中是如何运作的，以及具有贸易限制效应的不同类型的数据限制措施，指出某些措施可能不是针对数据的性质或内容，而是针对数据的存储、传输、处理和防止未经授权的入侵的方式，例如数据本地化措施。数据限制措施目的在于保护个人隐私、数据或网络的安全。[144]H Jacqueline Brehmer 认为 Schrems I（Data Protection Commissioner *v.*

---

[139] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY LAW JOURNAL 677, 677-739 (2014); See also Walczuch R M, Singh S K & Palmer T S, *An Analysis of the Cultural Motivations for Transborder Data Flow Legislation*, 8 INFORMATION TECHNOLOGY & PEOPLE 37, 37-57 (1995); See also Joshua Paul Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & THE PACIFIC POLICY STUDIES 90, 90-102 (2015).

[140] Anupam Chander, Uyên P. Lê, *Data Nationalism*, 64 EMORY LAW JOURNAL 677, 39 (2014).

[141] Matthias Bauer，Martina F. Ferracane，Erik van der Marel, *Tracing the Economic Impact of Regu lations on the Free Flow of Data and Data Localization: Global Commission on Internet Governance*, Ce ntre for International Governance Innovation(1 May 2016), https://www.cigionline.org/sites/default/files/gcig_ no30web_2.pdf (last visited October 10, 2026).

[142] Bret Cohen, Britanie Hall, Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy,* 32 ANTITRUST LAW JOURNAL 107, 107-112 (2017).

[143] Bret Cohen, Britanie Hall & Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy,* 32 ANTITRUST LAW JOURNAL 107, 107-112 (2017).

[144] Neha Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of*

Schrems）和合众国诉微软案（United States *v*. Microsoft Corp） 突出了美国和欧盟对数据隐私的不可调和的不同实践。这些案例通过打开增加立法的大门、禁止来自欧盟的数据传输以及限制执法请求的数据移动从而鼓励数据本地化。这些限制，无论是出于商业还是执法的目的，都通过将数据置于政府控制之下和分割企业信息安全实践，增加了公司成本，扩大了网络安全威胁的攻击面，并降低了数据安全工具的功效，破坏了用户隐私和企业数据安全。[145]

国家安全是本地化义务的主要理由，但其定义的模糊性引发争议。文献指出，部分国家以国家安全为由实施保护主义，限制外国企业进入市场。例如，中国的本地化政策被批评为贸易壁垒，违反 WTO 原则。学者们争论如何在国际法中界定国家安全的合理范围以避免滥用数据本地化政策，本地化是保障国家核心利益的必要措施。WTO 法律体系允许国家在满足“必要性”和“比例性”原则基础上设定合理的监管壁垒，数据本地化可通过 GATS 第 14 条中的“公共政策例外”或 GATT 第 20 条中的“安全例外”加以解释。比例原则要求管制措施与国家安全目标相称，但人工智能的动态数据处理使得“必要性”难以界定。学者们认为，人工智能技术需要新的法律规制平衡框架以兼顾国家安全与全球数据流动。未来法规可能根据数据类型实施差异化本地化义务，以提高规则精准度。

人工智能技术的战略地位使得数据成为国家安全的关键组成部分，数据被视为战略资源，类似石油或关键基础设施，促使各国通过本地化政策加强对数据的管辖。[146]本地化政策旨在防止外国政府或企业通过跨境数据访问威胁国家安全，例如通过数据窃取或网络攻击。数据本地化义务被进一步强化，以保护人工智能相关的关键数据资产。国家主权强调对领土内包括数据资源的控制权，而数据本地化被视为维护国家安全和经济主权的工具，印度 DPDP ACT 也提出本地化要求，反映了发展中国家的类似关切。

数据本地化与人工智能创新需求之间的矛盾是核心争论。人工智能大模型依赖跨国数据以提升性能，而本地化政策可能导致数据孤岛化，降低模型训练效率。[147]例如，强制本地化可能限制人工智能企业获取多样化数据集，影响算法的泛化能力。[148]数据本地化正在从物理存储向处理本地化转型，即算法、训练模型也需

Data Flows, 52 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 463, 463-509 (2019).

[145] H Jacqueline Brehmer, *Data Localization: The Unintended Consequences of Privacy Litigatio*n, 67 AMERICAN UNIVERSITY LAW REVIEW 927, 969 (2017).

[146] JAN-FREDERIK KREMER & BENEDIKT MULLER, CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY, PROSPECTS AND CHALLENGES 3-20 (2024).

[147] Nigel Cory & Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, Information Techonology & Innovation Foundation(July 19 2021), https://www2.itif.org/2021-data-localization.pdf (last visited October 10, 2026).

[148] Emily M. Bender, et al., On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?, in FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (Madeleine

在境内运行。学者们争论是否应豁免人工智能相关数据以促进技术发展。

在人工智能背景下，数据本地化规则的碎片化增加了全球数据治理的复杂性和冲突性。GDPR 的隐私保护标准与中国的本地化要求形成冲突，导致企业在多国运营时面临合规困境。学者们争论是否需要全球统一的数据本地化规则，以及如何通过多边框架协调国家安全与数据自由流动。数据本地化不仅限于个人数据，还包括人工智能训练所需的非个人数据和推断数据，因其对国家战略技术的关键性而备受关注。本地化义务可能表现为强制性存储要求、跨境传输审查或数据出口限制。

“数据本地化义务”作为实现数据主权与国家安全的重要制度工具，在人工智能与数据全球化高度融合的背景下日益成为中外法律制度的重要分水岭。GDPR、CPTPP 等国际法律框架为本地化提供了间接依据，但各国实践的碎片化提高了合规复杂性。中国学界正在从合宪性、比例性、国际义务协调等维度对其进行深入研究，未来应继续推动制度细化与国际协调，以保障国家利益同时兼顾全球合作。

4.数据出口管制

数据出口管制指国家通过法律或政策限制数据的跨境传输，通常以保护国家安全、公共利益或经济主权为目标。[149]数据出口管制的起源与网络安全和国家主权理念的兴起密切相关。20 世纪末，数据跨境流动的增加促使各国关注数据安全。[150]21 世纪 10 年代，随着网络威胁和地缘政治竞争加剧，中国、俄罗斯等国家开始实施严格的数据出口管制。例如，2020 年《中华人民共和国出口管制法》的颁布，标志着我国首次在法律层面明确可对“数据等物项”实施出口限制。后续《数据安全法》《网络安全法》《个人信息保护法》等对数据跨境流动构建了初步的审查机制，管制措施包括数据分类审查、出口许可要求及跨境传输禁令，但尚未形成一套体系化的数据出口法典结构，相关制度设计仍处于逐步推进阶段。俄罗斯《联邦数据保护法》（Bundesdatenschutzgesetz）规定公民数据不得随意出口。发展中国家如印度也在 DPDP Act 中引入了出口限制措施。随着人工智能技术的发展与全球战略格局的演变，数据出口逐渐被纳入国家安全治理体系之中，相关制度架构也从传统物理物项出口管制向涵盖数据、算法、模型等无形物的多维扩展。

在国际层面，目前尚无统一的数据出口管制国际规则。美国通过《出口管理条例》（Export Administration Regulations）对生成式训练软件、芯片设计资料等

Clare Elish, William Isaac & Richard S. Zemel, 2021).

[149] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY LAW JOURNAL 677, 710-739(2015).

[150] Christopher Kuner, Lee A. Bygrave & Christopher Docksey, The EU General Data Protection Regulation: A Commentary 57 (Laura Drechsler ed., 2020).

纳入其敏感技术清单，限制向某些国家的输出；欧盟虽推动数据自由流动，但其《数据法案》（Data Act）《数字服务法》（Digital Services Act）等法律也在特定条件下限制向非欧盟国家的数据传输。中国法律对数据出口的规制采取原则管制加动态清单路径。《出口管制法》第 2 条赋予主管机关根据安全需要设立出口清单的权力，但对数据类物项的界定和适用机制仍待细化。有学者指出，出口管制制度应在尊重国家主权的同时，兼顾 WTO 等多边义务，尤其是与 GATT 和 GATS 安全例外条款的协调。但是也有学者认为，过度宽泛的数据出口管制若缺乏比例性与透明性，可能构成 WTO 项下的技术性贸易壁垒。

人工智能技术强化了网络主权理论对数据出口管制的支持，以保护人工智能相关的关键数据资产，如算法训练数据和国家安全敏感信息。人工智能的战略价值使得数据被视为国家主权的核心资产，出口管制成为维护数据主权的工具。人工智能系统依赖跨国数据集训练模型，促使各国通过管制防止数据外流以保护技术优势。然而，人工智能的分布式计算特性模糊了数据管辖边界，挑战传统主权理论。[151]同时，人工智能技术将数据提升为国家安全的关键要素，数据出口管制被视为防止技术泄露和外国干预的手段。[152]例如，人工智能模型可能通过数据推断敏感信息，增加国家安全风险。但人工智能的全球化研发模式要求数据跨境共享，管制可能阻碍技术进步，引发国家安全与创新的理论张力。[153]

人工智能技术对海量、多样化数据的需求与出口管制形成显著张力。生成式人工智能需跨国数据集以提升模型性能，而管制可能导致“数据孤岛化”，降低算法效率。[154]学者们争论是否应为人工智能训练数据设置管制豁免，或通过技术手段缓解矛盾。数据是国家数字疆域的组成部分，国家有权依据宪法与安全利益对其进出境进行管制，从而维护技术自主权和制度独立性。有学者主张监管范围从原始数据向模型、算法等延伸，人工智能模型与训练数据紧密相关，基于模型和训练数据高度欧和，模型权重本质上封装了从数学中学到的能力，为此管制也应当应涵盖模型结构、权重、代码输出等对象。

---

[151] Mira Burri , Digital Trade: In Search of Appropriate Regulation, in JUSTICE, TRADE, SECURITY AND INDIVIDUAL FREEDOMS IN THE DIGITAL SOCIETY, (Fernando Esteban De La Rosa et al. eds.,2021); Peter Swire & Kenesa Ahmad, Encryption and Globalization, 23 COLUMBIA SCIENCE AND TECHNOLOGY LAW REVIEW 416, 481(2011).

[152] Joshua P. Meltzer & Peter Lovelock, Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia, Brookings(March 20 2018), https://www.brookings.edu/articles/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/。

[153] Susan Ariel Aaronson , Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 245, 245-272(2018).

[154] Emily M. Bender, et al., On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?, in FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (Madeleine Clare Elish, William Isaac & Richard S. Zemel, 2021); Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, https://www2.itif.org/2021-data-localization.pdf (last visited October 10, 2026).

[155]人工智能技术增加了数据再识别的风险，挑战出口管制的有效性。机器学习算法可通过推断重新识别匿名化数据，增加跨境传输中的安全隐患。[156]例如，人工智能生成的推断数据可能被外国实体用于其他目的从而威胁国家安全。[157]学者们争论是否应将人工智能推断数据和非个人数据纳入管制范围，呼吁建立数据出口清单制度。

数据出口管制旨在限制数据跨境传输以保护国家安全，但人工智能技术的特性，如海量数据需求、动态处理、分布式计算等技术对传统管制机制提出了新挑战。首先，人工智能技术加剧了各国数据出口管制实践的差异。中国《数据安全法》要求对人工智能相关的“重要数据”进行安全评估，涵盖算法训练数据集。美国 CLOUD ACT 允许政府访问境外人工智能数据，挑战他国管制措施。印度 DPDP Act 对人工智能驱动的敏感数据出口设置严格许可要求。GDPR 的隐私要求与中国的安全审查机制冲突，导致人工智能企业在多国运营时合规成本上升。例如，人工智能云服务涉及多国数据中心，难以满足各国的管制要求。[158]因此，学者们争论是否需要全球统一标准以简化合规。

其次，人工智能技术对双边和区域协议的出口管制协调提出挑战。2019 年，《欧盟委员会关于日本为欧盟居民个人数据保护提供充分保护水平的决定》（Commission Decision on the Adequacy of the Protection Afforded by Japan to Personal Data，）（以下简称《欧盟-日本数据保护充分性协议》）通过统一隐私标准减少了管制需求，但未涵盖人工智能训练数据的特殊性。中美之间缺乏数据共享协议，导致人工智能企业在跨境传输中面临高昂合规成本。APEC-CBPR 试图通过认证机制缓解人工智能数据管制压力，但效果有限。

人工智能技术深刻影响了数据跨境流动中的数据出口管制规则，其海量数据需求、动态处理特性和再识别风险对传统管制机制提出了新挑战。GDPR、CPTPP 等国际框架为管制提供了间接依据，但各国实践的碎片化增加了人工智能企业的合规复杂性。数据出口管制制度作为国家应对外部技术压力、维护国家安全和科技竞争力的重要法律工具，已经成为我国数字治理体系中不可或缺的一环。

（三）数据跨境流动规则的国际协调

随着人工智能在全球范围内的广泛应用，大量涉及个人隐私、国家关键基础

---

[155] Joe Khawam, *Export Controls and Open-Weight AI: A Framework for Weights, Outputs, and Dow nstream Conduct*, https://lawreforminstitute.org/openweights081726.pdf (last visited October 10, 2026).

[156] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye. E*stimating the Success of Re-identifications in Incomplete Datasets Using Generative Models,* 10 NAT COMMUN 3069, 3078(2019).

[157] Sandra Wachter, Brent Mittelstadt*, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2 COLUMBIA BUSINESS LAW REVIEW 1, 79(2019).

[158] Thomas Burri, *A Challenge for Law and Artificial Intelligence*, 5 NATURE MACHINE INTELLIGENCE 1508, 1509 (2023).

设施与企业敏感信息的数据以算法驱动的方式在各国之间高速流动，由此引发的隐私保护与国家安全之间的制度张力日益受到国际法学界关注。在此背景下，各国政府、国际组织及跨国企业，尝试通过双边协定、区域协定及多边框架协商制定数据跨境治理的制度规范，以求在数字主权、隐私保护与全球数据经济之间达成动态平衡。

1.国际法框架中的协调

跨境数据流动限制措施是否符合国际法的相关研究。有学者认为跨境数据流动限制措施在现有国际规则框架下存在适用困难。有学者指出 WTO 和 TPP 在识别合法公共政策目标和不合理贸易限制时，存在适用上的不确定性。也有不少学者提出现有规则仍有适用的可能。MacDonald, Diane A., Streatfeild, Christine M. 介绍了 WTO 在处理保护互联网中个人数据方面所扮演的角色。主要讨论 GATS 规则如何适用处理跨境服务纠纷，个人数据隐私与国际贸易规则的冲突。[159]Arvin Kristopher Razon 针对区块链技术服务在 WTO 规则下的合规性作出分析。他认为虽然最近大多数数字服务贸易的变动是在优惠贸易协定的层面上进行的，而且在 GATS 复制这些深层次的数字贸易规则是一项长期的工作，但 GATS 足够灵活可以用于调整区块链技术服务，这意味着许多成员的禁止性或谨慎性法规——从禁止采矿到将拥有秘密货币定为犯罪——可能会成为贸易壁垒。他同时研究与区块链相关的服务部门和 GATS 承诺，GATS 第十四条适用的可能性。[160]Gregory Shaffer 认为《欧盟数据保护指令》在 WTO 规则下具有符合最惠国待遇条款、国民待遇原则、具有保护欧盟居民的隐私的公共政策目标的合法性。[161]Svetlana Yakovleva 和 Kristina Irion 认为 GDPR 可能违反 GATS，充分性调查结果的使用违反了最惠国待遇原则；欧盟对其成员国和非欧洲经济区国家，特别是美国进行的监测采用了双重标准，可能不符合欧盟的国民待遇承诺；限制政策无法通过“必要性检验”，充分性方法不属于“最小贸易限制”。[162]有学者针对限制措施是否符合投资协定作出研究，认为鉴于数据具备财产属性，东道国的数据本地化立法应符合其加入的国际投资协定。在认定东道国的数据本地化措施是否违背其根据投资协定时，应结合国际投资仲裁庭的相关裁判，区分数字企业所在经济部门，数据本地化措施的实施路径和对经济的负面影响程度，立法意在保

[159] MacDonald & Diane A., *Streatfeild, Christine M., Personal Data Privacy and the WTO*, 36 HOUSTON JOURNAL OF INTERNATIONAL LAW 625, 625-652 (2014).

[160] Arvin Kristopher Razon, *Liberalising Blockchain: An Application of the GATS Digital Trade Framework*, 20 MELBOURNE JOURNAL OF INTERNATIONAL LAW 125, 126-157(2019).

[161] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of US Privacy Standards*, 25 YALE JOURNAL OF INTERNATIONAL LAW 1, 79 (2000).

[162] Svetlana Yakovleva & Kristina Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, 114 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 10, 10-14 (2020).

护的价值及该价值在国内法中的体现等因素具体分析。

有关贸易与安全的冲突与平衡受到关注。Kathleen Claussen 指出，国内法和区域法中处理贸易和新兴安全利益之间冲突的机制，如法定紧急权力、贸易制裁、出口管制和投资筛选，正在经历自身的重新配置。[163]J. Benton Heath 认为贸易与安全之间的关系似乎正在经历历史性转变的时刻。“国家安全”概念不断扩展，已被认为包括产业安全、网络安全以及应对气候变化和流行病等问题，各国政府对自身重大利益的观念正在迅速转变，而解决贸易与安全之间的冲突可以采取结构化政治、贸易法律主义和司法管理主义三种方式。每种方式都存在监督和灵活性方面的权衡，并且都与理想的制度环境相关联，不应试图证明一种模式适用于所有环境和所有目的，而应拥抱多元化。所以，从网络安全的角度来看，一些安全例外似乎已经过时或不适合解决当代现实。最近的例外情况，如美国针对华为、Tiktok、Grindr 的事件，其倾向性的提法似乎将网络安全措施凌驾于贸易规则之上。他发现更加灵活和开放的安全例外出现在相同的协议中，例如 CPTPP 和 USMCA 协议，这些协议也旨在为数字贸易提供最先进的规则。《美日数字贸易协定》（U.S.-Japan Digital Trade Agreement） 集合了美国在电子商务和数据自由流动方面的所有最新创新，然而仍不排除一方“采取其认为必要的措施”保护其自身的基本安全利益。[164]

隐私保护是跨境数据流动治理的核心议题之一。在国际法层面，《公民权利和政治权利国际公约》（International Covenant on Civil and Political Rights）第 17 条明确规定了隐私权的保护，但其条款较为原则性，缺乏针对人工智能数据处理的细化规则。Chander 等人指出，国际法在隐私保护方面的碎片化导致各国在人工智能数据跨境流动中的规则冲突。例如，美国倾向于通过市场驱动的方式促进数据自由流动，而中国则强调数据主权和国家安全优先。双边和多边协议为解决隐私保护问题提供了重要平台。USMCA 的数字贸易章节要求成员国制定隐私保护法律，同时鼓励数据自由流动。然而，USMCA 并未明确针对人工智能技术对隐私的具体影响，限制了其适用性。相比之下，APEC-CBPR 通过自愿性认证机制，试图在隐私保护与数据流动之间找到平衡。Greenleaf 指出，CBPR 的灵活性使其在亚太地区具有吸引力，但其非强制性特点导致执行力度不足，难以应对人工智能驱动的数据处理复杂性。

人工智能技术的高速发展对现有国际规则提出了新挑战。首先，人工智能对大规模、实时数据的依赖加剧了隐私保护的复杂性。Veale 和 Binns 指出，机器

[163] Kathleen Claussen, *Trade's Security Exceptionalism*, 72 STANFORD LAW REVIEW 1097, 1100-1164 (2020).

[164] J.Benton Heath, *Trade and Security among the Ruins*, 30 DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 223, 265 (2019).

学习模型可能通过推理攻击（inference attack）从匿名数据中提取敏感信息，这对传统隐私保护机制构成了挑战。其次，人工智能的黑箱特性使得数据处理过程的透明度和问责制难以实现，这与 GDPR 等框架的透明性要求相冲突。最后，人工智能的全球部署使得数据跨境流动的管辖权问题更加复杂，特别是在云服务和分布式计算环境中。

数据跨境流动规则的国际法律框架主要由多边、区域和双边协议构成。学者们普遍提到 WTO 协定、CPTPP、RCEP 等贸易协定对数据流动的规范。例如，Meltzer 指出，CPTPP 第 14.11 条明确规定了数据自由流动原则，同时允许为保护公共利益而设置例外条款。[165]然而，WTO 框架下的 GATS 对数据流动的规定较为模糊，难以适应人工智能驱动的数字化经济需求。[166]区域贸易协定在数据跨境流动方面取得了一定进展。CPTPP 和 USMCA 均包含数据自由流动条款，但允许各国以“合法公共政策目标”为由设置限制。然而，区域协定的碎片化导致全球规则的不统一。例如，RCEP 对数据流动的约束较弱，未能有效协调成员国之间的法律差异。现有研究为人工智能驱动的跨境数据流动提供了重要见解。GDPR 和 CBPR 等框架展示了隐私保护的多边合作潜力，而 USMCA 和 RCEP 等协议则反映了数据自由流动与国家安全之间的权衡。

国家安全是限制跨境数据流动的重要考量因素。国际法中的主权原则允许各国以国家安全为由对数据流动实施限制。GATS 第 14 条允许成员国以“维护公共秩序或国家安全”为由限制数据流动，但其适用范围在人工智能背景下仍存争议。例如，中国通过《数据安全法》和《个人信息保护法》建立了严格的数据本地化要求，强调国家安全优先。相比之下，美国更多依赖出口管制和网络安全审查机制，如《外国投资风险审查现代化法案》（Foreign Investment Risk Review Modernization Act）。在双边和多边规则中，国家安全与数据流动的平衡是一个复杂问题。RCEP 通过促进数据自由流动推动区域经济一体化，但其条款允许成员国以国家安全为由实施数据限制。Selby 批评 RCEP 在国家安全例外条款的定义上过于宽泛，可能导致滥用，削弱数据自由流动的目标。此外，欧盟与日本的 EPA 通过相互承认数据保护标准，试图在隐私保护与国家安全之间找到平衡，但其适用范围局限于双方的高标准数据保护体系。

2.国家层面的冲突与协调

各国重视跨境数据流动规制，但是国家间规则存在差异。Kuner 较为全面地回顾了 1980 至 2010 年间，全球范围内跨境数据流动立法的情况，并分析了背后

[165] Joshua Paul Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & THE PACIFIC POLICY STUDIES 90, 90-102(2015).

[166] Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 245, 245-272(2018).

的原因，指出商业和技术环境的根本变化使得个人数据处理发生变化。[167]随着人工智能技术对数据依赖程度的加深，数据跨境流动在隐私保护与国家安全之间的张力日益显著。中、美、欧三方作为全球数字治理中的关键参与者，在制度设计、理论基础与实践路径上展现出不同治理理念和规范导向。已有文献对此进行多维度分析，构成了当下国际数据治理研究的重要基础。

欧盟在数据治理上坚持“人格尊严”优先，强调个人数据是一种基本权利。欧盟 GDPR 确立了“充分性认定”机制，将数据跨境流动置于对方国家制度评估之上，形成一种规范扩张路径。[168]美国则基于“市场导向”与“国家安全优先”的逻辑，数据隐私保护零散分布于多个行业性法规中，国家安全通过《外国情报监视法》（United States Foreign Intelligence Surveillance Court）与行政命令授权的大规模数据获取体制构成核心。[169]中国自 2015 年提出网络主权以来，逐步构建数据本地化、出境安全评估、重要数据分类管理等制度，强调以安全为底线的数据治理理念。

欧盟在人工智能数据治理方面已提出《人工智能法案》（Artificial Intelligence Act，以下简称 AI Act），将人工智能系统按照风险分类治理，并要求算法可解释性与人类监督机制。GDPR 中的“自动决策”条款为人工智能算法施加合规责任提供基础。美国则依赖联邦贸易委员会等部门通过执法实践处理人工智能数据滥用问题，尚未形成统一法典。中国通过《个人信息保护法》《数据安全法》与算法推荐管理规定，建立人工智能数据活动分类监管与出境评估机制，尤其重视算法透明、备案与数据出境合规性。

欧盟模式被称为“规范帝国主义”，其充分性机制引发与美国、日本等国家的冲突（如“Schrems II”案）；[170]美国的国家安全优先逻辑被指侵蚀用户隐私权，限制对外制度互认；[171]而中国的本地化义务与“关键信息基础设施”模糊定义也引发企业界对合规不确定性的担忧。人工智能技术的不可解释性、黑箱性及大模型的跨境适用性进一步加剧了制度冲突，亟需在隐私与安全之间重建制度平衡。三方均趋于结构性重构而非价值趋同，欧盟强调人工智能伦理与基本权保障，推进 AI Act 立法进程；美国则通过执行与“软法”工具加强人工智能治理，提

---

[167] Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future, 16 Tilburg Institute for Law, Technology, and Society Working Paper, 2010.

[168] Oskar J. Gstrein & Andrej Zwitter, *Extraterritorial Application of the GDPR: Promoting European Values or Power?*, 3 Internet Policy Review 1576, (2021).

[169] Marc Rotenberg, *In Support of a Privacy Protection Board in the United States*, 8 GOVERNMENT INFORMATION QUARTERLY 79,79-80(2007).

[170] CJEU, Schrems II Case, Case C-311/18, 2020.

[171] Peter Swire, DeBrae Kennedy-Mayo, Drew Bagley, Sven Krasser, Avani Modak & Christoph Bausewein, *Risks to Cybersecurity from Data Localization,Organized by Techniques, Tactics and Procedures*, 9 JOURNAL OF CYBER POLICY 20, 37(2014),

出“可信人工智能标准体系；中国则推进“数据出境审查”的治理逻辑，强化平台责任与国家安全保护。

在区域合作方面，OECD 关于保护隐私和个人数据跨国界流动的准则的可信数据流动原则、中德数据跨境流动合作和中欧数据跨境流动交流机制等成为多边协调平台，但短期内达成统一强制性规则的可能性仍有限。GDPR 通过数据最小化、目的限制和跨境传输限制等原则，为人工智能处理数据的跨境流动提供了法律框架。Hoofnagle 等人指出，GDPR 的充分性决定机制要求数据接收国的隐私保护水平与欧盟相当，这对多边数据流动规则的制定产生了深远影响。[172]然而，GDPR 的严格要求也引发了关于其对全球数据经济效率的潜在限制的讨论，GDPR 的高合规成本可能阻碍中小型企业在全球市场中的竞争力。[173]GDPR 的“充分性决定”机制要求数据接收国的保护水平与欧盟相当，这在人工智能背景下引发了与非欧盟国家的法律冲突。例如，美国的 CLOUND ACT 允许政府在特定情况下访问存储在境外的用户数据，与 GDPR 的隐私保护要求相矛盾。双边协议是解决数据跨境流动问题的重要途径。例如，《欧盟-日本数据保护充分性协议》为数据流动提供了法律基础，但其适用范围有限，未能涵盖人工智能训练所需的非个人数据。[174]此外，中美之间缺乏类似协议，导致企业在跨境数据传输中面临高昂的合规成本。

四、评述

数据作为人工智能技术发展的核心要素，就有学者曾经预计，数据跨境流动的规制路径将从禁止性规定向有限制、有例外相统筹的方式转变，数据要素根据安全风险敏感度进行分类分级处理将成为跨境有序安全流动的有益方式。新一轮人工智能技术的发展对数据跨进管制原则、政策、格局提出了要求，各国为获取数据，已不再坚持对个人数据保护水平的严格要求并调整数据跨境管制立场，祈求与更多国家缔结数据跨境流动协定，“谋划以他国数据推动本国新一代人工智能技术的发展。”

生成式人工智能开发者和部署者开展数据跨境尤其是个人信息跨境传输活动中，未严格遵循数据出境评估、标准合同、个人信息保护认证等要求，存在潜

---

[172] Chris Jay Hoonfnagle, Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What it is and What it Means*. 28 INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 65, 97-98(2019).

[173] Han-Wei Liu, *Data Localization and Digital Trade Barriers: ASEAN in Megaregionlism*, in ASEAN LAW IN THE NEW REGIONAL ECONOMIC ORDER: GLOBAL TRENDS AND SHIFTING PARADIGMS (Pasha L. Hsieh & Bryan Mercurio eds., 2019).

[174] Graham Greenleaf, Global Data Privacy Laws 2019: 132 National Laws & Many Bills, 157 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 14, 18(2019).

在风险，即相关主体未满足或充分承担“说明—同意”义务、数据最小化原则、诸如删除权、被遗忘权、撤销-同意以及数据安全保障权利，将面临合规风险和法律制裁。对于需跨境调用算法或算力的生成式人工智能开发者和部署者，以及人工智能企业出海开拓域外市场需要而言，数据跨境合规已成为制约其发展的痛点。这不仅影响生成式人工智能模型的训练效果，也增加了中小型生成式人工智能开发者和部署者获取云计算等商业服务的成本，不利于生成式人工智能产业的整体创新，最终可能削弱国家在审查式人工智能领域的国际竞争力。

然而，现有研究存在以下不足，首先，当前各国研究主要是针对生成式人工智能技术爆发前的数据跨境流动规则，在生成式人工智能发展技术席卷全球后，针对人工智能的“基础模型—通用模型—专业模型”的业态和“基础层—技术层—应用层”的产业链构造，仍然缺少数据跨境在人工智能产业实践中面临的隐私保护、国家安全等问题能否以及如何在传统数据跨境流动规则下解决的专门研究；其次，虽然当前有研究提出全球主要国家或地区处于人工智能军备竞赛的需要，开始转变数据跨境流动规则方向，尤其是中国开始逐渐放松数据跨境流动管制，但我国目前尚未与欧盟、美国等签订数据跨境流动双边或多边协议，同时，双边和多边规则的碎片化导致全球数据治理缺乏统一标准，提高了中国人工智能企业合规成本。最后，关于如何在隐私保护与国家安全之间，尤其是在人工智能驱动的实时数据流动场景中通过规则协调实现动态平衡的研究仍然有限，针对技术特性的国际法规则仍显不足，现有框架多基于传统数据处理场景，难以应对人工智能的动态性和复杂性。

五、参考文献

（一）中文著作

【1】 张琨蓓：《数字贸易中跨境数据流动法律规制问题研究》，法律出版社 2025 年版。

【2】 赵威：《数据跨境流动法律问题研究 国家治理、企业合规与技术创新》，中国政法大学出版社 2024 年版。

【3】 郑文阳：《数据安全法治化研究》，中国政法大学出版社 2024 年版。

【4】 何晶晶：《中国健康医疗数据跨境流动规制》，法律出版社 2023 年版。

【5】 何跃鹰、卓子寒：《全球数据跨境流动治理》，科学出版社 2023 年版。

【6】 张敏：《数据法学》，中国政法大学出版社 2023 年版。

【7】 朱琳：《大数据时代跨境数据流动治理研究》，苏州大学出版社 2022 年版。

【8】 武长海：《数据法学》，法律出版社 2022 年版。

【9】 叶进芬：《WTO 法框架下数字产品跨境交易规则研究》，中国原子能出版社 2022 年版。

【10】 范晓宇：《数据秩序的法律治理》，法律出版社 2022 年版。

【11】 张尧学、胡春明：《大数据导论》（第 2 版），机械工业出版社 2021 年版。

【12】 徐英瑾：《人工智能哲学十五讲》，北京大学出版社 2021 年版。

【13】 武长海：《国际数据法学》，法律出版社 2021 年版。

【14】 涂子沛：《数文明——大数据如何重塑人类文明、商业形态和个人世界》，中信出版社 2018 年版。

【15】 王融：《大数据时代 数据保护与流动规则》，人民有点出版社 2017 年版。

【16】【美】弥尔顿·L·穆勒：《网络与国家》，周程、鲁锐、夏雪、郑凯伦译，上海交通大学出版社 2015 年版。

【17】【英】玛格丽特·A·博登：《人工智能哲学》，刘西瑞、王汉琦译，上海译文出版社 2006 年版。

（二）中文论文

【18】 张桁嘉、尤建新：《智能网联汽车数据风险的研究热点与展望》，载《上海管理科学》2025 年第 1 期。

【19】王小林、兰松：《“数字丝绸之路”数据跨境流动机制:逻辑框架与路径选择》，载《人文杂志》2025 年 1 月。

【20】魏媛媛：《人工智能时代的数据安全与国际治理合作框架探究》，载《中国科学院院刊》2025 年第 4 期。

【21】徐玉梅、杨柳等：《“自由”与“主权”：数据跨境流动治理模式的动态博弈——基于全球数字贸易规则视角》，载《行政论坛》2024 年第 6 期。

【22】洪延青：《中国数据出境安全管理制度的“再平衡”——基于国家间数据竞争战略的视角》，载《中国法律评论》2024 年第 3 期。

【23】张子琳、彭德雷：《CPTPP 核心数字贸易规则与中国加入谈判因应——基与 RCEP 的对比分析》，载《上海对外经贸大学学报》2024 年第 2 期。

【24】洪延青：《中国数据出境安全管理制度的“再平衡”——基于国家间数据竞争战略的视角》，载《中国法律评论》2024 年第 3 期。

【25】张墨洋：《我国证券公司数据出境的合规困境与监管应对》，载《天府新论》2024 年第 2 期。

【26】马忠法、郑文龙：《上海自贸试验区对接 DEPA 跨境数据流动规则：动因、差距及完善路径》，载《上海财经大学学报》2024 年第 4 期。

【27】吴玄：《海南自由贸易港数据跨境规则创新路径研究》，载《海南大学学报（人文社会科学版）》2024 年。

【28】张泳、闫芊伊：《粤澳数据跨境治理困境及其纾解——以横琴深合区数据跨境流通据点为视角》，载《港澳研究》2024 年第 4 期。

【29】孙冉：《粤港澳大湾区数据跨境流动的逻辑构造与优化进路》，载《地方立法研究》2024 年第 5 期。

【30】赵新潮：《个体权益·公共利益·国家安全：企业数据权利限制的三重考量》，载《湖北大学学报（哲学社会科学）》2024 年第 4 期。

【31】吴一楷：《金融安全观下我国涉外金融数据法治体系的生成逻辑与构建路径》，载《上海金融》2024 年第 2 期。

【32】张墨洋：《我国证券公司数据出境的合规困境与监管应对》，载《天府新论》2024 年第 2 期。

【33】冯泽华、刘志辉：《粤港澳大湾区金融数据跨境流动：现实问题与法治进路》，载《金融发展研究》2024 年第 5 期。

【34】陈永怡、孟彦辰：《澳大利亚健康医疗数据跨境流动法律规制研究及其对中国的启示》，载《中国全科医学》2024 年第 25 期。

【35】何俊辉：《不完全契约视角下的数据跨境流动沙盒监管机制研究》，载《数字图书馆论坛》2024 年第 4 期。

【36】张君周：《国际民航组织对旅客数据跨境流动的规制及挑战应对》，载《北京航空航天大学学报（社会科学版）》2024 年第 6 期。

【37】杨彩霞、邱圣童：《浅析欧盟 GDPR 对民航数据跨境之影响》，载《北京航空航天大学学报（社会科学版）》2024 年第 6 期。

【38】王珺、周小林、沈云怡、李子愚、任孝、杨云：《科学数据跨境流动治理的现状、思考与展望》，载《科学通报》2024 年第 14 期。

【39】单文华、邓娜：《从“数据隐私框架”看欧美数据跨境流动的规则博弈》，载《太平洋学报》2024 年第 1 期。

【40】廖欢、王义桅：《中美大国竞争视角下的美国全球数字战略研究》，载《中国科技论坛》2024 年第 6 期。

【41】杨楠：《美国对华数据政策论析》，载《情报杂志》2024 年第 8 期。

【42】陈振华、张伟华、王秉：《欧盟个人数据跨境流动充分性决定制度之评价分析》，载《太平洋学报》2024 年第 1 期。

【43】赵祺：《中国—东盟跨境数据流动治理合作：现实与路径选择》，载《南洋问题研究》2024 年第 3 期。

【44】曹旭东、桑栩：《论香港与内地个人信息的协同保护》，载《港澳研究》2024 年第 1 期。

【45】王彬彬、邓小婷：《JSI 谈判模式下中国国际数字贸易规则的建构》，载《国际贸易》2024 年第 12 期。

【46】郭朝先、李婷、罗芳：《数据跨境流通规则博弈与中国应对》，《中国流通经济》2024 年第 9 期。

【47】冉从敬：《捍卫国家数据主权刻不容缓》，载《图书馆论坛》2023 年第 9 期。

【48】熊光清、张素敏：《总体国家安全观视角下我国数据出境安全管理制度的完善》，载《哈尔滨工业大学学报（哲学社会科学版）》2023 年第 5 期。

【49】李烨：《RCEP 协定下我国数据跨境流动规则的检视与完善》，载《科技与法律（中英文）》2023 年第 1 期。

【50】张晓君、刘泽杨：《RCEP 数据跨境流动基本安全例外条款与中国方案》，载《郑州大学学报（哲学社会科学版本）》2023 年第 4 期。

【51】马忠法、苏婧怡：《RCEP 框架下共建中国—东盟跨境数据流动治理合作机制的挑战及因应之道》，载《广西社会科学》2023 年第 10 期。

【52】梅傲、李淮俊：《数字贸易中数据跨境流动规则的新发展——基于〈数据出境安全评估办法〉与 DEPA 的比较》，《企业经济》2023 年第 4 期。

【53】宋晓舒：《DEPA 视角下的数字贸易规则发展与应对策略》，载《商

业经济研究 》2023 年第 22 期。

【54】朱雅妮：《〈数字经济伙伴关系协定〉的治理重心、推进策略及中国的加入谈判》，载《南昌大学学报（人文社会科学版）》2023 年第 5 期。

【55】王楚晴：《申请加入 DEPA 背景下中国数据治理的相容性审视及优化路径》，载《太平洋学报》2023 年第 3 期。

【56】周念利、于美月：《“新式”数字贸易规则的演进趋向研究——基于 UKSDEA 和 KSDPA 的视角》，载《理论学刊》2023 年第 4 期。

【57】黄贵、陶如：《RCEP 缔约国数据跨境流动政策的数字生产力基础及其影响——以数字融合指数为参照》，载《中国科学院院刊》2023 年第 8 期。

【58】朱简：《数据跨境传输的制度困囿与优化设计——以浙江自由贸易试验区为例》，载《商业经济研究》2023 年第 7 期。

【59】周念利、于美月、刘春苗：《我国自贸区（港）数据跨境流动试点制度创新研究》，载《国际商务研究》2023 年第 4 期。

【60】黄琳琳：《金融数据跨境流动的国际贸易法规制》，载《上海对外经贸大学学报》2023 年第 6 期。

【61】郭德香、刘畅：《个人金融数据跨境流动法律规制的国际经验及中国因应》，载《征信》2023 年第 11 期。

【62】刘妍、冉从敬：《金融数据跨境监管的国际策略与中国进路》，载《金融评论》2023 年第 4 期。

【63】刘业：《美欧数据跨境流动博弈中的欧盟技术主权战略及其实现》，载《国际法研究》2023 年第 6 期。

【64】马忠法、苏婧怡：《RCEP 框架下共建中国—东盟跨境数据流动治理合作机制的挑战及因应之道》，载《广西社会科学》2023 年第 10 期。

【65】孙南翔：《CPTPP 数字贸易规则：制度博弈、规范差异与中国因应》，载《学术论坛》2022 年第 5 期。

【66】刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，载《行政法学研究》2022 年第 4 期。

【67】洪治刚、霍俊先：《RCEP 对数据跨境流动的规制及其重要影响》，载《西南金融》2022 年第 4 期。

【68】孙南翔：《CPTPP 数字贸易规则：制度博弈、规范差异与中国因应》，载《学术论坛》2022 年第 5 期。

【69】王玫黎、陈雨：《中国数据跨境流动规则与 CPTPP 的对接研究》，载《国际贸易》2022 年第 4 期。

【70】王玫黎、陈雨：《中国数据跨境流动规则与 CPTPP 的对接研究》，

载《国际贸易》2022 年第 4 期。

【71】赵精武：《数据跨境传输中标准化合同的构建基础与监管转型》，载《法律科学（西北政法大学学报）》2022 年第 2 期。

【72】刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，载《行政法学研究》2022 年第 4 期。

【73】卜学民、马其家：《论数据主权谦抑性：法理、现实与规则构造》，载《情报杂志》2021 年第 8 期。

【74】许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期。

【75】魏远山：《博弈论视角下跨境数据流动的问题与对策研究》，载《西安交通大学学报（社会科学版）》2021 年第 5 期。

【76】盛斌、高疆：《数字贸易：一个分析框架》，载《国际贸易问题》2021 年第 8 期。

【77】黄现清:《数字贸易背景下我国数据跨境流动监管规则的构建路径》，载《西南金融》2021 年第 8 期。

【78】许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期。

【79】马其家、李晓楠：《论我国数据跨境流动监管规则的构建》，载《法治研究》2021 年第 1 期。

【80】李金、申苏浩、孙晓蕾、邢潇：《重要数据跨境流动背景下风险路径的识别与分级》，载《中国管理科学》2021 年第 3 期。

【81】王玉珏、吴一诺、凌敏菡：《〈数据安全法〉与〈档案法〉协调研究》，载《图书情报工作》2021 年第 22 期。

【82】赵海乐：《比较法视角下的我国“车联网”数据治理路径选择》，载《上海财经大学学报》2021 年第 5 期。

【83】马治国、胡明强、张磊：《我国人工智能基础数据的专门法保护研究》，载《西北大学学报（哲学社会科学版）》2021 年第 6 期。

【84】洪延青：《数据竞争的美欧战略立场及中国因应——基于国内立法与经贸协定谈判双重视角》，载《国际法研究》2021 年第 6 期。

【85】董京波：《跨境数据流动安全治理》，载《科技导报》2021 年第 21 期。

【86】茶洪旺、付伟、郑婷婷：《数据跨境流动政策的国际比较与反思》，载《电子政务》2019 年第 5 期。

【87】齐爱民：《论大数据时代数据安全法律综合保护的完善——以〈网

络安全法〉为视角》，载《东北师大学报（哲学社会科学版）》2017 年第 4 期。

【88】 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》，载《太平洋学报》2015 年第 2 期。

【89】 董储超:《CPTPP 架构下数据跨境流动规则的时代表征与中国因应》，载《情报杂志》2024 第 7 期。

（三）学位论文

【90】 赵世璐：《跨境数据流动的例外规则研究》，华东政法大学 2024 年博士论文。

【91】 李晴：《个人数据跨境流动国际监管的法律问题研究》，辽宁大学 2023 年博士论文。

【92】 薛妮：《海南自由贸易港数据跨境流动法律制度研究》，海南大学 2023 年博士论文。

【93】 黄钰：《欧盟数据跨境流动监管的主要法律问题研究》，中南财经政法大学 2023 年博士论文。

【94】 余佳亮：《数字贸易背景下的跨境数据监管研究》，中南财经政法大学 2023 年博士论文。

【95】 白芳艳：《数字贸易的国际治理及其因应——以 CPTPP、DEPA 和 WTO 诸边判等为视角》，对外经济贸易大学 2023 年博士论文。

【96】 陈思:《数据跨境流动监管协调机制研究》，对外经济贸易大学 2023 年博士论文。

【97】 卜学民：《个人数据跨境传输限制法律问题研究》，对外经济贸易大学 2022 年博士论文。

【98】 姚亭亭：《数据跨境流动限制性措施对数字服务贸易的影响研究》，对外经济贸易法学 2022 年博士论文。

【99】 周濛：《云时代个人数据保护的国际法问题研究》，武汉大学 2021 年博士论文。

【100】 王基岩：《个人金融数据跨境流动法律制度研究》，重庆大学 2020 年博士论文。

【101】 田心月：《欧盟跨境数据流动法律规制研究》，武汉大学 2020 年博士论文。

【102】 伍艺:《欧美个人数据跨境流动规则比较研究——以数据隐私保护为视角》，西南政法大学 2020 年博士论文。

【103】 张舵：《跨境数据流动的法律规制问题研究》，对外经济贸易大学 2018 年博士论文。

（三）英文著作

【104】 JULIEN CHAISSE & CHRISTOPH HERRMANN (ED.), THE INTERNATIONAL LAW OF ECONOMIC INTEGRATION, OXFORD ACADEMIC, 2025.

【105】 SVETLANA YAKOVLEVA, GOVERNING CROSS-BORDER DATA FLOWS: RECONCILING EU DATA PROTECTION AND INTERNATIONAL TRADE LAW, OXFORD ACADEMIC, 2024.

【106】 SIMONE FISCHER-HÜBNER & FARZANEH KAREGAR, THE CURIOUS CASE OF USABLE PRIVACY: CHALLENGES, SOLUTIONS, AND PROSPECTS, SPRINGER, 2024.

【107】 ROMAN PASCAL KALIN, DIGITAL TRADE AND DATA PRIVACY：CROSS-BORDER FLOWS OF PERSONAL DATA BETWEEN DATA PROTECTION AND DATA PROTECTIONISM, SPRINGER, 2024.

【108】 ANUPAM CHANDER & HAOCHEN SUN (ED.), DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE, OXFORD ACADEMIC, 2023.

【109】 ALESSANDRO MANTELERO, BEYOND DATA: HUMAN RIGHTS, ETHICAL AND SOCIAL IMPACT ASSESSMENT IN AI, SPRINGER, 2022.

【110】 BRYAN MERCURIO & RONALD YU, REGULATING CROSS-BORDER DATA FLOWS: ISSUES, CHALLENGES AND IMPACT, ANTHEM PRESS, 2022.

【111】 DANIEL BETHLEHEM (ED.) ET AL., THE OXFORD HANDBOOK OF INTERNATIONAL TRADE LAW (2E) (2ND EDN), OXFORD ACADEMIC, 2022.

【112】 ERIC J. LARSON, THE MYTH OF ARTIFICIAL INTELLIGENCE: WHY COMPUTERS CAN’T THINK THE WAY WE DO, HARVARD UNIVERSITY PRESS, 2022.

【113】 MARTIN MOORE & DAMIAN TAMBINI (ED.), REGULATING BIG TECH: POLICY RESPONSES TO DIGITAL DOMINANCE, OXFORD ACADEMIC, 2021.

【114】 JULIEN CHAISSE, LEÏLA CHOUKROUNE & SUFIAN JUSOH, HANDBOOK OF INTERNATIONAL INVESTMENT LAW AND POLICY,

SPRINGER, 2021.

【115】 ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD, OXFORD UNIVERSITY PRESS, 2020.

【116】 BENEDICT KINGSBURY (ED.) ET AL., MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP, OXFORD ACADEMIC, 2019.

【117】 DAN JERKER B SVANTESSON AND DARIUSZ KLOZA (EDS), TRANS-ATLANTIC DATA PRIVACY RELATIONS AS A CHALLENGE FOR DEMOCRACY, CAMBRIDGE UNIVERSITY PRESS, 2018.

【118】 CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, OXFORD ACADEMIC, 2013.

【119】 CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, OXFORD UNIVERSITY PRESS, 2013.

【120】 DIRK VAN GERVEN, CROSS-BORDER MERGERS IN EUROPE, CAMBRIDGE UNIVERSITY PRESS, 2010.

（四）英文论文

【121】 Shuai Guo & Xiang Li, *Cross-Border Data Flow in China: Shifting from Restriction to Relaxation?* 56 COMPUTER LAW & SECURITY REVIEW 1(2025).

【122】 Wanxiu Xu, Shuo Wang & Xiaodong Zuo, *Global Data Governance at a Turning Point? Rethinking China-U.S. Cross-Border Data Flow Regulatory Models*, 55 COMPUTER LAW & SECURITY REVIEW 1 (2024).

【123】 Frank Schweitzer & Ian Saccomanno, *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade*, 1 THE GLOBAL TRADE LAW JOURNAL 1 (2024).

【124】 Meltzer, J. P., *The Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & THE PACIFIC POLICY STUDIES 90 (2015).

【125】 Mira Burri, *Cross-border data flows and privacy in global trade law: has trade trumped data protection?* 39 OXFORD REVIEW OF ECONOMIC POLICY 85 (2023).

【126】 Ferracane Martina Francesca, Janez Kren & Erik Van Der Marel, *Do Data Policy Restrictions Impact the Productivity Performance of Firms and*

Industries?, 28 REVIEW OF INTERNATIONAL ECONOMICS 676 (2020).

【127】 Xiao Xiaolei and Zhao Xuilian, *Review on the Governance of Cross-border Data Flow in China*, 10 INFORMATION NETWORK SECURITY 45 (2022).

【128】 Liu Jinrui, *Towards Global Regulation of Cross-border Data Flow: Basic Concerns and Chinese Solutions*, 4 ADMINISTRATIVE LAW STUDIES 73 (2022).

【129】 J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 THE YALE LAW JOURNAL 924 (2020) .

【130】 Shi Yuhang, *Sovereign Network Borders: Regulating Cross-border Data Transfers*, 37 INTELLIGENCE JOURNAL 160 (2018).

【131】 Rojszczak M, *CLOUD Act Agreements from an EU Perspective*, 38 COMPUTER LAW & SECURITY REVIEW 38 (2020).

【132】 Xavier Tracol, *"Schrems II": The return of the Privacy Shield*, 39 COMPUTER LAW & SECURITY REVIEW 105484 (2020).

【133】 Dan Jerker B. Svantesson & Lodewijk van Zwieten, *Law Enforcement Access to Evidence via Direct Contact with Cloud Providers - Identifying the Contours of a Solution*, 32 COMPUTER LAW & SECURITY REVIEW 671 (2016).

【134】 Xavier Tracol, *Invalidator Strikes Back: the Harbour has never been Safe*, 32 COMPUTER LAW & SECURITY REVIEW 345 (2016).

【135】 Jean-Baptiste Velut, *Trade Linkages or Disconnects? Labor Rights and Data Privacy in US Digital Trade Policy*, 11 POLITICS AND GOVERNANCE 249 (2023) .

【136】 Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 JOURNAL OF INTERNATIONAL ECONOMIC LAW 389 (2019).

【137】 W Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASHINGTON INTERNATIONAL LAW JOURNAL 485 (2019).

【138】 S Yakovleva, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade Deal?*, 17 WORLD TRADE REVIEW 477 (2017).

【139】 Anupam Chander, *Trade 2.0*, 34 YALE JOURNAL OF INTERNATIONAL LAW 281 (2009).

【140】 Andrew D Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 JOURNAL OF INTERNATIONAL ECONOMIC LAW 389 (2019).

【141】 Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST LAW REVIEW 57 (2018) .

【142】 Peiru Cai & Li Chen, *Demystifying Data Law in China: A Unified Regime of Tomorrow*, 12 INTERNATIONAL DATA PRIVACY LAW 75 (2022).

【143】 Daniel Albrecht, *Chinese First Personal Information Protection Law in Contrast to the European GDPR*, 23 COMPUTER LAW REVIEW INTERNATIONAL 1 (2022).

【144】 Fengan Jiang, *China's Legal Efforts to Facilitate Cross-Border Data Transfers: A Comprehensive Reality Check*, 32 ASIA PACIFIC LAW REVIEW 81 (2024) .

【145】 Paul M Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 THE GEORGETOWN LAW JOURNAL 115 (2017).

【146】 J. Russell Blakey, *The Foreign Investment Risk Review Modernization Act: The Double-Edged Sword of US Foreign Investment Regulations*, 53 LOYOLA OF LOS ANGELES LAW REVIEW 981 (2019).

【147】 Graham Greenleaf, S*heherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, 23 JOURNAL OF LAW, INFORMATION AND SCIENCE 4 (2014).

【148】 Susan Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, 18 WORLD TRADE REVIEW 541 (2019).