对接 CPTPP 数字贸易规则的跨境数据流动及中国因应法律检索报告

余纪萱 22102096

目录

一、引言

当今世界全球化和数字化的步伐仍在进一步加快，数据已经成为了贸易中不可或缺的一部分，数据对于各个国家来说就是国家实力较量的重要武器，企业或者国家可以通过数据来分析其他公司或者国家的人员结构，国民的消费偏好，当地的经济水平等私密或者机密信息，并且有针对性地做出应对措施。正因数据的跨境传输造成的一些个人隐私以及国家机密的外漏，社会公众已经开始担心个人、企业数据安全和国家数据安全问题。FTA 等纷纷出台的数字贸易规则，对数据跨境流动进行了符合自身利益的规制，由于 2021 年 9 月 16 日，中国正式申请加入 CPTPP，商务部新闻发言人高峰表示，中方已经就 CPTPP 协定内容进行了充分、全面和深入的研究评估。

CPTPP 新架构基本保留了原 TPP 的内容，其在市场准入、贸易便利化、电子商务和服务贸易等方面均无任何差异。跨境数据流动是数字贸易的前提，因此跨境数据流动政策深刻影响全球数字贸易与数字经济。CPTPP 的跨境数据流动规则已然成为新一代的数字贸易范本，会影响到中国在全球的双边或多边贸易，因此需要比较中国的数据流动规则是否符合 CPTPP 数字贸易规则下跨境数据流动的规则以及中国如何通过自身的努力去适应 CPTPP 规则以及全球的数据跨境流动。

由于 CPTPP 是众多经贸协定中的一个，并且其前身是美国主导的 TPP，CPTPP 并没有相关援引的司法判例，因此，需要从跨境数据流动的角度去检索欧美这些主要国家和地区的跨境数据流动政策及趋势，进而反观 CPTPP 对待跨境数据流动的态度，预测未来趋势，本篇数据检索报告的思路就是从中国的法律法规、案例以及相关文献出发，探究中国对数据跨境流动的态度，对比国外相应数据处理的规则以及实践，可以发现中国与国外在数据立法以及判例方面的异同，找到冲突点，在了解到世界主要国家地区的跨境数据流动政策以及这些国家地区如何协调与贸易协定的数据跨境流动的关系的基础上，最终落脚到中国如何借鉴这些不同的经验来修改国内的法律法规来缩小差距以更好地对接 CPTPP 数字贸易规则下的跨境数据流动政策，更快地推动中国加入 CPTPP。

二、中文检索部分

（一）法律及部门规章

由于在我国数字立法中，并没有专门“数据跨境流动”，而是以“数据出境/入境”来代替，数字在我国也有多种表述以及细分，如“数据”“信息”。因此笔者在“北大法宝”中，以“数据”、“数字”、“网络”、“个人信息”、“个人数据”、“企业数据”、“数据出境”、“数据入境”等为关键词进行标题以及全文检索，在 300 余条法律法规中经过相关性筛选，获得的结果如下：

1、法律

我国数字立法中，相关的法律有三大上位法，笔者摘取与数据跨境流动相关的部分条款：

（1）《中华人民共和国数据安全法》

第三十一条　关键信息基础设施的运营者在中华人民共和国境内运营中收集

和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

(2)《中华人民共和国网络安全法》

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

(3)《中华人民共和国个人信息保护法》

第三章 个人信息跨境提供的规则

2、部门规章

(1)《数据出境安全评估办法》：第三、四、五、六、八、九、十二、十四、十七、二十条都规定数据出境过程中应当遵守的制度。

(2)《网络安全审查办法》

第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

（五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

(3)《汽车数据安全管理若干规定》：第十一、十二、十四条规定了汽车行业的重要数据、未列入重要数据的个人信息数据出境等的具体要求。

(4)《个人信息出境标准合同办法》(尚未生效)

(5)《工业和信息化领域数据安全管理办法(试行)》第二章涉及数据的分类分级管理，在划分工业数据的基础上对数据处理以及对外提供提出要求。

第二十一条 工业和信息化领域数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据，法律、行政法规有境内存储要求的，应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。

工业和信息化部根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国工业、电信、无线电执法机构关于提供工业和信息化领域数据的请求。非经工业和信息化部批准，工业和信息化领域数据处理者不得向外国工业、电信、无线电执法机构提供存储于中华人民共和国境内的工业和信息化领域数据。

第三十一条 工业和信息化部制定行业数据安全评估管理制度，开展评估机构管理工作。制定行业数据安全评估规范，指导评估机构开展数据安全风险评估、出境安全评估等工作。

(6)《数字经济对外投资合作工作指引》

（十）做好数字经济走出去风险防范。鼓励数字经济企业完善内部合规制度，严格落实我国法律法规有关数据出境安全管理的规定，遵守东道国法律法规及国际通行规则，妥善应对数字经济领域审查和监管措施。提高知识产权保护意识，健全数据安全管理制度，采取必要技术措施，保护数据安全和个人信息，支持企业通过法律手段维权。密切跟踪全球数字经济反垄断及加征数字税最新政策动向，做好应对准备。

（7）《互联网个人信息安全保护指南》

5.3.1　云计算安全扩展要求

a）应确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定；

个人信息的保存行为应满足以下要求：

6.2　保存

a）在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定；

（二）案例

笔者在北大法宝全文检索以下“数字”“数据”“网络”“个人信息”四个关键词并选择涉外专题，共有 25 个案例，发现多为诈骗以及知识产权侵权的案件，继续选择个人信息保护专题，共有 2 个案例，一则为名誉侵权，一则为合同纠纷，并未涉及到真正关于跨境数据的案例。在无讼中以相同关键词进行检索也并未搜到相关案例，经过思考一是因为本文写作是国际法的内容，数据跨境流动在国内并没有相应的判决，二是中国关于数据跨境的上位法还在进行建构。笔者在微信公众号中进行搜索，搜索到的也是国内企业在境外因违反当地的数据跨境流动规则而受到处罚的案例。因此，笔者转化检索思路，由于本文写的是中国如何对接跨境数据流动规则，国内司法案例的检索，应当以国内数据法律法规进行检索，以中国对数据的态度与 CPTPP 进行对比，进而探求对接路径。因此检索中国的法律最后在北大法宝司法案例中全文检索关键词“个人信息保护法”或“数据安全法”或“网络安全法”，选择“典型案例”，共有 39 则案例，从中筛选出 5 则相关度较高的案例。且这五个案例可以大致分为两类，第一类（前三个案例）为用户和网络平台企业之间的纠纷；第二类（后两个案例）为网络平台企业之间的纠纷。

案例一：广东省深圳市中级人民法院发布 2021 年度数字经济知识产权十件创新案例之四：王某某与腾讯公司个人信息保护纠纷案

【法宝引证码】CLI.C.414968160

在案件中，在原告王某某没有同意的情况下，被告微视 APP 仍然显示其微信好友浏览信息。

深圳市中级人民法院二审认为，划入隐私的个人信息重在其“不愿为他人知晓”的“私密性”，王某某“微信好友关系” 以及真实的“地区、性别”，信息已在微信中相同范围公布，对前述信息不具有隐私期待故不属于隐私，但属于受

法律保护的个人信息。微视强制获取用户地区、性别信息违反了必要性原则，未经授权继续使用原告微信好友关系违反正当性原则。

该案件为全国首例适用《个人信息保护法》的案例，要旨在于互联网平台收集个人信息的范围和限度。本案提出了关于互联网平台对个人信息的法律定义标准以及合规原则，对合法性、必要性、正当性结合该案件详细说明了相关适用评判标准。这为规范互联网平台和 APP 服务商在用户数据收集和使用方面提供了司法审查的渠道，对于促进数字经济健康有序发展具有积极作用，也可以更好地去对接更严格的国际数据法案，与国际上的告知-同意规则相一致。

案例二：上海市嘉定区人民法院发布 10 个数字经济司法研究及实践（嘉定）基地首批典型案例之二：蔡某某诉上海某电子商务有限公司网络购物合同纠纷案——电子商务平台经营者处理个人信息合法性基础的认定

【法宝引证码】CLI.C.500911005

该案案情主要为：被告上海某电子商务有限公司运营的 B2C 电商平台 1 号店在《服务协议及隐私声明》规定每位用户仅限使用一个 1 号店账户，告蔡某某同意该条款后注册成功，通过多个与 1 号店关联的账户、设备、IP 地址下单购买商品，订单收货人、联系电话、送货地址大多指向原告本人，再次下单时其订单被系统判定为“异常订单或经销商订单”，遂被系统取消并隐藏。法院认为被告收集、处理客户账户、设备地址、联系电话、送货地址等信息，系履行合同所需，事先已征得客户同意，亦未超过约定的判断是否“因生活消费购买商品或服务”之用途目的。

本案在个人信息处理合法性的判断，私人利益需要告知同意，而公益性的只需要告知，保障知情权，且不超出目的，处理个人信息行为的合法性，需结合具体场景进行判断的同时也需要符合《个人信息保护法》的规定。该案例多次强调“合法、正当、必要”原则，由于数字经济的发展，告知-同意规则在平台和用户之间大多通过格式条款来进行，在国际上，跨境数据流动主要是通过 SCC 条款来进行约定，这就需要在国内立法的过程中修改相应的 SCC 规定，以更好地使国内和国际的数据传输水平相一致。

案例三：最高人民检察院发布 8 件个人信息保护检察公益诉讼典型案例之四：江西省宜春市人民检察院督促保护医疗健康个人信息行政公益诉讼案

【法宝引证码】CLI.C.504133552

部分保险代理机构业务人员在推销保险产品过程中，通过合作医院违法获取大量患者的姓名、手术类型、联系电话等医疗健康信息，对相关患者进行保险推销，宜春市检察院审查认为，根据《中华人民共和国个人信息保护法》、《医疗机构病历管理规定》等法律法规，医疗健康等信息属于敏感个人信息。未经公民本人同意，或未具备具有法律授权等个人信息保护法规定的理由，医院向保险代理机构提供患者医疗健康信息，改变了公民公开个人信息的范围、目的和用途，不属于法律规定的合理处理；保险从业人员收集、使用获取的医疗健康信息从事保险营销违反国家规定，侵害了不特定多数患者个人信息权利。

典型案例也是个人信息保护的示范，医疗机构违反法律规定的合法、正当、必要和诚信的原则，未经患者同意向保险代理机构提供相关个人信息，严重侵害

公民个人信息安全和合法权益，扰乱了社会公共秩序。运用了个人信息保护法对敏感信息进行保护，彰显了我国对个人信息此类数据安全的重视。

案例四：杭州互联网法院 2020 年度知识产权司法保护十大案例之一：深圳市腾讯计算机系统有限公司等诉浙江搜道网络技术有限公司等不正当竞争纠纷案——数据权益的权属判断与分类保护

【法宝引证码】CLI.C.318023236

该案件案情主要为：深圳市腾讯计算机系统有限公司和腾讯科技（深圳）有限公司（合称“两原告”）开发的个人微信产品是提供即时社交通讯服务的应用程序，主要包含个人微信用户的用户账号数据、好友关系链数据、用户操作数据等个人身份和行为数据。浙江搜道网络技术有限公司和杭州聚客通科技有限公司（合称“两被告”）开发的“聚客通群控软件”利用 Xposed 外挂技术将该软件中的“个人号”功能模块嵌套于个人微信产品中运行，为购买该软件服务的微信用户在个人微信平台中开展商业营销、商业管理活动提供帮助。两原告认为被告未经授权获取、使用涉案数据，侵犯了其对微信平台数据的权益，并构成不正当竞争。两被告则辩称，涉案数据属于微信用户的信息且归用户自己所有，并不存在数据权益的问题；同时，被告所开发的软件增强了微信平台的电商营销管理功能和用户服务效率，是一种创新性的竞争行为，不应被认定为不正当竞争。

法院认为网络平台方对于数据资源整体与单一原始数据个体所享有的是不同的数据权益，原告对前者应当享有竞争权益，对后者，依其与用户的约定享有原始数据的有限使用权，使用他人控制的单一原始数据只要不违反“合法、必要、征得用户同意”原则，一般不应被认定为侵权行为。两被告擅自将该部分并不知情的微信用户的数据移作自己存储或使用，违反了《网络安全法》的相关规定，构成了对微信用户信息权益的侵害。

该案件是首例微信数据权益认定的案件，申卫星教授认为该判决明确指出尽管数据是源于用户，但单一的数据和通过技术资本劳动力的投入汇聚而形成的数据的整体是不同的。法官在判决里创造性地使用了因此而形成一个竞争性的财产权益，承认了该利益要受法律保护。

此类案例可以为此类数据的所有权、用益权进行明确，并推动相关立法。为中国对接 CPTPP 数字跨境流动提供借鉴。

案例五：广州知识产权法院发布 2021 年度知识产权司法保护十大典型案例之五：深圳市腾讯计算机系统有限公司与杭州祺韵网络技术有限公司、广州优视网络科技有限公司著作权侵权及不正当竞争纠纷案——强化数据安全与保护 促进新技术发展运用

【法宝引证码】CLI.C.411353101

被告一祺韵公司擅自在“5G 芝麻”云游戏平台预装原告腾讯公司的网络游戏，被告二优视公司提供“5G 芝麻”APP 的下载和分发服务，原告认为其构成帮助侵权。

广州互联网法院经审理认为，在侵犯著作权方面祺韵公司成立侵权，但优视公司不构成帮助侵权。在不正当竞争方面，用户数据属于原始数据，腾讯公司是

经过授权才拥有收集的权利，祺韵公司运营的 5G 芝麻平台在收集游戏用户的账号及游戏相关数据时，同样获得了游戏用户的授权，且没有破坏腾讯公司的技术保护措施，并非违法取得，因此不构成不正当竞争。

虽然本案判决依据的是《反不正当竞争法》和《著作权法》，但是在判断数据权属以及数据处理行为的合法性给了指引，为我国《数据安全法》的完善提供了方向。

初步总结:

以上五个案例中，两个属于知识产权方面的纠纷，另外三个涉及的是个人信息合法性的处理。由于并没有一个系统完整的数据法来作为判案的依据，实务中多是用个人信息保护法、知识产权相关的法条、商业秘密、反不正当竞争法等法律来进行判决，在网络平台企业之间大多使用的是知识产权相关的法律以及反不正当竞争法；而在个人用户与网络平台企业则用的都是个人信息保护法。但其实个人信息作为数据的最初来源，以上这五个案例都涉及到了个人信息，每个单一原始个人数据构成了整个数据领域的底层，在此基础上对数据的处理利用，最终形成数据整体资源，在个人信息保护方面，法院无不例外提出三个原则，即“合法、正当、必要”，并结合案件对每一个原则进行了阐释，但是并未涉及个人数据、企业平台形成的数据等分类，需要对这些数据进行区分，除了以上的健康数据等敏感个人数据和隐私之外，还有地理地图数据等与地理以及自然资源相关的数据，也要对其进行分类。最后涉及到的就是分类分级管理，在分级分类需要有一个前提就是确定数据的权属问题，解决了这个问题之后法院可以将以上的案例运用数据相关的法律来进行判决，也能更好地与 CPTPP 电子商务章节进行对接。为了更清晰地展现中国的数据法律法规现阶段的进展，还需要对比国外的相关案例。

（三）专著

笔者在独秀上检索以“CPTPP”和“数据跨境流动”为关键词进行全部字段检索。经过筛选，整理出 3 本关联性较高的专著，但是在收集专著的时候并没有找到相应的图书电子资源：从立先的《TPP CPTPP 知识产权问题研究》，黄洁的《中国应对<全面与进步跨太平洋伙伴关系协定>电子商务和数字贸易运行规则的研究》，张国军的《亚太区域经济合作机制:变迁、战略博弈与对策》，但并没有相应的内容以供参考，继续通过 CALIS 以及 Cashl 进行检索，未看到直接相关的书籍，且大部分书籍未提供在线预览和下载的路径。从论文的脚注中也未发现比较集中讨论这一问题的书籍，仅有一些法律评注以及法学教科书中有所涉及，因此笔者目前只找到三本相关的著作。

1、朱琳. 大数据时代跨境数据流动治理研究[M]. 苏州：苏州大学出版社, 2022.06

朱琳在书中对跨境数据流动进行概念界定、对数据进行分类。并将我国的数字立法通过《网络安全法》《数字安全法》为两个节点，将我国的数据流动立法分为 1.0、2.0 和 3.0 时代。并对境内外的立法实践和我国地方的探索进行分析总结。朱琳对我国数据跨境流动的治理现状，通过不同的法律法规进行分类解读，以便于更好的与境外的跨境数据流动政策进行对比。作者认为中国的数据跨境流动政策与 CPTPP 还有很大的差异，需要完善国内的相应立法，比如建立健全数

据出境安全评估机制、开展分级分类等，在此基础上加入 CPTPP 等国际协定，推动数据跨境安全有序流动。

2、张丽，孙菲阳 跨境数据流动：全球治理趋势与我国规制策略 电子工业出版社 2022.04

作者认为如何平衡数据跨境流动产生的经济红利与数据保护之间的矛盾是跨境数据流动法律规制的重要议题。从国际法的角度来看，我国关于跨境数据流动的法律规制是独立于“欧美模式”之外的第三种模式，总结出我国跨境数据流动法律规制具有“将维护国家数据安全与数据主权放在首位”的特点，比并提出我国要重视安全的同时也要注重自由，完善数据本地化规则、数据出境安全评估机制，建立分级分类的管理机制。

3、梅宏 数据治理之论 中国人民大学出版社 2020.07

作者认为数字治理面临着很多问题，系统化的数据治理框架尚未形成，开放共享、安全与隐私保护、质量评估、价值预测等关键技术远未成熟。如何构建联动的治理技术体系、如何建立良好的数据共享开放环境、如何建立有效的数据管理体制机制和层级化的数据安全隐私与保护屏障，以及如何建立体系化系统标准规范等都值得探讨。其中第六章为法学视角下的数据治理，认为在个人信息保护法方面，我国未来可能采取的模式会更接近于欧盟，分析了著作权法、商业秘密法、反不正当竞争法对企业数据权属的保护，认为未来设立数据集合有限排他权。并且作者认为数据跨境流通的安全问题是数据安全问题中的一个很重要的方面，不同国家的跨境数据流动模式不是绝对的，应该根据不同类型的数据选择不同的跨境书流通规制模式。

以上著作的观点都比较一致，认为中国应当尽快做到数据的确权以及完善数据治理方面的法律体系，特别是最后一本书总提到的“设立数据集合有限排他权”与之前在王利明教授的讲座中提到的“权利束”观点相一致，也与我国出台的“数据二十条”中的观点相一致。以上著作对中国跨境数据流动模式的认定和预测为我国对比 CPTPP 并发现其差异给了指引。

（四）论文

中文期刊论文笔者主要从中国知网检索关键词“CPTPP”、“数据跨境流动”等，并结合脚注中关联性较大的内容对文献进行补充，对比中国数据法律法规与 CPTPP 数字贸易规则中的跨境数据流动政策的异同，从数十篇论文中挑选出比较具有典型性的论文：

阅读相关论文之后可以发现主要观点可以分为两类，一种观点认为中国的跨境数据流动制度总体符合 CPTPP 规则（第一篇论文），另一种观点认为两者之间有多方面差异，后者占了大多数。

1、 徐程锦.中国跨境数据流动规制体系的 CPTPP 合规性研究[J].国际经贸探索,2023,39(02):69-87

徐程锦认为中国法律中虽然没有“跨境数据流动”的概念，但从语义上看，数据 “出境”和 “向境外提供”应无本质区别。接着从中国国内法如何规制跨境数据流动及其限制措施，并将其放在 CPTPP 框架下进行合规性分析，认为由

于有基本安全例外保护，要求此类可能属于国家核心数据使用境内服务器的措施不违反 CPTPP 规则。限制数据跨境流动的措施不违反 CPTPP 第 14.11 条第二款，数据出境安全评估满足 CPTPP 的例外规定。最终得出除数据跨境安全网关对部分外国网站的整体屏蔽外，中国的跨境数据流动规制体系可以满足 CPTPP 第 14 章的规则要求的结论，并对完善相关国内法以及加入 CPTPP 给出建议。

2、 孙南翔.CPTPP 数字贸易规则:制度博弈、规范差异与中国因应[J].学术论坛,2022,45(05):44-53

孙南翔通过对比欧美数字贸易规则，探究数字经济国际规则的发展动向，认为 CPTPP 数字贸易规则成为主要经济体可能共同接受的规则样本，对比 CPTPP 数字经济规则与我国法律制度的规范差异后认为 CPTPP 数字贸易规则在数据跨境流动、计算设施本地化、源代码规则、数据内容流动等层面与我国相关法律制度存在一定程度的不一致性，并提出中国加入 CPTPP 的对接策略。

3、何波.中国参与数据跨境流动国际规则的挑战与因应[J].行政法学研究,2022(04):89-103.

何波从多边贸易规则出发，发现中国国内数据跨境流动政策的不足之处，分析认为中国对数据跨境流动采取限制措施的目的恐难以满足 CPTPP 中“合法公共政策目标”的必要性要求，需要在数据分级分类管理的基础上，采取更加精细化的数据出境管理政策，以期符合 CPTPP“合法公共政策目标”的必要性要求。

4、马光.FTA 数据跨境流动规制的三种例外选择适用[J].政法论坛,2021,39(05):14-24.

马光在对比 FTA 文本并总结三种例外后认为中国与的法律不论是在内部法律之间还是在与条约的对接上都有不协调的问题，CPTPP 中一般例外和国家安全例外条款会对我国具有很好的启发借鉴作用，或许能达成数据跨境自由流动和国家安全利益的平衡。

（五）台湾文献

虽然我国反对台湾单独申请加入 CPTPP，但是可以通过台湾学者对中国大陆加入 CPTPP 的看法了解中国在加入 CPTPP 遇到的困难以及改进办法，因此，笔者在月旦知识库中检索关键词“CPTPP”以及“数据跨境流动”筛选出以下论文:

1、探討台灣申請 CPTPP 入會的若干問題 謝正一 華人經濟研究 202109 19 卷 2 期 25-32

作者认为 CPTPP 的入会要求，大陆是做不到的，CPTPP 是高度开放的贸易规则，在跨境数据流动方面，服务器的开放会是非常大的挑战。

2、中國大陸為加入 CPTPP 進行法規調適的初步觀察 吳子涵 經濟前瞻 202209 203

作者将中国大陆加入 CPTPP 面临的制度挑战分为 3 类，认为中国大陆的改革方向以及现在的能力来看与 CPTPP 的差距越来越小，但在电子商务方面仍然存在差距，未明确争端的解决方式，CPTPP 高度保障资料跨境流动，但是中国大

陆却禁止非国家公用的电脑资讯网路直接进行国际联网，同时对互联网内容进行过滤监控;《网路安全法》亦以国家安全为由，允许对来自境外的特定资讯采取技术措施和其他必要措施阻断传播。面对上述法制方面的落差，目前中国大陆主要采取两大方式因应。一是积极运用已签署的经贸协定，作为和国际标准调和的管道;二是进一步加快国内改革与试点步伐，从根本改善国内法规的内涵与做法。同时还建立自贸区，如海南自贸港，对接 CPTPP 的数字贸易规则。作者认为都有利于中国加入 CPTPP。

上述两个台湾学者的观点也有所不同，谢正一认为中国与 CPTPP 的存在着很大的差异，到那时吴子涵则认为仅是在电子商务方面存在差距，并且已经有相应的有利措施。

由于数据跨境流动中的自由流动与数据主权有着天然的联系，除以上关于数据跨境流动政策之外，笔者也对相关概念，如“数据主权”“数字主权”“网络主权”等为关键词进行检索，也可以发现学者对数据是否能够成为主权有所争议，部分结果如下：

1、黄海瑛,何梦婷,冉从敬.数据主权安全风险的国际治理体系与我国路径研究[J].图书与情报,2021(04):15-28.

黄海瑛等人认为，在性质上，数据主权属于国家主权的下属权力，继承了国家主权相应属性。数据主权包括数据管理权和数据控制权。

2、谢卓君,杨署东.全球治理中的跨境数据流动规制与中国参与——基于 WTO、CPTPP 和 RCEP 的比较分析[J].国际观察,2021(05):98-126.

谢卓君、杨署东对 WTO、CPTPP 和 RCEP 进行分别的比较分析，认为数据主权具有双重属性，因为它既可以视为领土主权在数据领域的延伸，也可以视为数据世界的独立主权。

3、 陈曦笛.法律视角下数据主权的理念解构与理性重构[J/OL].中国流通经济:1-11[2022-05-23]

陈曦笛与以上学者持相反意见，把国家主权和网络空间主权做对比，认为“只有能够容纳现实或虚拟活动开展的领域，方能构成适格的国家主权客体”，“数据是经过整理和分析的信息之集合，本质上属于宽泛意义上的物”，“借助地域或国籍等国家管辖联结点，主权国家就能依靠领土主权和网络空间主权有效赋予数据管辖合法性”，因此没有必要为数据视为新型主权，数据主权是对主权概念的过度延伸。

由此可见，黄海瑛以及谢卓君等人认为可以单独设立数据主权，是国家主权的一种，但是陈曦笛则认为不需要单独设立数据主权的概念，在国际法上对此概念也颇有争议。

在了解了中国数据法律关于数字贸易规则下跨境数据流动的规定以及法院、学者对数据持有的态度以及相关概念的解析之后，进行比较法的研究，对比就会比较清晰。

三、比较法检索部分

（一）法律法规及国际条约

首先，由于 CPTPP 是 TPP 的前身，TPP 为美国主导，并且 CPTPP 延续了 TPP 大部分的规定，其次中国与美国关于数据跨境流动政策以及数据主权的态度差异较大，最后，美国是中国数字贸易的主要国家之一。因此，在比较法方面主要检索美国的相关法律法规以及案例法律及其他规范性文件。欧盟作为跨境数据流动立法的主要地区之一，对数据流动的探索较早且更成熟，体现了明显的区域色彩。由于篇幅限制，国际法律资源部分仅从美国法、欧盟法、CPTPP 以及部分 FTA 来进行检索。首先，谷歌学术上直接检索需要的 CPTPP，然后，笔者通过 Westlaw 的 regulation 中检索 data/digital transfer/transmission 得到的法律法规关联性不强，接着在 lexis 的 status and regulations 中检索 data/digital transfer/transmission ，International Data Transfers，trans-border data flows。得到的相关法律法规有上万条，因此，笔者通过微信公众号去搜索相关的限缩单词，再去 westlaw 和 lexis 中检索相关的法律。最后，用北大法宝的境外法律信息资源指引进行检索，检查是否有遗漏，得到以下法律法规和条约：

1、Comprehensive and Progressive Agreement for Trans-Pacific Partnership（CPTPP）/全面与进步跨太平洋伙伴关系协定

主要集中在第 14 章 电子商务章节 CHAPTER 14 ELECTRONIC COMMERCE，涉及数据跨境流动的主要有：

14.1 定义中关于数字产品、电子传输或通过电子方式传输以及个人信息的定义：

digital product means a computer programme, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically；

electronic transmission or transmitted electronically means a transmission made using any electromagnetic means, including by photonic means；

personal information means any information, including data, about an identified or identifiable natural person。

14.11 通过电子方式跨境传输信息

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure：

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction

on trade; and

(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

说明了跨境数据传输各国都有不同的规定，并解释了合法公共目标

14.13 计算时设施的位置 Location of Computing Facilities

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

在本条除了规定了合法公共政策之外，最重要的一点就是规定了任何缔约方不得要求一涵盖的人在该缔约方领土内将使用 或设置计算设施作为在其领土内开展业务的条件。

14.17 源代码 Source Code

1. No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.

2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.

3. Nothing in this Article shall preclude:

(a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or

(b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.

同样，该条文规定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。

美国对待数据跨境流动大多体现在双边、多边协议中。

2、《澄清海外合法使用数据法》(Cloud act) 该法案旨在提高执法过程中获取跨国界存储数据的能力

法案规定：电子通信服务或远程计算服务的提供者（“服务供应商”）应当遵守法案规定的义务，保存、备份和披露有线和电子通信的内容以及拥有、监管或控制的与其用户或订户的相关的任何记录或其他信息，无论此类通信、记录或其他信息位于美国境内或是境外。作为例外或限定性规定，法案给予服务供应商在14 天内提出撤销或变更（获取数据）法律程序的动议的权利，理由可以是：(1) 目标对象不是“美国人”且不在美国境内居住；(2) 所要求的披露将会使服务供应商陷入违反适格外国政府法律的实质性风险。法案进一步规定了政府可以对服务提供者的申请作出回应，除了判断是不是美国人和对外国法律的违反外，法院可以综合考虑政府对“个案情形”的阐释，决定最终是否对法律程序作出改变或撤销。特别是美国利益 (the interests of the United States)、适格外国政府 (qualifying foreign government) 对于保护禁披露信息的利益等 7 项依据，以及寻求使用其他替代性手段并能及时有效获取所需披露信息的可能性等。也即，如果法院经过制衡决定优先考虑美国利益等因素，服务提供商也需提供境外数据，即使是外国人或与外国法律存在冲突。

§ 2713. Required preservation and disclosure of communications and records

“A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.”.

“电子通信服务或远程计算服务的提供商应遵守本章的义务，以保存、备份或披露有线或电子通信的内容以及该提供商拥有的与客户或订户有关的任何记录或其他信息、保管或控制，无论此类通信、记录或其他信息位于美国境内还是境外。”

3、《美国出口管理条例》(EAR) 对部分关键技术与特定领域的数据出口进行限制

根据 EAR 第 734.3 节的规定，受 EAR 管制物项包括：(1) 所有在美国境内的物项（包括商品、技术和软件，下同），包括经过美国转运的物项；(2) 所有美国原产物项（无论位于何地，已出口到外国的也不例外）；(3) 外国商品集成了受管制的美国原产商品，外国商品“捆绑”了受管制的美国原产软件，外国软件“参杂”了受管制的美国原产软件，以及外国技术“参杂”了受管制的美国原产技术，对于第 734.4(a)节所述的受管制美国原产物项而言（以高性能计算机组件为代表）为任何比例（0%），对于第 734.4(c)和 734.4(d)节所述的受管制美国原产物项而言比例分别为超过 10%（适用于古巴、伊朗、朝鲜、苏丹和叙利亚）和超过 25%，以价值计算美国原产成分占比（见表 1）；(4) 利用美国原产技术或软件直接生产而来的某些外国商品（具体范围依照第 736.2(b)(3)节而定）；(5) 由利用美国原产技术或软件建设的、美国境外的工厂或其主要设备生产的某些外国商品（具体范围依照第 736.2(b)(3)节而定）。

4、《美墨加协定》(USMCA)

其中第 19 章数字贸易章节，与 CPTPP 类似。围绕着进一步推动跨境数据流动的自由化展开，充分反映了美国在跨境数据流动上的几点核心主张：(1)免征关税；(2)非歧视；(3)隐私保护方面参照 APEC 的《隐私保护框架》和 OECD 的《理事会关于隐私保护和跨境数据流动指南建议(2013 年)》；(4) 除非为了公共政策目标(public policy objective)，不得禁止和限制以电子手段进行的跨境信息传输；(5)不得要求计算设施设置在本地；(6) 在数字安全方面尽力采取基于风险的方式，而不是一概性的规定；(7)不得对另一国的个体以允许在本地经营为条件强制要求提供、转让或接入其持有的软件的源代码；(8)不应在判定损害责任时将交互计算机服务（ interactive computer service) 视同信息内容提供者；(9)尽力促进政府持有数据的公开。

5、《外国投资风险审查现代化法》

（一）CFIUS 的管辖范围

CFIUS 拥有并保留审查外国人或可能导致外国人控制美国企业交易的管辖权，从而识别和解决因交易而产生的国家安全风险。

其中：2、涉及关键技术、关键基础设施和美国公民个人数据的其他投资。FIRRMA 向 CFIUS 提供明确的管辖权，以便其审查外国人对美国企业与关键基础设施或关键技术相关、或是能维护或收集美国公民个人数据的任何其他投资。其他投资只要符合以下条件，即使是非控制性的，也需要接受审查：在涉及关键基础设施、关键技术或敏感个人数据的企业中，给予外国人以在收购美国企业方面的重大非公开技术信息获取权，或者董事会成员资格，或者其他除通过股份投票之外的实质性决策权。

3、外国投资者权利变化导致受外国人控制的美国企业或其他投资。FIRRMA 对受管辖交易的定义还包括任何会导致外国人对其投资的美国企业所享有的权利产生变动的投资，只要这种变动会导致外国人控制该企业，或者这种变动构成对涉及关键基础设施、关键科技、美国公民个人数据的企业的投资。

6、《国家安全和个人数据保护法案》(NSPDPA)

虽然还未生效，但是已经通过了美国参众两院的通过。其中的 NSPDPA SEC.3 对科技公诉提出了六项数据安全要求：

（1）数据收集最小化。相关科技公司只能收集其网站、服务、应用程序运营所必须的数据，不得收集更多的用户数据；

（2）禁止二次利用。相关科技公司不得将根据第（1）款收集的任何用户数据用于网站、服务、应用程序运营以外的其他途径，包括提供定向广告、非必要地与第三方共享或非必要地用于人脸识别技术；

（3）个人享有查看和删除数据的权利。相关科技公司应允许个人查看公司持有的该个人的相关数据，并根据该个人的要求永久地删除公司持有的、直接或间接收集的任何用户数据；

（4）禁止向相关国家传输数据。相关科技公司不能向相关国家传输（包括通过

非相关国家的第三国简介传输）用户数据或用于解密用户数据的信息（如加密秘钥）；

（5）数据储存要求。相关科技公司不得将所收集的美国公民或居民的数据或用于解密用户数据的信息储存在美国或与美国有相关协议、通过法律规定的程序共享数据的国家之外的服务器或数据储存设备上；

（6）报告要求。相关科技公司的 CEO 或同等级别高管应当以至少每年向联邦贸易委员会等有关部门提交一份报告以证明公司符合上述要求

总结以上法案可以看出，美国虽然强调数据跨境流动，凭借其长臂管辖，影响其他国家的数据跨境流动，并非在一个平等自由的环境下进行跨境数据的流动。

7、欧盟的《通用数据保护条例》(GDPR)

主要规定了 GDPR 的地域适用范围、个人敏感数据、数据主体的权利（知情权、访问权、更正权、可携权、删除权、限制处理权、反对权和自动化个人决策相关权利）、数据处理者、数据泄露和通知以及设立数据保护官。由于条文过多，就不一一例举。

8、欧盟《数据法案(Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data)》草案

该草案涉及数据共享、公共机构访问、国际数据传输、云转换和互操作性等方面规定，重点规制了非个人数据向第三国司法或行政当局的跨境传输，具有较多数据主权意义上的考量，但针对非向第三国司法或行政当局进行的数据传输。

（二）案例

笔者首先通过 westlaw 高级检索 "data transfer" or "data transmission" or "digital transfer" or "digital transmission"，发现有 2240 个 cases，接着用“cross-border data transfer" or "cross-border data transmission" or "cross-border digital transfer" or "cross-border digital transmission”进行限缩，共找到相关案例 5 则：

1、IN RE VALSARTAN, LOSARTAN, AND IRBESARTAN PRODUCTS LIABILITY LITIGATION

本案是一起药品销售跨境诉讼案件，也是首次涉及中国《数据安全法》与美国法院取证权之间关系的案件。原告指控这些药品中含有致癌物质 NDMA 和 NDEA，并导致了消费者的身体健康受到损害。该案涉及多个原告和被告，包括药品生产商和销售商等，美国法院进行了调查取证，但中国当事人以中国保密法规定为由提出抗辩。在本案审理过程中，中国《数据安全法》颁布和施行，中国当事人进一步以该法规定为依据提出抗辩。尽管美国法院认为该法仅限制将中国信息“提供给美国法院”，并未禁止将信息提供给对方当事人，但未对中国《数据安全法》进行详细分析。因此，本案中涉及到了目前中国数据安全法律框架与美国法院取证权之间的争议。

2、Philips Medical Systems (Cleveland), Inc. v. Buan

在本案中，原告 Philips Medical Systems (Cleveland), Inc.控告被告 Buan 在其医疗产品中使用了其专利技术，构成侵权。

美国法院首先从举证责任入手审理此案，认为中国当事人未能承担充分的举证责任。此外，中国当事人也未能证明中国《数据安全法》（Data Security Law）实际上禁止出示有争议的具体文件。因此，法院在审理中驳回了中国当事人的抗辩。此外，美国法院也认为，由于“在美国普通法体系中，取证请求和对取证的回应发生在当事人之间”，中国《数据安全法》并不适用于本案。

3、Heng Ren Silk Road Investments LLC v. Duff & Phelps, LLC

本案中，原告为 Heng Ren Silk Road Investments LLC，被告为 Duff & Phelps, LLC。该案件涉及到公司评估及咨询服务，原告指控被告提供给他们的服务存在瑕疵，并导致一笔不良投资。原告认为被告违反了与其签订的协议和陈述，需要被告对其造成的经济损失进行赔偿。

纽约州法院认为被告中国法专家关于中国《数据安全法》下的潜在法律责任是推测性的，“没有充分的理由”。此外，在本案中有争议的文件是在中国《数据安全法》颁布前三年多创建的，法院认为被告没有证明“中国政府有可能追溯性地适用中国《数据安全法》”，从而回避了对中国《数据安全法》的实质性分析。

4、CF 125 Holdings LLC v VS 125 LLC - 2022 NY Slip Op 32676

本案中，原告向被告提供了融资和借款服务，以便被告能够完成一项房地产交易，并且双方签订了相关的协议。但是，被告最终没有按照协议履行义务，未能还清所借款项。因此，原告提起了诉讼，要求被告赔偿全部债务，包括利息和违约金。被告辩称，由于中国《数据安全法》和《个人信息保护法》的规定，披露的负担和法律风险超过了所要求的文件的效用。纽约州法院驳回了这一抗辩，认为“被告未能证明外国法律禁止提供文件”，并批准原告强制取证的动议。目前，本案已进入上诉。

5、Juul Labs, Inc. v. Chou

“Juul Labs, Inc. v. Chou”是一起关于违反竞业限制协议和商业机密侵权的案件。原告 Juul Labs, Inc.控告前雇员 Chou 违反了其与公司签署的竞业限制协议，泄漏了公司商业机密信息，从而对公司造成了损失。

该案经历了多轮诉讼和上诉。原告要求对被告的各种电子设备进行取证检查，其中若干设备位于中国。被告争辩说，中国《数据安全法》禁止其在未经政府批准的情况下将这些设备运出中国。美国法院认为：虽然中国《数据安全法》问题不是决定性的，但结合被告引用的其他因素，足以限制这一取证申请给被告造成的负担。虽然美国法院未对中国《数据安全法》展开分析，但接受了据此提出的抗辩。美国法院拒绝了原告请求被告出示位于中国境内的电脑以交法庭鉴定的要求，原因来自于综合考虑被告提交证据的负担（其中包括被告提出提交电脑将违反我国个人信息保护法）以及原告未能证明被告故意毁灭或藏匿有关电子证据、原告要求的证据多且对被告经营有较大影响但原告未能提出其要求的某项证据可能于某项所要求的设备之内存储、原告要求的证据可能延期返还对被告利益的损害这三项考虑，法院拒绝了原告要求被告提交位于中国境内的相关设备作为电子证据的动议。从法庭的公开文书可以看出，法院拒绝原告动议主要是程序法的考量，被告提出出示证据将违反我国法律也被法官视为被告提出证据的一个负担（burden）予以考虑。

从上述案例中可以看出美国法院包括联邦法院及州法院对美国法院取证权力与中国《数据安全法》二者谁优先的做法存在差异，虽然有几个案件回避甚至不适用中国的法律，但是美国法院对依据中国法律提出的抗辩依旧予以考虑，这也是中国对接国际，提升域外效力的动力所在。笔者通过上述相同的方式进行欧盟和国际法院的案例检索，并通过欧洲人权法院官网等检索到如下相关案例：

1、United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services（美国赌博案）

该案主要为：由于美国通过在国内封杀网络赌博，甚至通过专门立法和司法判例限制美国网民使用信用卡和通过银行账户向国外赌博网站支付赌金对以赌博业和博彩业为重要财政收入的安提瓜造成了沉重打击，2003 年 3 月 21 日，安提瓜正式向 WTO 争端解决机构提起磋商请求，认为美国联邦和地方政府采取的措施影响了对赌博和博彩服务的跨境交付。这些措施不仅违反了 GATS 关于服务贸易市场准入的规定，而且违反了美国服务贸易减让表中所做的承诺。

本案的焦点：在美国服务贸易减让表分部门 10.D 中，服务门类是“其他娱乐服务（不包括体育）”，在该门类的“市场准入限制”中，美国列出了四种服务的提供类型，在模式 1“跨境交付”项下，美国标注的承诺是“没有限制”(None)。对此，安提瓜主张，美国就赌博和博彩服务的跨境交付项下做出了完全的市场准入承诺。美国认为，由于在“其他娱乐服务”的分部门中明确标记有“体育除外”，表明美国已经将赌博和博彩服务排除在该门类之外。美国主张，赌博是一种特别的服务活动，如果要将其归入其减让表第 10 类部门（娱乐、文化和体育服务），其应当归入第 10.E 项下。第 10.E 分部门的类别是“没有产品分类的其他服务”。而对于第 10.E 分部门，美国所做出的承诺是“不作承诺”，即美国没有承担任何市场准入义务。

专家组认为，在本案的情况下，没有必要详尽地界定属于“赌博和投注服务”范畴的服务活动，因为这些不是本争端中的条约条款。因此，小组不需要这样“解释”这些术语。就上述字眼的一般涵义、各方提交的意见书及我们所参考的专门文献而言，专家组认为“赌博及投注服务”包括任何涉及投注的活动，即:指某人拿有价值的东西(通常是钱)去冒险，以换取不确定事件的结果。对于博彩类游戏、彩票和体育赛事，无论这些服务是如何提供的，都可以进行下注或打赌。小组注意到，“赌博和投注服务”的定义包括安提瓜试图跨境向美国提供的服务以及美国允许跨界提供的其他服务。

2、CNIL & Google 案

2022 年 1 月 6 日，CNIL 在其官网上宣布了罚款的消息。CNIL 表示，通过对 Facebook.com、Google.fr 和 YouTube.com 网站的在线调查发现，虽然两家网站均提供了允许用户“立即接受”cookie 的按钮，但对于拒绝接受 cookie 的选择却不是同样的容易——用户需要多次点击才能拒绝所有 cookie，而用户只需要点击一次就可以接受 cookie。CNIL 认为，用户可能因为拒绝机制过于复杂而选择放弃，这相当于“变相强制”用户接受 cookie，影响了互联网用户的同意自由，因而违反《法国数据保护法》(the French Data Protection Act) 第 82 条规定。这并非 Google 第一次受到处罚。2020 年 6 月，法国国务委员会宣布，就谷歌因个性化广告涉嫌违反欧盟《通用数据保护条例》(GDPR) 一事作出最终决定：谷歌未向安卓用

户提供足够清晰、透明的告知，应支付 CNIL 开出的五千万欧元罚单。CNIL 调查认为，谷歌有两处违反了 GDPR：一是未满足透明度和信息披露的相关要求，比如数据用途、存储时限、个性化广告所需的个人数据类型等重要条款分散在不同的文件里，有时甚至需要跳转 5、6 次才能看全。

从该案可以看出，仅仅依靠第三方数据处理公司进行数据合规是远远不够的。中国及世界其他国家先后颁布并实施自己的隐私保护法，毫无疑问，个人信息保护已然进入了全球化的阶段。在万物互联的物联网时代，保护用户个人信息安全已经成为各大 IT 公司最需要关心的问题。

3、Schrems 案

欧盟法院于 2020 年 7 月 6 日发布了“Schrems II”案的判决，认定“隐私盾”协议作为欧盟与美国之间的数据传输通道已经无效。这一判决意味着大量企业无法再依靠该协议来合法地跨境传输数据。判决指出，美国国内法对公权力访问数据的限制未能满足欧盟法律的要求，不符合比例性和严格必要等原则。此外，在美国的监视行为中，欧盟数据主体也缺乏可诉诸的司法补救措施。这是欧盟法院继 2015 年判决“安全港”协议无效后再一次否定欧美间的跨境数据传输机制。

该案件说明美国和欧盟对数据跨境流动的态度还是有所差异，目前欧盟与美国正在通过其他协议达成数据跨境合作。

4、Facebook 诉 DPC 案

奥地利律师兼数据保护活动家 Maximillian Schrems 先生认为 Facebook 公司将其个人数据提供给美国政府机构，违反了欧洲联盟的《通用数据保护条例》(GDPR)和《欧盟基本权利宪章》，他因此向爱尔兰数据保护委员会（DPC）提出投诉。但 DPC 否决了他的投诉，Schrems 先生不服，向爱尔兰高等法院提起上诉，并请求欧盟法院就该案作出裁决。此案涉及到欧盟数据保护和隐私权的关键问题，也是对欧盟与美国之间数据保护协议的挑战。Facebook 认为其将数据从爱尔兰传输到美国的行为是合法的，基于欧盟与美国签署的保护盾保护协议（以下简称“保护盾”），欧盟委员会(European Commission)（以下简称“欧委会”）已经给予该行为充分保护认定(adequacy decision)且满足欧委会在第 2010/87 号决定附件中列出的“数据保护标准条款”(“standard data protection clauses”)中的要求。

在 2020 年 7 月 16 日，欧盟法院做出了初步裁决，认为基于“保护盾”所做出的充分保护认定是无效的。欧盟法院认为个人数据的保护必须“基本等同于”GDPR 所提供的保护水平。法院认为，在“保护盾”下，美国情报机关仍有可能获取用户信息，欧盟公民的个人数据无法得到应有的保护。2021 年，爱尔兰都柏林法院驳回了 Facebook 对爱尔兰 DPC 监管程序所提出的质疑。爱尔兰 DPC 认为 SCCs 不足以提供与欧盟 GDPR 及相关法律“实质上等同”(essentially equivalent)的保护水平。

以上的案例可以看出欧盟法院对公民个人信息的保护比较严格，而美国与安提瓜的案件中，美国最终败诉也说明了美国并非完全的数据自由流动的捍卫者，只是其“长臂管辖”的工具。

（三）专著

在英文著作方面，笔者在 Oxford Scholarship Online、谷歌图书以及 library genesis 进行检索，例如：在 Oxford Scholarship Online 下的 subject 中选择 international law，选择下列 IT and Communications Law，检索和案例相同的关键词，共有 85 个结果，由于跨境数据流动是一个比较新的话题，笔者在关联性结合时效性的基础上选择出了 5 本专著，其中前 3 本为美国的专著：

1、Harcourt, Alison, George Christou, and Seamus Simpson, Global Standard Setting in Internet Governance (Oxford, 2020; online edn, Oxford Academic, 23 Apr. 2020)

作者认为鉴于自我监管的兴起，以及跨国公司、律师事务所和主导跨国法律秩序的积极知识政治的政治力量，在互联网治理方面，民间社会团体正在推动国际组织，美国也在积极寻求与他国的合作，但作者也猜测即使是像电子前沿基金会等成熟的、历史上成功的数字权利组织，也可能带来重大僵局。

2、Kettemann，Matthias C.，The Normative Order of the Internet：A Theory of Rule and Regulation Online (Oxford, 2020; online edn, Oxford Academic, 18 Feb. 2021)

在瑞典和瑞士等以人权为导向的国家与俄罗斯和中国等以主权为导向的国家之间，在规范性方法方面出现了进一步的裂痕，这些国家寻求和监管政府对互联网的更多控制，将电信提供商国有化，规定了数据本地化法律，并对在线异议（或过滤异议言论）实施严厉的惩罚。作者不赞同这种严格的数据本地化立场，他认为数据方面的法律具有碎片化的特征，在对适用于互联网的国际法律规则的以实质为导向的分析中，发展“互联网国际法”新体系的论点被证明是没有根据的。国际法完全适用于互联网，互联网治理是国际法中具有规范价值的补充，是管理互联网资源及其指导相关的社会政治进程的体系。

3、Lawrence Lessig, Code and Other Laws of Cyberspace[M]，BASIC BOOK，2006：83-138.

这本书中，美国的 Lessig 教授反复强调了一个概念：代码即法律。有什么样的代码，就有什么样的网络社会。而网络空间的法律，现在却越来越受到外界（即现实世界）的政策影响。言论自由的限制、实名制的提出与实施，以及网络隐私问题，都发生在中国的互联网上。Lessig 教授提出数据财产化理论，认为应该授予数据主体数据所有权，确定个人对于自身数据的财产权利。Lessig 提醒我们要关注谁在控制代码、谁在制定网络空间的法律，以及这些法律对个人权利和社会公共利益的影响。"The regulation of code is, in a sense, a form of regulation. But it is regulation that acts indirectly – by changing the background conditions against which individuals and firms act, rather than by specifying directly what those individuals and firms can or cannot do."在某种意义上，代码的规制是一种规制形式。但这是一种间接规制——通过改变个人和企业行动的背景条件，而不是直接指定这些个人和企业可以或不可以做什么。Lessig 强调在网络空间治理中需要在代码、法律和市场之间找到一个平衡点。这意味着要权衡各方的利益和自由，以实现有效的网络空间治理，同时保护用户的权益和自由。

从以上的著作中可以看出美国比较注重行业的力量，并且偏向于数据的自由流动而非本地化，Lessig 教授提出的理论就是我国目前正在探讨的数据确权，以上的著作对我国的数据立法以及对接国际条约都有很重大的指导意义。

4、Kuan Hon, W, Christopher Millard, and Ian Walden, 'What is Regulated as Personal Data in Clouds?',in Christopher Millard (ed.), Cloud Computing Law (Oxford, 2013; online edn, Oxford Academic, 23 Jan. 2014)

本章为 Cloud Computing 书中的相关章节，考虑根据欧盟数据保护法，云中的哪些信息是，以及哪些应该被归类为个人数据。首先解决这个问题至关重要，因为欧盟国家数据保护法规定的权利和义务只适用于个人数据，而且往往是在 "全有或全无 "的基础上进行，这取决于特定个人是否被识别或可识别。在云计算中使用加密、匿名化、数据分割和其他技术，对这个门槛问题有影响。

5、塔林手册 2.0

在北约卓越合作网络防御中心（NATO Cooperative Cyber Defence Centre of Excellence）所发布的《关于可适用于网络行动的国际法的塔林手册 2.0》(简称“塔林手册 2.0”）中，最终承认了网络主权和数据主权，将网络空间划分为“物理层”“逻辑层”与“社会层”三层：物理层主要包括各种硬件设备；逻辑层主要是存储在硬件设备中的软件、数据与协议；社会层主要是参与网络活动的个人或机构，主权的行使主要是在物理层与社会层两层，在逻辑层的行使主要是在数据的加密传输方面，通过互联网协议对网络行为进行管理。

以上两本著作对我国数据立法中的数据分级分类提供了参考和借鉴。

（四）论文

笔者在 Westlaw、Heinonline、Lexis Advance 中全文检索 digital/data transmission，在 Westlaw 中选择 secondary sources，共有 74 篇，多属于法律评论类文章，笔者继续在 Heinonline 中选择 Journals and Periodicals 检索 digital/data transmission，cross-border data flows 并结合相关论文引文，但是最终结果较少，接着用 Springer、谷歌学术、检索关键词“CPTPP”和“data/digital transmission”，结合学者论文引文，共得到以下结果：

1、New York University Journal of International Law & Politics Fall, 2021 Matthew S. Erie， Thomas Streinz

作者认为中国对跨境数据流动的影响日益增加，他认为中国推崇的是数据本地化的网络主权概念，并提出了“北京效应”的概念，中国的发展项目“一带一路”和 DSR，特别是中国政府和中国企业提供自己版本的数字发展。这条道路取决于使数字基础设施可访问，同时名义上集中控制东道国政府的数据。政府控制数据流的主张与强调数据“自由流动”的发展模式相矛盾。他们认为数据主权对发展中国家来说是虚幻的。作者认为中国在 2021 年 9 月申请加入 CPTPP 不太可能成功的关键原因方面，CPTPP 成员有可能协调其承诺，支持跨境数据传输和反对领土数据本地化，根据“一带一路”与中华人民共和国的关系，CPTPP 没有将特定数据治理模式强加给东道国。另一方面，希望效仿中国数据主权方法的有利于北京效应的国家将希望避免做出 CPTPP 式的承诺。但也不得不承认中国在现有和新成立的全球数据治理机构中发挥着越来越果断的作用。由于中国、欧盟和美国的方法也有重要的共同点，中国可以通过对冲，即三角化他们与数字超级大国的关系。最后作者认为，数字发展战略需要相应地发展法律框架，以引导数字转型走向社会有益的方向。

2、CROSS-BORDER DATA FLOWS, THE GDPR, AND DATA GOVERNANCE， W. Gregory Voss， Washington International Law Journal June, 2020.

作者认为欧盟和美国在数据隐私立法上有障碍，美国就数据隐私而言，对硅谷几乎没有监管，隐私侵权对保护个人信息没有什么帮助，但是随着数据的发展，美国的《加州消费者隐私法》和拟议的《华盛顿隐私法》欧洲和美国某些州已经或正在通过具有域外效力的数据隐私法，将其法律的范围扩大到其海岸之外。美国各州正在受到 GDPR 的影响。然而，其他国家进一步增加了复杂性，这些国家已经通过了数据本地化法。比如，作者把中国归入数据本地化的典型，中国寻求“网络主权”的目标，并采用了一种强调国家利益而不是公司利益的互联网监管模式。在域外法律的“竞争对手标准”和“规则重叠”限制了跨境数据流动，作者认为，在这种法律规则重叠的情况家，公司可以借助合同来保护数据流动。

3、Frenz, W. (2022). Who Owns the Data?. In: Frenz, W. (eds) Handbook Industry 4.0.

Data protection is comprehensively regulated at the EU level. According to the General Data Protection Regulation, there is a need for a company organisation that limits the processing and storage of personal data to the absolute minimum.

数据保护在欧盟层面得到了全面的监管。根据《通用数据保护条例》，公司组织有必要将个人数据的处理和存储限制在绝对最低限度。仅仅收集数据并不能确立数据的所有权--例如，生产者相对于自动驾驶或生产系统的用户而言。数据分配应根据欧盟法律进行安排。如果数据被发送给电子通讯媒体的免费平台（WhatsApp）的运营商，至少是基于使用权的转让，或者进一步说，是所有权的反转让，那么系统的汇编就不同了。然而，在这方面，必须确保透明度--例如提交同意声明或将其纳入条款和条件。

4、Digital Trade in the Australia—EU FTA: A Future-Forward Perspective. In: Bungenberg, M., Mitchell, A. (eds) The Australia-European Union Free Trade Agreement. European Yearbook of International Economic Law（springer)

该文章介绍了欧盟的 PTA 条款，以及欧盟和澳大利亚在数字贸易上的差异，澳大利亚最近的许多 PTA 都严格遵循了大型地区 CPTPP 中包含的语言。拟议的欧盟文本第 5（1）条规定了严格禁止不合理的数据本地化措施，这反映了欧盟的数字贸易政策，并与欧盟-英国 TCA 中包含的语言相同（上文在 Sect.3.1):

双方致力于确保跨境数据流，以促进数字经济中的贸易。为此，不应通过以下方式限制缔约方之间的跨境数据流：

(a) 要求在缔约方领土上使用计算设施或网络元素进行处理，包括强制使用在缔约方领土上认证或批准的计算设施或网络元素；

(b) 要求在缔约方领土上对数据进行本地化以进行存储或处理；

(c) 禁止在另一方境内储存或加工；

(d) 使数据的跨境传输取决于在缔约方领土上使用计算设施或网络元素的情况，或取决于缔约方领土上的本地化要求

该条款是适用于所有部门的横向条款，涵盖个人和非个人数据。欧盟一贯拒绝纳入任何可能使其隐私法受贸易义务约束的条款。这种方法也反映在欧盟提出的上述条款中，旨在为 GDPR 下跨境数据流的现有监管壁垒提供全面豁免。

作者通过对比之后认为欧盟和澳大利亚在数字贸易方面的立法存在区别，但是目前，他们的 PTA 实践中出现了更大的趋同，欧盟在其最近的自由贸易协定中同意了关于源代码披露要求和数据本地化的规定。然而，关于跨境数据流和数据保护的条款的制定对各方来说可能是一个棘手的问题。欧盟的提案草案表明，它倾向于为其关于跨境数据流的 GDPR 纪律提供全面豁免。这种方法不适合澳大利亚的商业利益，也与他们过去的自由贸易协定做法不一致。作者认为可以继续通过谈判建立共识。

以上文章可以说明欧盟在跨境数据传输中更加注重保护个人信息，但是也逐渐向区域范围内的数据跨境自由流动过渡，这也是我国加入 CPTPP 的目的，我国也可以参考欧盟与他国之间的协定，他们之间如何协调各自的数据利益关系来调整我国的立法，以便于更好地加入 CPTPP。上述论文对中国加入 CPTPP 的障碍在于中国倾向数据本地化，目前各个国家、地区之间对数据跨境流动的规则存在这很大的差异，可以通过例如数据跨境传输标准合同（SSC）等来解决部分问题。当然，也正是因为有差异，中国才需要加入 CPTPP，进而减少“规则重叠”此类妨碍跨境数据流动的现象。

四、检索心得

选择这个检索题目的原因是和笔者的毕业论文相关，通过这次检索，笔者发现在 CPTPP 这个话题下能检索到的资料有限，且多数为中国学者的论文，这也是因为 CPTPP 主要是亚太国家参与，且美国已经退出，因此欧美在这一方面的研究并不丰富，相关数据比较少，因此笔者只能从更加广泛的概念，也就是数据跨境流动这个概念来对不同国家、地区之间的跨境数据流动进行检索，发现不同国家、地区之间的异同，别的国家和地区在协调国内立法和国际协定之间的经验，进而研究中国相关立法加入 CPTPP 在电子商务章节是否可以调和以及如何调和。

对跨境数据流动的英文翻译不够全面，在检索了所有的 data/digital transmission 之后偶然发现有些外文献写的是 cross-border data flows，因此又重新检索了之前的结果，浪费了一些时间。且笔者在检索过程中发现与 CPTPP 直接相关的文献和案例并不多，得从各国的数据政策出发，发现各国对数据跨境流动的态度，在案例以及法院的判例中发现不同的数据流动规则，因此相关概念的检索也非常重要，这就需要对数据相关的所有领域有所涉猎才能更全面的检索出文献，但是有些资料的相关性并不强，这也是目前撰写论文的一大困难。

当然，在本次检索之后，我获得了更全面的资料，甚至发现了台湾学者对我国加入 CPTPP 的态度，也找到了许多与数据流动相关的案例支持我继续研究。

五、初步结论

通过此次文献检索，可以发现中国以及国际在数字立法方面还不完善，各国之间不同的数据跨境流动政策不利于数据价值的发挥，中国积极加入 CPTPP，但也必须直面困难。研究 CPTPP 也不仅仅从 CPTPP 文本本身出发，也要研究相关国家以及同类协定对数据流动的态度异同。CPTPP 作为一个高度开放的国际协定，

需要中国在研究我国与其数据跨境流动方面的差异，对未来做出预判。我国目前是以个人信息保护为主的一个态度，与欧盟的有些相似，但是 CPTPP 与其前身 TPP 的主导国美国是高度自由的模式，因此中国在加入的过程中势必会遇到很多阻碍，对比欧盟、美国对待数据的不同态度以及合作的趋势，可以为我国对接 CPTPP 提供思路和方案。