密码与网络空间安全 学院本科生 2024—2025 学年 第 1 学期

《国际贸易法》课程 期末论文

专业：信息安全、法学 学号：2113203 姓名：付政烨 成绩：

国际数字贸易中的跨境数据流动规制方案研究

摘 要

随着人工智能（AI）技术的飞速发展，跨境数据流动成为推动全球数字经济和 AI 技术创新的核心驱动力。然而，数据主权和隐私保护之间的矛盾日益突出，成为国际贸易法和数字治理中的重大挑战。各国通过立法强化对本国数据的控制，尤其在个人数据和敏感数据的跨境传输中，实施严格的法规，如欧盟的《通用数据保护条例》和中国的《数据安全法》等等。这些政策虽然保障了数据安全与隐私保护，但也加剧了跨境数据流动的法律冲突与合规难题，阻碍了全球技术合作与经济发展。为了平衡数据流动与隐私保护，本文提出了通过国际多边框架推动数据保护标准化、评估跨境数据流动的技术安全性、建立跨国纠纷解决机制等措施。通过加密技术、去标识化与匿名化、数据审计与合规性日志等技术手段，提升数据安全性与隐私保护。最终，本文呼吁国际社会加强合作，构建更加完善的数字治理体系，推动数据流动自由化与隐私保护的和谐共生，促进全球经济和 AI 技术的可持续发展。

关键词：跨境数据流动；数据主权；隐私保护；GDPR

目 录

一、引言

随着人工智能（AI）技术的飞速发展，数字经济在全球范围内迅速崛起，成为推动各国经济增长的关键力量。在这一进程中，跨境数据流动成为AI技术创新与国际贸易的核心驱动力。AI的研发与应用，尤其是在机器学习和大数据分析等领域，依赖于大量的跨境数据流动[①]。然而，数据流动背后隐藏着复杂的法律与伦理问题，特别是在数据主权和隐私保护方面，成为全球数字经济发展中的重要挑战。在数字经济时代，各国对数据主权的关注愈加增强，纷纷通过立法强化对本国数据的控制。数据主权，指的是国家或地区在其境内对数据流动、存储与使用的主权管理[②]。这一理念近年来得到广泛推动，许多国家出台了数据本地化和隐私保护法规，试图在保障国家安全与个人隐私的同时控制数据跨境流动。然而，这些政策往往阻碍了跨境数据的流动，尤其在AI技术的国际合作与贸易中，带来了不少法律与合规难题。然而，现有研究表明，AI技术的快速发展离不开全球数据的共享与流通，而跨境数据流动的障碍不仅阻碍了国际技术合作，还可能加剧全球科技竞争中的不平衡，影响技术进步与经济发展[③④⑤]。因此，在确保隐私和国家安全的前提下，如何推动数据流动自由化，已成为国际贸易法与数字治理亟待解决的关键问题。

二、数据主权对AI跨境贸易的影响

数据主权作为现代国家治理的一个重要方面，已经成为全球数字经济和国际贸易中的核心议题。这一概念随着大数据、云计算和AI技术的崛起愈加引起各国政府的高度重视。特别是在跨境数据流动日益频繁的今天，各国纷纷出台相关政策，强调数据的本地化存储和处理，例如，欧盟的《通用数据保护条例》（GDPR）、中国的《数据安全法》和美国加州的《消费者隐私法案》（CCPA）。这些政策对跨境AI技术贸易产生了深远的影响，直接影响着AI技术的发展和全球化布局。

数据主权对AI跨境贸易的主要限制于对数据跨境转移设置了严格的条件。特别是在涉及个人数据、尤其是敏感数据的跨境传输时，这些政策通常要求对数据流动实施严

① Mayer-Schönberger V, Cukier K. Big data: A revolution that will transform how we live, work, and think[M]. Houghton Mifflin Harcourt, 2013.
② Voigt P, Von dem Bussche A. The eu general data protection regulation (gdpr)[J]. A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017, 10(3152676): 10-5555.
③ Brynjolfsson E, McAfee A. The second machine age: Work, progress, and prosperity in a time of brilliant technologies[M]. WW Norton & company, 2014.
④ Chander A, Lê U P. Data nationalism[J]. Emory LJ, 2014, 64: 677.
⑤ Meltzer J P. The I nternet, Cross‐Border Data Flows and International Trade[J]. Asia & the Pacific Policy Studies, 2015, 2(1): 90-102.

格监管。例如，GDPR 第 45 条规定，仅当欧盟委员会认定某第三国或国际组织的数据保护水平足够充分时，才允许数据自由传输至该地区；而第 46 条则列出了在缺乏充分性决定情况下进行跨境传输的其他机制。我国《数据安全法》第 21 条、第 25 条和第 31 条分别规定了关于敏感数据的管理、出口管制以及关键信息基础设施运营者的数据出境安全管理方面的内容。其次，随着全球数据保护法律的不断演进，各国在数据管辖权方面的法律体系展现出显著差异，由此引发的法规冲突成为数据主权的重要表现之一。在 2007 年的一起网络诈骗案件中，比利时警方要求美国雅虎公司提供涉案邮箱的注册信息以协助调查。然而，雅虎援引美国《电子通信隐私法》的相关规定，拒绝共享该数据，理由是此类数据共享行为在美国法律下受到限制。这充分反映了不同国家在数据管辖权上的冲突以及跨境数据流动的法律挑战。类似的冲突也存在于欧盟与美国的数据保护法律之间，GDPR 对个人数据的跨境传输设有严格条件，要求数据接收方具备充分的数据保护水平，以保障欧盟公民的隐私，而美国的《云法案》（CLOUD Act）赋予政府在必要时获取存储于境外数据的权力。这种法律框架上的不对称性不仅反映了跨境数据流动中存在的治理分歧，还进一步凸显了国际法律体系在协调不同数据保护政策方面的局限性和不足。

然而，当前的国际贸易框架难以有效应对数据主权问题。以世界贸易组织（WTO）为代表的国际机构，尽管在推动贸易自由化方面取得了显著成就，但面对数字贸易和跨境数据流动等新兴领域，其规则体系则略显滞后[①]。具体而言，WTO 关于数据主权的规定较为笼统，难以协调各国在数据保护与隐私问题上的分歧，尤其针对上述两大问题时，缺乏有效的解决方案。鉴于当前 AI 技术对数据流动的高度依赖[②③④]，这种规则滞后不仅未能推动技术的自由流动，反而可能加剧全球数据保护政策的碎片化，进一步阻碍数字经济的健康发展。

① Aaronson S A, Leblond P. Another digital divide: The rise of data realms and its implications for the WTO[J]. Journal of International Economic Law, 2018, 21(2): 245-272.
② Chen M, Yang Z, Saad W, et al. A joint learning and communications framework for federated learning over wireless networks[J]. IEEE transactions on wireless communications, 2020, 20(1): 269-283.
③ Chen M, Gündüz D, Huang K, et al. Distributed learning in wireless networks: Recent progress and future challenges[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(12): 3579-3605.
④ Chen M, Challita U, Saad W, et al. Artificial neural networks-based machine learning for wireless networks: A tutorial[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3039-3071.

三、数据流动与隐私保护的平衡路径

（一）矛盾分析

数据自由流动与隐私保护之间的根本矛盾源于二者所追求目标的内在差异。数据自由流动的核心目的是通过跨境信息交换来促进技术创新，为高新技术产业（如人工智能、跨境电商等）提供支持。在当前的数字经济环境下，数据被视为重要的生产要素，其流动性直接影响技术研发的效率，甚至决定资源的全球配置和产业竞争力。相对而言，隐私保护则更加侧重于对个人数据的控制和管理，旨在确保数据在流动过程中不被滥用，符合合规要求，保护个人隐私和数据安全。这一矛盾的内在根源在于，数据自由流动要求尽量减少国家对数据流动的干预和限制，以确保数据能够快速且高效地跨越国界，进入需要的数据流动场景。而隐私保护则要求对数据流动实施严格的监管措施，特别是在涉及个人数据时，必须保证数据处理过程符合隐私保护的标准。这意味着，在隐私保护框架下，跨境数据流动往往需要满足严格的安全性、透明度和可控性要求，从而可能对数据流动进行限制，甚至产生对跨境数据流动的干预。

这种矛盾加剧了全球数据治理的复杂性。不同国家对隐私保护的理解、法律框架以及合规要求的差异，使得数据自由流动面临诸多法律和政策上的摩擦。各国数据保护政策的不一致性不仅影响了数据跨境顺畅流动，还可能导致全球数据治理体系的碎片化，进而限制数据共享的规模和效率。这种治理碎片化对跨国企业的运营和国际合作构成了障碍，削弱了全球数字经济的协同发展潜力。

（二）解决方案

尽管现有的国际贸易体系已经具备推动货物、服务与资本流动的规则框架，但针对跨境数据流动的多边贸易规则却尚未形成系统的规范。因此，如何在确保隐私保护与国家安全的基础上，推动跨境数据流动的自由化，已成为国际贸易法亟待解决的重要议题。

1.国际规范的评估标准

数据流动与隐私保护在不同国家的法律框架中存在显著差异，这种差异不仅源自各国对隐私的文化认知，还与其各自的法律框架及政策目标息息相关。为应对这一挑战，WTO 等多边贸易机制应当发挥引领作用，推动全球范围内跨境数据流动的国际规则制定，旨在构建统一的数据保护标准。欧盟 GDPR 中的“充分性决定”机制为解决这一问题提供了成熟的经验。所谓“充分性决定”是指欧盟委员会依据某一国家或地区的数据保护

水平评估其是否提供足够的隐私保护，从而决定是否允许欧盟个人数据在该地区自由流动。如果该地区符合欧盟要求，便会被授予“充分性决定”，从而使数据流动不再需要额外保障措施或复杂的合规程序。借鉴这一机制，国际组织如 WTO 和国际电信联盟（ITU）可以建立统一的跨境数据保护评估框架。该框架应对各国或地区的数据保护法律、隐私保护实践及技术措施进行综合评估，确保数据流动过程中的安全性与隐私保护标准能够得以统一。

然而，评估标准的制定在跨境数据流动的过程中至关重要，尤其是在技术层面的评估内容。这些技术性评估标准不仅应确保数据在跨境传输过程中免受未经授权的访问，还应避免对数据流动施加不必要的限制。因此，从技术角度构建一套全面、可操作的评估标准显得尤为重要。基于此，本文对数据传输领域的技术文献进行了调研，并选取了三个关键技术领域进行深入评估，分别是：数据加密、去标识化与匿名化、以及数据审计与合规性日志：

(1) **加密技术**：加密技术在保障跨境数据流动的安全性方面发挥着至关重要的作用。通过对数据进行加密处理，能够有效防止数据在传输和存储过程中遭遇恶意篡改或泄露。Kaaniche 等人（2017）[①]指出，采用符合国际标准的加密算法（如 AES-256）以及传输协议（如 SSL/TLS）能够显著提高数据安全性，并减少数据在传输过程中的截获风险。Schneier（2015）[②]也在其文章中进一步证实了，加密技术作为现代数据保护架构的核心，不仅能防范各类网络攻击与数据盗窃，还能有效保障数据流动过程中的隐私与安全性。在跨境数据流动的评估框架中，加密技术不仅是保护数据的基础手段，也是确保数据安全的核心措施。通过选用具有全球公认标准的、在有限时间内难以破解的加密技术，可以有效保护用户隐私，并避免因传输技术的不安全性而引发的额外数据流动限制。

(2) **去标识化与匿名化**：去标识化指通过技术手段去除或修改数据中的身份标识信息，使得数据无法直接或容易识别出特定个体的身份，而匿名化则是一种更加严格的去标识化形式，其目的是彻底移除一切可能与个体身份相关的信息，使

① Kaaniche N, Laurent M. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms[J]. Computer Communications, 2017, 111: 120-141.
② Schneier B. Data and goliath: The hidden battles to collect your data and control your world[M]. WW Norton & Company, 2015.

得数据无法再与任何特定的个体关联。Sweeney（2002）[①]指出，去标识化技术能够在不影响数据分析和应用的前提下，最大程度地减少个人身份信息的暴露，从而降低数据泄露时对数据主体的潜在风险。Narayanan 与 Shmatikov（2008）[②]进一步强调，去标识化与匿名化技术能够有效减少数据泄露时的身份识别风险，尤其在大规模数据处理的背景下，这些技术能够为跨境数据流动提供更高层次的隐私保护。尤其是在涉及敏感数据和大数据环境中，跨境数据流动的评估框架必须评估各国或地区是否实施了严格的去标识化与匿名化技术。这样，即便数据在传输过程中发生泄露，第三方也难以通过技术手段恢复出个人隐私数据，从而为数据保护提供了第二道防火墙。

(3) **数据审计与合规性日志**：该标准对于确保跨境数据流动的透明度和可追溯性十分关键。 Wang 等人（2009）[③]指出，审计跟踪系统通过记录数据在整个生命周期中的访问、修改和删除操作，能够确保数据处理过程的透明性和可验证性。审计日志不仅为数据处理提供了有效的监控手段，还能够在隐私泄露或数据滥用的情况下，为追溯责任方提供数据支持。合规性日志的记录能够帮助各国监管机构有效监督数据处理活动，确保数据处理方遵循隐私保护的相关法律法规，尤其是在发生数据泄露事件时，能够迅速采取相应的措施并追溯相关人员的责任。

2 跨国纠纷解决机制

随着全球数字贸易的不断扩展，数据流动所涉及的法律冲突和纠纷已成为不可避免的现象。由于各国在数据隐私保护方面的法律规定存在显著差异，跨境数据流动过程中频繁发生的法律冲突往往使企业和政府面临合规性困境。因此，建立一个有效的纠纷解决机制，确保在数据流动过程中发生法律争议时能够及时、公正地加以解决，已成为保障数据自由流动的重要前提。

首先，可以借鉴世界贸易组织（WTO）争端解决机制的模式，设立一个专门处理跨境数据流动法律纠纷的国际争端解决机构。该机构应当具有裁决跨境数据流动相关法律

① Sweeney L. k-anonymity: a model for protecting privacy'International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10, 5 (2002) 557-570[EB/OL].(2002)
② Narayanan A, Shmatikov V. Robust de-anonymization of large sparse datasets[C]//2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008: 111-125.
③ Wang C, Chow S S M, Wang Q, et al. Privacy-preserving public auditing for secure cloud storage[J]. IEEE transactions on computers, 2011, 62(2): 362-375.

问题的权力，并具备快速响应机制，以便在发生法律争议时能够及时采取应对措施。此类机构应确保通过公正的程序解决争端，特别是在面对合规性冲突时，能够提供迅速且有效的法律救济，从而消除对跨境数据流动的障碍。其次，鉴于数据流动涉及技术与法律两个层面的交织，纠纷解决机制应当结合技术审查与法律审查的双重审查机制。在技术审查方面，重点应放在评估数据传输过程中所采用的技术手段是否符合国际公认的安全标准。例如，应审查是否使用符合国际标准的加密算法（如 AES-256）、传输协议（如 SSL/TLS），以及数据保护技术（如去标识化与匿名化）是否符合全球隐私保护的最佳实践。这些技术措施的有效性是确保数据在跨境流动中得到充分保护的前提。与此同时，法律审查应从数据传输合同的角度入手，分析当事各方的权利与义务，并结合适用的国际法规对合同条款进行审查，确保各方在数据流动中的行为符合法律规定，尤其是在隐私保护、数据安全等方面的合规性。此外，纠纷解决机制必须具备高度的透明度与可追溯性。这一机制不仅需要确保争议处理过程的公开透明，还要为各方提供可追溯的法律依据与证据链条，从而增强各国对国际规则的信任与遵循。透明且可追溯的机制有助于确保全球数据流动过程中合规性的维持，防止不正当行为的发生，并保障数据主体的权益。当发生数据泄露或隐私侵权时，通过纠纷解决机制能够迅速追溯责任，确保当事方对其不当行为承担相应的法律责任。

3.其他

除了建立国际数据保护评估框架和跨国纠纷解决机制外，还可以考虑以下几种解决方案：第一，推动各国制定更加统一的数据保护法律和标准，尤其在跨境数据传输方面建立更为明确的规则。第二，鼓励企业采用数据保护技术的国际认证体系，确保跨境数据流动符合全球最佳实践。第三，加强国际合作，推动信息共享与风险预警机制的建设，提前识别潜在的法律和技术问题。最后，增设数据保护领域的国际仲裁机制，为企业提供灵活的争议解决途径。

四、总结

随着全球数字经济的蓬勃发展，跨境数据流动与隐私保护的平衡问题愈发突出。数据主权和隐私保护的法律分歧已成为国际贸易与技术合作的障碍，制约了 AI 技术的创新与全球化进程。本文深入探讨了数据流动的挑战与法律机制，并提出了构建国际数据保护评估框架、跨国纠纷解决机制以及推动法律统一等解决方案。这些措施为推动全球数据流动自由化、保障隐私安全提供了可行路径。展望未来，国际社会亟需加强合作，

建立更加完善的数字治理体系，推动数据流动与隐私保护的和谐共生。只有在保障国家安全与个人隐私的前提下，跨境数据流动才能为全球经济注入新的活力，推动人工智能等高新技术的快速发展。国际组织、企业与政府应携手共进，创新法规与技术，构建互信、透明、可持续的数据治理环境，共同迎接数字经济时代的挑战与机遇。

参 考 文 献

[1]. Mayer-Schönberger V, Cukier K. Big data: A revolution that will transform how we live, work, and think[M]. Houghton Mifflin Harcourt, 2013.

[2]. Voigt P, Von dem Bussche A. The eu general data protection regulation (gdpr)[J]. A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017, 10(3152676): 10-5555.

[3]. Brynjolfsson E, McAfee A. The second machine age: Work, progress, and prosperity in a time of brilliant technologies[M]. WW Norton & company, 2014.

[4]. Chander A, Lê U P. Data nationalism[J]. Emory LJ, 2014, 64: 677.

[5]. Meltzer J P. The I nternet, Cross‐Border Data Flows and International Trade[J]. Asia & the Pacific Policy Studies, 2015, 2(1): 90-102.

[6]. Aaronson S A, Leblond P. Another digital divide: The rise of data realms and its implications for the WTO[J]. Journal of International Economic Law, 2018, 21(2): 245-272.

[7]. Chen M, Yang Z, Saad W, et al. A joint learning and communications framework for federated learning over wireless networks[J]. IEEE transactions on wireless communications, 2020, 20(1): 269-283.

[8]. Chen M, Gündüz D, Huang K, et al. Distributed learning in wireless networks: Recent progress and future challenges[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(12): 3579-3605.

[9]. Chen M, Challita U, Saad W, et al. Artificial neural networks-based machine learning for wireless networks: A tutorial[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3039-3071.

[10]. Kaaniche N, Laurent M. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms[J]. Computer Communications, 2017, 111: 120-141.

[11]. Schneier B. Data and goliath: The hidden battles to collect your data and control your world[M]. WW Norton & Company, 2015.

[12]. Sweeney L. k-anonymity: a model for protecting privacy'International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10, 5 (2002) 557-570[EB/OL].(2002)

[13]. Narayanan A, Shmatikov V. Robust de-anonymization of large sparse datasets[C]//2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008: 111-125.

[14]. Wang C, Chow S S M, Wang Q, et al. Privacy-preserving public auditing for secure cloud storage[J]. IEEE transactions on computers, 2011, 62(2): 362-375.

致　谢

本文的完成，离不开赵晶晶老师《国际贸易法》课程的指导与启发，这门课程为我打开了理解全球贸易规则与法律框架的大门，使我得以全面把握国际贸易中的重要法律制度与实践应用。赵老师以其扎实的学术功底和严谨的教学态度，深入浅出地将复杂的国际贸易法理论与实际案例相结合，使我能够更清晰地理解跨国贸易中的法律问题与解决路径赵老师的教诲让我在国际贸易法的研究道路上获得了更多的视角与思考的深度，为本文的选题与写作奠定了坚实的基础。赵老师不仅激发了我对国际贸易法领域的浓厚兴趣，也让我在理论学习与实际操作的结合中获益匪浅。在此，我谨向赵老师表达我最诚挚的感谢！