【国际私法】

数据立法域外适用引发的法律冲突与中国解决方案

文 淑

【摘 要】大数据时代，数据立法域外适用的趋势明显，各国据此实现数据主权的扩张和抢占战略博弈的制高点。然而，一国数据立法域外适用边界和效力的延展，难免触及他国主权权力和管辖利益的边界，引发国家间在立法、执法和司法层面的剧烈冲突。单边数据立法域外适用还涉嫌违反现行双边司法互助协议和国际经贸投资条约，引发国内法与国际法的冲突。冲突的成因在于，传统管辖权理论的式微、国际数据治理与冲突协调规则的赤字以及国家间的利益竞争与话语权争夺。为解决冲突，中国须在涉外法治与国际法治的互动视野下构建攻防兼备的数据立法域外适用制度，加强数据领域域外执法与司法领域的双边合作与国际礼让，同时，在数据流动的多边规则构建和全球治理中发挥引领作用。

【关 键 词】域外适用；法律冲突；数据治理；国际礼让

【作者简介】文淑，女，云南昆明人，中国人民大学在读博士研究生，研究方向为国际经济法、数据治理(北京 100872)。

【原文出处】《云南师范大学学报》：哲学社会科学版(昆明)，2023.6.96～108

【基金项目】国家社会科学基金重大项目“我国政府数据治理与利用能力研究”(20&ZD161)。

引言

随着数字经济的深入发展和数据价值的日益凸显，数据流动在推动国际贸易、促进经济增长、加速企业创新和增进社会福祉的同时，也面临着数据主权、国家安全、隐私保护、数字鸿沟等挑战。[①]各国结合自身经济水平与利益诉求，纷纷围绕数据治理展开日趋激烈的规则博弈与制度竞争。各国虽然根据不同的数据治理理念形成了殊别的数据立法范式，却在数据立法的域外适用倾向上趋于一致，不断扩展着本国数据立法域外适用的广度和深度。据统计，所有“二十国集团”(G20)国家的数据立法均确立了域外适用规则，[②]以进一步扩展本国数据治理规则的核心竞争力和国际影响力。

本文所称数据立法，主要是指以个人数据保护、数据跨境流动和数据跨境调取为规制对象的国内法律规则。数据立法域外适用，是本国针对位于或发生在其管辖领域外的人、物或行为适用本国数据立法的过程。[③]域外适用以立法机关制定域外效力条款或主张域外管辖权为基础，[④]通过执法机关和司法机关适用法律规则实现。数据立法的域外适用有一定的必然性，数据治理的国际规则尚不完备，各国无法仅通过数据立法的域内适用达到数据立法目的和数据治理效果。但另一方面，数据立法的域外适用打破了传统地域因素对法律效力的基础控制作用，势必引发国家间管辖利益与主权利益的冲突；国际法是主要处理国家间关系的法律规范，已然形成一套独立于特定国家的理论建构和法律秩序，数据立法的域外适用可能打破现行国际法对国家权限和管理规则的分配标准，因此也可能引发国内法与国际法的冲突。处理不当易造成国家间的恶性竞争、破坏国际法律秩序和国际关系的稳定。从理论层面，数据立法域外适用是国内法域外适用在数据领域的具体体现，具备国内法域外适用的涉外法治属性。涉外法治是一种介于国内法治与国际法治之间的双

向互动形态，既涉及涉外法治与国内法治的互动，也涉及涉外法治与国际法治的互动。由于国内法治有广义与狭义之分，广义上的国内法治概指国家基于主权依法治国，处理自己对内、对外事务的立法、执法、司法、守法、用法的活动，因此涉外法治本质上是国内法治的一部分；狭义的国内法治是处理纯国内事务的法治活动，与涉外法治并列构成国家法治体系的组成部分。[5]因此，“涉外法治与国内法治的互动”既可以指代本国视角下的纯国内事务与对外事务的法治活动的互动关系，也可以指代作为本国国内法治一部分的涉外法治与他国的国内法治的互动关系。本文重点阐释后者。将此互动关系投射到数据立法的域外适用上，即表现为因数据立法域外适用引发的国家间法律冲突，以及因数据立法域外适用引发的国内法与国际法冲突。

目前，中国正加快法治中国和数字中国建设，在此背景下，鉴于数据治理的重要性与数据立法域外适用的现状，以涉外法治与国内法治的互动，以及涉外法治与国际法治的互动为视角，研究数据立法域外适用引发的法律冲突并提出中国解决方案，具有一定的理论价值和现实意义。

一、相关研究文献综述

近年来，有关数据立法域外适用的国内外研究成果不断涌现。当前研究主要以单个主权国家出台的政策法律或国际经贸投资协定为研究对象，可以归纳为以主权国家为视角和以国际贸易视角的研究。

主权国家视角下，学者梳理了欧盟、美国等重要主权国家的数据立法，对相关数据立法域外适用的前提，即对数据立法的域外效力或域外管辖权进行研究。Dan Jerker B，俞胜杰，叶开儒等以欧盟《通用数据保护条例》(以下简称GDPR)第3条为中心论证了欧盟积极主张GDPR域外效力的立法动因与规制思路。[6]Adèle Azzi，何叶华认为GDPR的域外适用范围尽管相当广泛，但其符合国际判例的默示承认和国际习惯法原则，具备国际法正当性基础。[7]杨永红，何叶华认为美国利用《澄清合法使用境外数据法》(以下简称《云法案》)将美国企业在全球互联网行业的优势转变为美国对域外数据的管辖权，严重威胁包括中国在内的大多数国家数据主权。[8]Federico Fabbrini等的《跨境数据保护：跨大西洋视角下的治外法权与国家主权》一书结合欧美数据领域的最新立法、判例探讨了在数据立法域外适用背景下欧美的紧张关系与合作空间。[9]张哲等认为通过国内数据立法进行域外效力扩张已成为多数国家维护数据主权的主流做法，我国应借鉴欧美数据立法、完善我国数据立法域外效力制度的适用性、体系性与国际性。[10]

国际贸易视角下，学者主要探讨了国际投资贸易规则对数据跨境流动和个人数据保护等议题进行规制的可行性与具体模式。Margaret Byrne Sedgewick认为，鉴于欧美对世界贸易组织(WTO)现行《服务贸易总协定》(GATS)的推崇，应将跨境数据流动议题纳入GATS框架[11]；石静霞提出WTO协定在数字贸易规制上存在明显不足，电子商务诸边谈判有望重振WTO的规则制定权，但中美欧等主要成员在数据跨境流动、软件源代码及算法规制和税收问题上存在较大分歧。[12]谭观福，戴艺晗，石静霞梳理了《区域全面经济伙伴关系协定》(RCEP)《全面与进步跨太平洋伙伴关系协定》(CPTPP)《美墨加协定》(USMCA)《数字经济伙伴关系协定》(DEPA)等新近自由贸易协定(FTA)对数据跨境流动的规制原则与例外。[13]彭岳认为WTO和FTA通过贸易例外和贸易事项两种方式纳入个人数据保护问题。[14]张生则以国际投资协定(IIAs)与跨境数据流动的内在关联为视角，关注国际投资协定对跨境数据流动的保护及其限度。[15]Neha Mishra认为国际贸易规则、互联网治理和数据跨境流动之间应建立起“桥梁”[16]。Andrew D等认为涵盖国际投资法、国际贸易法的全面法律框架以及涵盖各种利益相关者的广泛法律政策将更好地实现数据的安全、开放与高效流动。[17]

总体而言，既有研究已经关注到国别层面或国际法层面的、与数据立法域外适用相关的问题，所提建议具有借鉴性和被动性。也有少量研究以数据立法的域外适用为研究对象，系统性地梳理了欧美数据立法域外适用的核心概念与现行规则，[18]为本文的研究奠定了重要基础。但以数据立法域外适用引发的法律冲突为研究对象，从涉外法治与国内法治和

国际法治的互动视角，系统性审视数据立法域外适用的法律冲突、揭示冲突成因，并提出统筹性和主动性解决方案的研究较为欠缺。因此，本文首先阐述数据立法域外适用的前提与保障措施，在对数据立法域外适用的广度和深度有充分认知后，探讨数据立法域外适用已经或可能引发的法律冲突并分析其成因，最后提出中国解决数据立法域外适用法律冲突的协同应对方案。

二、数据立法域外适用的现实基础

(一)适用前提：数据立法域外管辖的确立与扩张

一国数据立法域外适用的前提是域外管辖的确立。互联网乌托邦下数据天然的流动属性与威斯特伐利亚体系下的传统管辖权理论形成鲜明错位，各国突破地域因素的局限，通过制定“设立机构准则”“目的意图准则”和“数据控制者准则”，实现对域外数据处理或控制实体，或域外数据处理行为的管辖，有效扩张了本国数据立法的适用范围。例如GDPR第3(1)条规定了“设立机构准则”，使GDPR适用于在欧盟境内设立机构的数据控制者或处理者所进行的数据处理行为，不论该行为是否发生在欧盟境内。GDPR序言第22条对“设立机构”的定义是“通过稳定安排开展真实有效的数据处理活动”，并不将设立机构局限于具体的地理位置或法律形式(子公司分支机构、代理人等)。其次，设立机构不需要为实际的数据处理者，只要设立机构开展的活动与实际的数据处理具有“无法割裂的联系”，在欧盟境内盈利，就应适用GDPR的规定。[19]可见，“设立机构准则”实现了对传统属人管辖权内涵的技术性扩张。菲律宾《2012年数据隐私法案》、南非《2020年个人信息保护法案》和澳大利亚《1988年隐私法》等立法均以“设立机构准则”为基础制定了域外适用范围条款。

不止于此，欧盟GDPR第3(2)条还确立了更为激进的管辖思路——“目的意图准则”。对于未在欧盟境内设立机构的数据控制者或处理者，只要其针对欧盟境内的数据主体实施了提供商品或服务的行为，或对数据主体活动进行监控，GDPR便对其产生效力。“数据主体”并不限于具有欧盟成员国国籍的主体，更在于主体所处的地理位置是否位于“欧盟境内”。构成“监控”行为的类型也非常广泛，包括提供特定广告、地理定位、个性化饮食和健康分析等。该准则以介于属地管辖和保护性管辖间的效果原则为基础，凡是影响到数据主体利益的行为均被纳入管辖。有学者批评该准则过于虚无缥缈，在全球互联网高度融合的背景下上述影响因素可轻易达到，并引发频繁的管辖权冲突。[20]由于“设立机构准则”侧重行为与主体间联系，“目的意图准则”侧重行为与客体间联系，连接点并不冲突，一国可以同时采纳两种准则。巴西《2020年通用数据保护法》、日本2023年修订的《个人信息保护法》和新加坡《2021年个人数据保护条例》即借鉴了欧盟GDPR的立法范式，将广泛的域外主体和行为纳入管辖范围。

美国《云法案》、加拿大《个人信息保护和电子文件法案》、欧盟《电子证据条例》等数据立法则从跨境数据调查取证的角度实现了从“数据存储地准则”向“数据控制者准则”的转变，明确本国执法机构有权要求本国网络服务提供者披露其所拥有、保管或控制的数据，无论该数据位于境内或境外。上述立法通过对数据控制者行使属人管辖，延伸获得了数据控制者可获取的境外数据的管辖权，赋予了属人管辖之于属地管辖更优先的适用顺位。而且，美国《云法案》所确立的“数据控制者准则”也不局限于国籍等传统属人连接因素，只要数据控制者与美国的联系符合美国判例法的“最低程度联系”原则，在境外成立的数据控制者也可被纳入适用范围。[21]

(二)适用保障：数据跨境传输工具对数据立法域外适用的强化

以欧盟GDPR为代表的数据立法不仅通过适用范围条款确立了对域外主体和行为的管辖，还引入了充分性认定、标准合同条款(SCCs)、约束性公司规则(BCR)、认证机制等数据跨境传输工具，以监管欧盟数据出口方向境外数据进口方的数据传输活动。根据欧盟数据保护委员会(EDBP)发布的《指南》，二者为补充与补足的关系而非互斥关系。当境外数据进口方依据“设立机构准则”或“目标意图准则”落入GDPR适用范围时，数据进口方与数据出口方间仍应依据数据跨境传输条款要求采纳SCCs等保障措施。因为跨境传输活动项下的数据仍面临数据进口

国国内法律、政府访问以及难以获取或执行数据保护救济等风险。[22]该规定一方面旨在弥补数据进口国数据保护水平的不足，另一方面，无论境外数据进口方是否符合GDPR的适用范围，数据进口方与数据出口方必须通过数据跨境传输工具进行数据跨境传输。数据跨境传输工具的特殊性和强制性可实现数据立法对域外主体或行为的直接或间接适用，对数据立法的域外适用有强化作用。

具体而言，国家层面，一国为获得欧盟的充分性认定，需修改本国的数据立法和执法制度以达到与欧盟同等的数据保护水平，并接受欧盟的整体审查和持续监督。这意味着该国将主动适用欧盟的数据立法，使欧盟数据立法产生事实上的域外效力，即域外影响力。[23]

企业层面，境外数据进口方与欧盟数据出口方订立的SCCs或BCR中，包含强制性的准据法条款和管辖权条款，能够产生强制域外数据进口方企业适用GDPR的效果。就SCCs而言，3种传输模式下的SCCs第17条均规定，合同双方必须选择适用欧盟成员国的法律。此法律必然包括以GDPR为首的数据立法；SCCs第18条则规定，合同双方认可欧盟成员国法院对合同争议拥有管辖权。就BCR而言，尽管欧盟没有明确要求跨国公司选用BCR时适用GDPR，但EDBP第29条工作组发布的《BCR批准标准》显示，获批的BCR须说明其与相关适用法律间的关系，若当地立法要求对个人数据提供更高水平的保护，则该立法应优先适用。鉴于GDPR高水平的个人数据保护标准，其适用在所难免。其次，当数据出口方在欧盟未设立机构时，《BCR批准标准》要求BCR赋予数据主体在其经常居所地提起诉讼的权利，欧盟成员国法院可据此获得案件管辖权，保障了GDPR域外适用的实现。该管辖权条款与GDPR第79条类似，均是通过第三人受益条款赋予数据主体损害赔偿请求权和原告所在地管辖权，[24]使欧盟法院能具备所有与欧盟仅有微弱联系的个人数据保护案件管辖权。SCCs和BCR本质上具有契约属性，根据传统合同纠纷的意思自治原则，当事人应享有协议管辖自由和准据法选择自由，但上述条款要求当事人必须约定适用GDPR和接受欧盟成员国法院管辖，阻断了当事人利用意定管辖排除GDPR适用的可能，变相扩大了GDPR的域外适用范围。而且，数据进出口方不得对获批后的SCCs进行修改，除非修改内容使数据获得更严格的保护；获批后的BCR也不得作出重大变化，否则须另行启动批准程序。欧盟通过数据跨境传输工具强化欧盟数据立法域外适用的决心可见一斑。

综上可见，以欧美数据立法管辖权的扩张为代表，各国扩大本国数据立法域外适用范围、强化本国数据立法域外适用效力的趋势日益凸显。这已成为各国维护数据主权和参与国际数字治理的共同做法，但数据立法域外适用引发的一系列现实和潜在冲突也亟待正视与解决。

三、数据立法域外适用引发的法律冲突及其成因

(一)数据立法域外适用引发的法律冲突

1.数据立法域外适用引发的国家间法律冲突

数据立法兼具公私属性，但其域外适用不以私法领域的“多边主义法律选择方法”为体系构造，即从法律关系出发，探讨该法律关系应当适用本国法或其他国家的法律；而是以公法领域的“单边主义法律适用方法”为基础。[25]这意味着一国法院只需考虑本国法可否适用于境外的人或行为，无须同等考虑外国法可否适用于本国境内的人或行为。这不仅造成了国内外法适用的不平等，而且随着各国数据立法域外适用范围的扩大、数据立法域外适用趋势的强化，势必引发频繁的国家间法律冲突。

立法层面，国家间的法律冲突表现为各国立法机关竞相制定具有域外效力的数据立法，立法边界的重叠导致立法冲突。各国立法规制的范围越广，冲突的可能性就越大。由于各国数字经济发展水平和数据立法进程的不均衡，可将立法冲突分为消极冲突和积极冲突：消极冲突是指一国针对数据立法域外适用作出扩张性规定，而其他可能受影响的国家尚未采取任何法律规制措施，由此构成潜在的管辖冲突；积极冲突是指各国依据不同的管辖权原理和准则对同一数据处理行为进行规制所导致的管辖冲突。例如微软公司处理其存储于爱尔兰数据中心的数据可能引发美国基于“数据控制者准则”和欧盟

基于“设立机构准则”管辖的竞合。即使美欧为实现商业利益接续达成双边合作协议，也只是暂时的动态平衡。[26]从欧美《安全港协议》到《隐私盾协议》的失效，已表明该平衡为更显著的数据规制理念冲突所取代。2022年3月达成的《跨大西洋数据隐私框架》能否弥合双方在数据保护与数据监控间的规制分歧，成为数据跨境流动的合作范本尚未可知。然而，立法冲突属于虚拟的法律冲突，数据立法域外适用是否会产生现实法律冲突，主要取决于各国如何执行和适用相关数据立法。

执法层面，一国行政机关单边执行具有域外效力的数据立法的行为，既包括司法机关/行政机关对域外数据行使的调查取证行为，也包括行政机关对域外主体的直接行政处罚与强制。[27]习惯国际法承认域外行使立法管辖的自由，但仍然认为执法管辖应严格遵循属地原则，[28]因此，与立法层面的冲突相比，数据立法的域外适用将在执法层面引发国家间更剧烈的冲突。首先，一国单边的数据跨境执法调取严重侵犯他国数据主权、削弱国家间的政治与法律互信、引发他国的阻断与反制。例如，美国《云法案》的出台触发欧盟效仿美国制定了同样具有域外效力的《电子证据条例》，并刺激中国、瑞士、新加坡等国制定阻止《云法案》在本国适用的阻断法规、设定数据出境的负面清单。但事实上阻断法规的实践效果并不理想，美国法院和执法机关通常不会支持当事人依据阻断法规提出的抗辩要求。在Cadence Design Systems，Inc. v. Syntronic AB案和Philips Medical Systems v. Buan案中，被告以涉及向中国跨境取证的证据开示动议违反《数据安全法》《个人信息保护法》等数据立法为由抗辩，但美国法院认为被告没有充分举证证明中国的数据立法禁止其履行证据开示义务、且遵守证据开示要求并不会使被告遭受中国政府的严厉处罚。在Rollins Ranches LLC v. Watson案和Giorgi Global Holdings v. Wieslaw Smulski案中，被告也未能成功援引GDPR阻断美国法院对欧盟境内个人数据的跨境取证要求。这表明各国的阻断法规能否成为数据攻防战中的“盾牌”、起到实际封阻他国单边跨境数据取证的效果仍然存疑。其次，行政机关对域外主体执法的可执行性有待观察。近日，来自英国、希腊、意大利和法国的数据监管机构向美国Clearview AI公司发出执法通知，认定Clearview AI公司从Facebook等社交媒体中收集人脸图像并建立全球数据库的行为违反GDPR，要求Clearview AI公司删除相关个人数据并处超过4000万欧元的罚款。但该执法行动明显受挫，Clearview AI公司否认了违规行为，并反驳执法机关的执法管辖权。[29]由于该公司并未在欧盟或英国境内设立任何机构或可供执行的财产，上述行政执法机构不具备强制域外执行的条件。

司法层面，国家间的法律冲突表现为一国法院适用具有域外效力的数据立法、强制域外数据控制或处理主体执行具有域外效力的判决。不仅冲击他国司法主权，还可能导致不同法域的法律价值冲突。以Google Inc. v. CNIL案为例，法国国家信息与自由委员会根据GDPR赋予数据主体的“被遗忘权”要求谷歌公司删除欧盟境外全球范围内的相关网页链接，Google公司拒绝了该执行令并被处以10万欧元罚款。Google公司辩称，域外执行“被遗忘权”将严重侵犯国家主权原则、不干涉内政原则和相称性原则；过度保护个人数据权也可能侵犯他国公民的言论自由权，甚至触发他国的违宪审查。学界也质疑了欧盟的做法，认为欧盟无权在欧盟境外世界范围内对个人数据保护与言论自由权进行权衡；有学者则担忧其他国家和搜索引擎公司效仿欧盟做法，以数据保护为名限制言论自由，容易引发严重损害言论自由的“逐底竞争”[30]。尽管欧盟法院最终妥协，将被遗忘权的执行范围限于欧盟境内。但一方面欧盟法院是从“地理封锁”这一技术层面说明域内执行可达到保护个人数据权利的效果，刻意回避了域外执行的合法性及合理性问题；另一方面其并未放弃域外执行的主张，各成员国的司法机关或数据监管机关依然有权以本国的基本人权标准个案判断是否域外执行被遗忘权。这表明欧盟依然在不遗余力地通过数据立法域外适用来推行欧盟的“数据帝国主义”[31]战略。此外，一国法院适用域外效力的数据立法作出的判决，并不一定能得到外国法院的承认与执行。被请求国在对外国判决进行司法审查时，首先会质疑请求国法院依据“目的意图准则”等行使司

法管辖的合理性[28];其次被请求国可以“公共政策例外”为由拒绝外国判决的承认与执行。在Google Inc.v. Equustek Solutions Inc.案中,加拿大最高法院作出了要求Google公司在全球范围内删除链接以阻止知识产权侵权行为的判决,Google公司随即向美国加利福尼亚北区法院提出执行异议。美国法院认为执行判决将违反美国宪法第一修正案,Google公司无须在美国版本的搜索引擎中删除相关链接,致使加拿大法院判决的域外执行受阻。

2.数据立法域外适用引发的国内法与国际法冲突

前已述及,国际法是国家权力和国家利益在国际社会的法律表达,现行国际法虽然不是理想的产物,而是现实的回应,[29]但不可否认的是,国际法是一套需要国家遵守和服从的法律秩序。因此,国家基于数据主权的规制行为要受到该国接受的国际规则的约束,一国数据立法域外适用的行为需要经过现行多双边国际条约的检视。

数据调取层面,一国适用以“数据控制者准则”为基础的数据立法,进行单边数据跨境调取的行为,不仅侵犯了数据权属国的专属执法管辖权,还涉嫌违反以国家合意为支撑的双边司法合作机制的规定。以美欧间的数据跨境调取为例,美欧签订了《司法互助协议》(MLAT),未签订《云法案》框架下的“适格政府”双边执法协议,但美国政府有理由无视美欧MLAT,直接凭借《云法案》要求数据控制者提供欧盟相关数据。这是因为《云法案》“免除数据控制者披露义务”的3个条件中并不包括MLAT优先适用的情形[30];美国司法部仅认可外国政府获取美国数据时MLAT的可适用性、并未反向明确MLAT的可适用性或优先适用顺位;况且,美国一直秉持着“数据控制者准则”构成域内执法而非域外执法的观点。[31]美国单方跨境调取欧盟数据的行为,一则明显违反GDPR第48条非经互惠不得跨境转移数据的规定,构成上文所谓的国家间法律冲突;二则《云法案》的规定明显违背美欧MLAT的个人数据保护标准和程序要求。首先,数据最小化原则的适用范围较窄,仅适用于美国居民的数据,美欧MLAT的规定则涵盖美国与非美国居民的数据、数据主体可获取的所有数据和与调查无关的数据。其次,《云法案》下数据主体的救济权仅限于违反《存储通信法案》(Stored Communication Act,SCA)下的民事司法救济,达不到美欧MLAT下充分保障数据主体的行政救济权和司法救济权的要求。复次,《云法案》赋予了美国执法机关依据调查令单方面调取境外数据的权力,并不要求数据控制者或美国执法机关向数据权属国行使告知义务,特别在美国执法机关向数据控制者发布禁止披露命令时,数据权属国的数据出境知情权得不到保障,违反了美欧MLAT的程序规定。[32]欧盟完全可诉诸MLAT自身的争端解决机制解决上述争议。余外,美国与有关国家签署的“适格政府”双边执法协议也具有国际法上的不法性,经美国认定的“适格政府”可借助此协议要求美国企业提供其存储在第三国的数据,这显然与“非经第三国同意,条约对第三国无法律拘束力”的条约法精神不符。

数字贸易层面,一国数据跨境传输工具的域外适用易与他国产生管辖竞合和规范溢出,他国要么反向制定数据本地化措施,要么跟风制定有条件的数据跨境传输规则,均产生限制数据跨境自由流动的效果。数据跨境流动限制性措施涉嫌构成国际贸易投资法框架下的贸易壁垒和投资壁垒,受到国际贸易投资法的规制。在WTO框架下,WTO的争端解决机构可通过“技术中立”原则将成员国限制数据跨境流动的措施纳入GATS的管辖范围,并根据成员国的具体承诺个案认定贸易壁垒的存在。[33]在FTA下,以CPTPP、USMCA、DEPA为代表的新近自由贸易协议定基本以数据跨境自由流动为原则,例如CPTPP第14.11.2条规定“每一缔约方应当允许以电子方式进行跨境信息传输,包括个人信息”,“应当”的措辞为缔约方施加了具有法律约束力的强制性义务;对数字贸易壁垒的界定亦有从边境措施向境内限制措施扩展的趋势,[34]这将导致缔约方采取的数据跨境流动限制性措施更容易违反上述FTA的规定。在IIAs下,跨境流动涉及的数据可能构成IIAs项下的适格投资,因此,一国针对数据跨境流动的限制措施可能构成投资壁垒,或涉嫌违反国民待遇、公平公正待遇或禁止征收条款,并触发国际投资争端解决程序。

尽管缔约方可援引一般例外条款、安全例外条款或FTA下的合法公共政策目标例外条款免责，但一方面，参照WTO的争端解决实践经验，缔约方的数据跨境流动限制性措施(特别是数据本地化措施)较难通过“必要性测试”等要件的审查；[39]另一方面，例外条款的内涵模糊，并不能为缔约方的限制性措施提供足够的法律确定性。在国际贸易投资法下探讨数据跨境流动的规制，将始终存在着国家实现公共利益或合法政策目标与实行贸易投资保护主义的区分难题，[40]以及促进贸易投资自由化与保障国家数据规制主权的平衡问题。

(二)数据立法域外适用引发法律冲突的成因

1.传统管辖权理论划定数据立法边界的水土不服

传统国际法理论根据管辖依据的不同将国家管辖权分为属地管辖、属人管辖、保护性管辖和普遍管辖。属地管辖原则在界定国家主权范围上起到基础性控制作用，各国一般通过物理空间的地域关联划定其国内法的效力边界。但大数据与云计算技术的应用实质上在地域之外创设出一个虚拟的网络空间。在这一空间，数据的流动呈现出瞬时性、无界性和全球性，数据全生命周期下的数据活动包括数据收集、存储、加工、使用、共享、删除、销毁等数据处理各个流程，丰富多样的数据活动增大了同一数据与多个地域产生联结的可能性，以传统属地管辖原则进行追索必然带来管辖权的冲突；在数据流动过程中，也难以确定数据的收集者、传输者或使用者等数据活动参与者，主张传统属人管辖原则将导致管辖权的不确定。在此背景下，国家只能立足其域内侧面、在传统管辖权理论的基础上扩张或衍生新的管辖权内涵。固守属地主义的保守型管辖权体系已逐渐为进取型管辖权体系所取代。[41]但如前所述，各国对数字时代的管辖权内涵莫衷一是，数据立法管辖权的非排他性和重叠性引发数据主权的碰撞与冲突。

2.国际法协调数据立法域外适用冲突的规则赤字

国际法不禁止数据立法的域外适用，但缺乏统一和协调数据立法域外适用冲突的约束性国际规则，加剧了各国数据立法域外适用的竞争与冲突。1927年“荷花号案”判决通常被视为讨论国内法域外适用国际合法性的出发点。国际常设法院指出，只要国际法未明确禁止，“国家可以按其认为的最佳方式发展域外适用规则”[42]。联合国国际法委员会报告亦肯定了国际法赋予国内法域外适用的能动空间。[43]但国内法的域外适用不得过度扩张，应受到实际联系原则、反域外适用推定原则和国际礼让原则等的限制。[44]然而，就涉及数据跨境流动和个人信息保护的规制而言，迄今尚未形成广泛认可的和具有约束力的、协调域外适用冲突的国际规则。在数据规制路径下，中美欧三大数字经济体对个人数据保护、数据跨境流动的规制理念迥异，短期内达成综合性国际数据条约的可能性不大；在贸易规制路径下，数据规制与传统贸易协定的价值取向并不完全匹配，仍需要各国在WTO开放式诸边谈判和FTA中进一步探索解决方案。是故，在国际法尚未对国内法域外适用做过多限制以及多边主义难以达到规制效果的情形下，主权国家数据立法域外适用引发的法律冲突难以得到妥善协调。

3.国家利益竞争和国际话语权争夺为冲突根源

国家间数据立法的域外适用及由此引发的法律冲突，究其根源，在于数字经济背景下国家间的利益竞争与国际话语权争夺。欧盟扩张其立法域外适用范围的动机不仅源于全面保护数据主体权利，还在于通过保护的一致性拉平欧盟内外企业的竞争条件、向全球推广欧盟规则范式，最终引领和塑造符合欧盟价值观与利益的国际规则[45]；美国作为数字产业大国，其扩张域外管辖权，一则可助力其进一步抢占全球数据市场，发挥美国企业“监控资本主义”的优势，[46]二则有利于提升其在数字领域的国际主导地位、增强其在网络执法合作领域的话语权和规则制定权。与美欧相比，俄罗斯和印度数据立法仍以属地管辖为原则，数据立法的域外适用范围相对限缩，两国主要通过数据存储和处理本地化规则解决数据治理与本地执法问题，目的在于维护国家安全、预防网络攻击和网络制裁及发展本国数字产业。[47]可见，国家利益和国际话语权深刻影响着国内法与国际法的形塑。

四、解决数据立法域外适用法律冲突的中国方案

我国数字经济规模位列全球第二，[48]这一数字背后既反映了中国数据产业的强大实力，又对我国个人数据保护、数据跨境流动和数据跨境调取等领域的数据治理提出更高要求。在国际数据治理的规范和制度供给赤字的背景下，为维护我国国家安全和网络主权、充分保护个人数据权利和参与国际数据市场的良性竞争，我国存在推动数据立法域外适用的现实需求。目前，我国《个人信息保护法》和《数据安全法》已包含域外适用范围条款、数据跨境传输规则、法律责任条款和阻断条款，[49]可见我国已基本完成数据立法域外适用的顶层设计，并以《阻断外国法律与措施不当域外适用办法》为配套作为应对域外适用冲突的主要工具。然而，数据立法的域外适用具有一体两面性，其本质是一国数据主权权力的扩张，必然导致他国数据主权权力的消减，进而造成与他国数据主权权力的冲突。在扩张、冲突、反制的反复博弈下，国家数据主权力量有望达成新的平衡并塑造出普遍认可的国际数据治理规则体系。换言之，数据立法域外适用的冲突过程与国际造法过程高度耦合。因此，中国应在更全面的、涉外法治国际法治的互动视角下考量数据立法域外适用冲突的解决方案，既坚持国家本位路径，又符合国际法治精神与网络空间命运共同体理念，最终引领全球数据治理的国际造法和国际秩序构建。

（一）单边层面：构建攻防兼备的数据立法域外适用制度

党的二十大报告指出，“加强重点领域、新兴领域、涉外领域立法”[50]。构建数据立法域外适用制度，属于二十大报告中所谓重点领域、新兴领域、涉外领域立法的题中之义。目前，国际社会对数据立法域外适用的边界尚无定论。当他国主张数据立法的不当域外适用，特别是以“数据控制者准则”为依据进行数据跨境执法调取时，阻断立法不失为一国所能采取的最直接的办法。我国的《国际刑事司法协助法》第4条、《个人信息保护法》第41条至第43条、《数据安全法》第26条和《阻断外国法律与措施不当域外适用办法》为阻断和反制提供了法律依据。但一方面我国阻断立法缺乏实施细则和实际处罚案例，难以作为我国企业抗辩他国单边数据跨境执法调取要求的有力支撑，另一方面我国应审慎采取阻断立法和反制措施。“以牙还牙”的方式使各国陷入零和博弈的困境，容易引发新一轮法律与外交冲突，还可能加剧数据处理者同时违反两国法律的双重风险。

与“防守型”的阻断立法相对，我国还应采取“进攻型”的应对策略，以更加精细化和灵活化的方式提升数据立法的域外适用性，为数据跨境的有序治理提供制度保障。在我国完成粗线条立法后，各部委及地方政府应加快出台实施细则和地方条例的步伐。首先，可根据条款所涉法益的区别，划定差异化的域外适用范围。例如，数据主体权益保护层面的条款，可依据较低程度联系对数据控制或处理者实施域外管辖；行政管理义务层面的条款，可在联系达到显著程度时再实施域外管辖，细化数据规则域外适用范围的颗粒度。其次，就数据跨境传输规则而言，我国网信办出台了《个人信息出境标准合同办法》及标准合同范本，明确将准据法限定为“中华人民共和国相关法律法规”，但合同双方可就合同纠纷选择境外仲裁机构进行仲裁，体现出我国数据跨境流动规则域外适用和司法管辖的合法性与合理性。然而，我国现存的数据跨境传输工具存在功能与内容交叉重叠的问题。可在后续立法中针对不同的数据跨境传输风险需求，匹配不同的数据跨境传输工具。例如，利用数据出境安全评估应对外国政府强制跨境调取数据的安全风险，标准合同应对数据接收方的违约责任风险，专业机构认证应对外部网络攻击造成的技术漏洞风险等。[51]再者，我国应注重国内跨境流动限制性措施与国际法的协调。比如我国对个人信息和重要数据的本地存储要求，及数据出境安全评估制度可能无法通过国际经贸投资协定的压力测试。对此，国内立法上我国可订立负面清单，规定透明度条款、非歧视条款，进一步厘清重要数据的范围和出境要求，做到有法可依；国际立法上我国可主导国际经贸投资协定的成员国就例外条款的适用范围、测试要件的可操作性等方面达成共识，以便我国在兼顾数据跨境流动安全与发展利益的同时，避免与现行国际规则相矛盾。

(二)双边层面:加强数据领域域外执法司法的双边国际合作与国际礼让

单边执行和适用具有域外效力的数据立法,将造成现实法律冲突,甚至引发国际纠纷,迫切需要各国理性应对。因此,我国行使执法和司法管辖权时应展现数据主权的谦抑性,以国际合作和国际礼让原则为基础,[52]实现管辖权域外行使与尊重他国数据主权的平衡。这是主权博弈下协同治理的相对"最优"选择。[53]首先,我国在《全球数据安全倡议》中明确提出,我国对境外数据的调取通过国际合作机制实现,并未将执法权限单边延伸至境外,凸显了我国对他国主权的尊重。但传统的执法合作与MLAT机制逐渐暴露出缺乏稳定的调取标准和快捷的调取流程的弊端,难以适应数据跨境调取的现实需求。对此,我国应结合电子数据的特点有针对性地改造升级传统的执法合作与MLAT机制。例如简化官文传递手续、明确响应与取证的时限要求、统一调取标准和适用、允许文书证据在线传输和证人证言视频取证,[54]确立以协商为基础的争议解决条款,必要时推动境内外双方执法者的直接合作。其次,可基于国际礼让原则允许外国政府或个人请求调取存储在我国的数据。与美国《云法案》以美国利益为优先、跨境调取条件非对等、保留充分自由裁量权的"国际礼让分析"不同,我国应构建起对等的、层次分明的外国政府数据跨境调取审核机制。对国家核心数据和行业重要数据的跨境调取设置严格的审批程序,对其他数据的跨境调取,我国应在不损害数据主权与安全的前提下,尽可能尊重和承认他国的数据主权与正当请求。再者,我国法院应充分发挥跨国司法权,[55]在适用和解释具有域外效力的数据立法时遵循合理原则,在阐释相关法律的域外适用边界时对本国利益、他国利益和国际社会共同利益进行价值平衡。在承认与执行判决时,一方面可依据"市场主权"理论,借助境外主体对我国广阔数据市场的依赖,加强我国司法判决对境外主体的可执行性。[56]另一方面,应以多双边条约或互惠原则为依据,承认与执行外国法院依据具有域外效力的数据立法作出的判决。必要时利用管辖权审查和公共政策审查,阻却他国不当的域外司法管辖。

(三)多边层面:引领数据流动的多边规则构建和全球治理

国家间基于数据立法域外适用的法律冲突和博弈对抗最终将导致数据治理的碎片化和国际社会在虚拟网络空间的"无秩序状态"。因此,从长远来看,破解数据立法域外适用冲突的理想方案是,各国在多边层面达成共识、形成统一的数据治理国际规则体系。首先,国际贸易投资协定应作为数据跨境流动和个人信息保护的规制框架。数据跨境流动是开展数字贸易的前提,[57]但各国对数据跨境流动的限制性措施会产生域外适用效应,也可能构成贸易壁垒,最终阻碍数字贸易的发展。在全球化面临脱钩的背景下,强调数字自由贸易具有重要意义。尽管WTO协定目前尚无专门针对数字贸易的规定,但该路径奉行多边主义理念、以非歧视待遇为基石、具有规制协调和争端解决的权力与经验,有望开展最广泛融合国际主体和共性认知的数据流动治理。近年来,WTO正积极推进"电子商务联合声明倡议"的开放式诸边谈判,谈判成果有望基于最惠国待遇扩及WTO全体成员并最终达成多边化。[58]我国应在诸边谈判中发挥引领作用,以尊重各国数据主权为底线,以安全、自由的数据跨境流动为导向,以FTA的规则设计为借鉴,促进数据流动规制的国际协调。我国还应特别考虑发展中国家的诉求,为发展中国家和最不发达国家争取特殊但有区别的待遇,缩小数字鸿沟。

此外,对数据流动的规制和治理不能仅限于数字贸易维度。由数据流动引发的个人信息保护、国家安全、域外司法执法管辖等非贸易关切,需要各国在更广阔的平台探索构建数据流动的全球治理方案。中国一直以来是多边主义的践行者,坚定维护以联合国为核心的国际体系。[59]联合国框架下的信息安全政府专家组(UN GGE)和开放式工作组(OEWG)是讨论网络空间国际规则的重要平台。作为数据资源大国和负责任大国,中国关于保障供应链开放、稳定和安全的主张已被纳入UN GGE的共识性报告中。[60]中国可延续此路径向上述平台提出其他数据治理议题和推行中国方案。尽管短期内各国恐难达成规范性共识,但各国政府、国际组织和互联网企业可以在价值理念、基本原则层面等保持谈

判沟通和凝聚共识，携手推进数据流动的全球治理进程。

结语

随着数字经济与云计算技术的发展，世界各国基于数据主权和数据利益不断加大博弈的范围与强度。数据立法的域外适用已愈演愈烈，数据立法域外适用契合了国家的数据治理理念和数据规制需求，但立足国家本位的域外适用难免引发国家间的法律冲突。其中，立法冲突表现为广泛的管辖竞合，执法冲突削弱国家间的政治与法律互信和影响域外执法的可执行性，司法冲突体现为不同法域间的法律价值之争和判决的域外执行受阻。数据立法的域外适用一定程度上也涉嫌违反双边协定的国家合意与多边条约的目的宗旨，造成国内法与国际法的冲突。这主要与数字时代传统管辖权理论的式微、国际法协调数据立法域外适用冲突的规则赤字和国家利益与国际话语权的争夺有关。为有效解决数据立法域外适用引发的双层次法律冲突，中国应加快构建攻防兼备的数据立法域外适用制度。此外，以网络空间命运共同体思想为引领的国际合作机制是“化冲突为共赢”的根本出路。建议中国推动多双边司法协助条约的制定与升级，充分运用国际礼让原则处理域外执法与司法冲突，在以WTO为核心的国际贸易治理框架下推动数据跨境流动等议题的谈判，在联合国框架下引领和推进全球数据治理进程。

注释：

①唐巧盈，杨嵘均.跨境数据流动治理的双重悖论、运演逻辑及其趋势[J].东南学术，2022，(2).

②UNCTAD. Data Protection and Privacy Legislation Worldwide[EB/OL]. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

③目前学界尚无对国内法域外适用概念的统一界定，但上述概念得到较多学者的赞同。参见廖诗评.国内法域外适用及其应对——以美国发域外适用措施为例[J].环球法律评论，2019，(3)；孔庆江，于华溢.数据立法域外适用现象与中国因应策略[J].法学杂志，2020，(8)；刘宁，蔡午江.我国原子能技术出口管制规范域外适用研究[J].中国政法大学学报，2022，(1)；霍政欣.我国法域外适用体系之构建——以统筹推进国内法治与涉外法治为视域[J].中国法律评论，2022，(1).

④本文认为域外效力与域外管辖权虽在语义表达和表现形式上有所差别，域外效力关注静态的法律效力，域外管辖权关注动态的管辖权能，但两者均指一国对其管辖范围外的行为或事项进行规制的权限，包括立法规制权、行政规制权和司法规制权。因此，后文将按具体语境的需要交替使用这两个术语。参见霍政欣.域外管辖、“长臂管辖”与我国法域外适用：概念厘定与体系构建[J].新疆师范大学学报(哲学社会科学版)，2023，(2).

⑤黄惠康.准确把握“涉外法治”概念内涵 统筹推进国内法治和涉外法治[J].武大国际法评论，2022，(6).

⑥Dan Jerker B. Svantesson. The Extraterritoriality of EU Data Privacy Law-Its Theoretical Justification and its Practical Effect on U. S. Businesses[J]. Stanford Journal of International Law, 2014, (1)；俞胜杰，林燕萍.《通用数据保护条例》域外效力的规制逻辑、实践反思与立法启示[J].重庆社会科学，2020，(6)；叶开儒.数据跨境流动规制中的“长臂管辖”——对欧盟GDPR的原旨主义考察[J].法学评论，2020，(1).

⑦Adèle Azzi. The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation[J]. Journal of Intellectual Property, Information Technology and E-Commerce Law, 2018,(2)；何叶华.论数据保护法的域外效力[J].北京理工大学学报(社会科学版)，2021，(9).

⑧杨永红.美国域外数据管辖权研究[J].法商研究，2022，(2)；何叶华.论数据保护法的域外效力[J].北京理工大学学报(社会科学版)，2021，(9).

⑨Federico Fabbrini, Edoardo Celeste, John Quinn. Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty[M]. New York: Hart Publishing, 2021: 1～280.

⑩张哲，齐爱民.论我国个人信息保护法域外效力制度的构建[J].重庆大学学报(社会科学版)，2022，(5).

⑪Margaret Byrne Sedgewick. Transborder Data Privacy as Trade[J]. California Law Review, 2017,(5).

⑫石静霞.数字经济背景下的WTO电子商务诸边谈判：最新发展及焦点问题[J].东方法学，2020，(2).

⑬谭观福.数字贸易中跨境数据流动的国际法规制[J].比较法研究，2022，(3)；戴艺晗.贸易数字化与监管碎片化：国际贸易制度框架下跨境数据流动治理的挑战与应对[J].国际经济法学刊，2021(1)；石静霞，陆一戈.DEPA框架下的数字贸易核心规则与我国的加入谈判[J].数字法治，2023，(1).

⑭彭岳.数据隐私规制模式及其贸易法表达[J].法商研究，2022，(5).

⑮张生.国际投资法制框架下的跨境数据流动：保护、例外和挑战[J].当代法学，2019，(5).

⑯Neha Mishra. Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows[J]. Vanderbilt Journal of Transnational Law, 2019,(2).

⑰Andrew D. Mitchell & Jarrod Hepburn, Mitchell, Andrew D. and Hepburn, Jarrod, Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer[J]. Yale Journal of Law and Technology. 2017,(1).

⑱张新民,张稷锋.网络法域外适用的法理阐释:概念、逻辑与原则[J].太平洋学报,2022,(12);王燕.数据法域外适用及其冲突与应对——以欧盟《通用数据保护条例》与美国《澄清域外合法使用数据法》为例[J].比较法研究,2023,(1);孔庆江,于华溢.数据立法域外适用现象及中国因应策略[J].法学杂志,2020,(8).

⑲EDPB. Guidelines 03/2018 on the Territorial Scope of the GDPR (Article 3) [EB/OL]. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

⑳Lilian Mitrou. The General Data Protection Regulation: A Law for Digital Age?[A]. Synodinou T, et al. EU Internet Law: Regulation and Enforcement[C]. Switzerland: Springer cham, 2017: 32.

㉑U. S. Department of Justice. Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper[EB/OL]. https://www.justice.gov/opa/press-release/file/1153446/download.

㉒EDPB. Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR (Version 2.0)[EB/OL]. https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf.

㉓Christopher Kuner. Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law[J]. International Data Privacy Law, 2015,(4).

㉔金晶.作为个人信息跨境传输监管工具的标准合同条款[J].法学研究,2022,(5).

㉕宋晓.域外管辖的体系构造:立法管辖与司法管辖之界分[J].法学研究,2021,(3).

㉖单文华,邓娜.欧美跨境数据流动规制:冲突、协调与借鉴——基于欧盟法院"隐私盾"无效案的考察[J].西安交通大学学报(社会科学版),2021,(5).

㉗邵怿.论域外数据执法管辖权的单方扩张[J].社会科学,2020,(10).

㉘Permanent Court of International Justice, Series A: collection of judgments(1923~1930), The Case of the S. S."Lotus", France v. Turkey, pp. 18~19.

㉙Luke Irwin. Clearview AI Insists it isn't Subject to GDPR After Committing Several Privacy Breaches[EB/OL]. https://www.itgovernance.eu/blog/en/clearview-ai-insists-it-isnt-subject-to-gdpr-after-committing-several-privacy-breaches.

㉚Christopher Wolf. Impact of the CJEU's Right to Be Forgotten[J]. Maastricht Journal of European and Comparative Law, 2014,(3).

㉛Oreste Pollicino. Data Protection and Freedom of Expression Beyond EU borders-EU Judicial Perspectives[A]. Fabbrini F, et al. Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty[C]. New York: Hart Publishing, 2021: 90~96.

㉜Kurt Wimmer. Free Expression and EU Privacy Regulation: Can the GDPR Reach U. S. Publishers?[J]. Syracuse Law Review, 2018,(3).

㉝熊玠.无政府状态与世界秩序[M].杭州:浙江人民出版社,2001:3~4.

㉞《云法案》规定,在同时满足以下条件时,数据控制者可被免除披露境外数据的义务:(1)数据控制者合理地相信披露义务将会导致其实质性地违反"适格政府"的立法并因此产生法律冲突;(2)法院需综合案件总体情况和司法公正利益决定是否足以驳回或更改搜查令;(3)数据控制者合理地认为搜查令针对的目标不是美国人且不居住在美国。

㉟U. S. Department of Justice. Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper[EB/OL]. https://www.justice.gov/opa/press-release/file/1153446/download.

㊱U. S.-EU Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, Art. 5, 8, 18, 19; Paul M. Schwartz. Legal Access to the Global Cloud[J]. Columbia Law Review, 2018,(6); Eleni Kyriakides. The CLOUD Act, E-Evidence, and Individual Rights[J]. European Data Protection Law Review, 2019,(1).

㊲WTO Panel Report, United States-Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/DS285/R, para. 6. 285.

㊳彭岳.数字贸易治理及其规制路径[J].比较法研究,2021,(4).

㊴谭观福.数字贸易规制的免责例外[J].河北法学,2021,(6);张倩雯.数据跨境流动之国际投资协定例外条款的规制[J].法学,2021,(5).

㊵Anupam Chander, Uyen P. Le. Data Nationalism[J]. Emory Law Review, 2015,(3).

㊶宋杰.进取型管辖权体系的功能及其构建[J].上海对外经贸大学学报,2020,(5).

㊷Permanent Court of International Justice, Series A: collection of judgments(1923～1930), The Case of the S. S."Lotus", France v. Turkey, p. 18.

㊸United Nations General Assembly. Report of the International Law Commission-Fifty-eighth Session[EB/OL]. https://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

㊹Bruno Simma, Andreas Th. Müller. Exercise and Limits of Jurisdiction[A]. James Crawford & Martti Koskenniemi. The Cambridge Companion to International Law[C]. Cambridge: Cambridge University Press, 2012: 153～154; American Fourth Restatement of Foreign Relations Law, §404 & 405; Andrew Woods. Litigating Data Sovereignty[J]. Yale Law Journal, 2018,(2).

㊺ European Commission. An EU Strategy on Standardisation Setting Global Standards in Support of a Resilient, Green and Digital EU Single Market[EB/OL]. https://ec.europa.eu/docsroom/documents/48598; European Commission. A EU Strategy for Data [EB/OL]. https://eur- lex.europa.eu/legal- content/EN/TXT/?uri=CELEX％3A52020DC0066.

㊻监控资本主义(Surveillance Capitalism)是美国学者肖莎娜·祖博夫提出的一个政治经济学概念,其是指企业通过广泛监控和收集互联网用户数据、建立相应模型计算出用户商业和政治行为预期的“预期产品”,最终将“预期产品”出售获得经济利益和实现政治操控的商业模式。典型的监控资本主义企业包括美国的 Acxiom 公司、Google 公司和 Facebook 公司。在信息时代,监视资本主义企业已成为新帝国主义巩固全球霸权、强化金融垄断、打击竞争对手、传播意识形态的重要工具。See Shoshana Zuboff. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization [J]. Journal of Information Technology, 2015,(1);符豪.21 世纪美国左翼学者对监视资本主义的批判研究[J].马克思主义与现实,2020,(5).

㊼孙祁,尤利娅·哈里托诺娃.数据主权背景下俄罗斯数据跨境流动的立法特点及趋势[J].俄罗斯研究,2022,(2);邱静.数据规则的国内构建、国际竞争和协调[J].安徽师范大学学报(人文社会科学版),2023,(1).

㊽中国国家互联网信息办公室.数字中国发展报告[EB/OL].http://www.cac.gov.cn/2023- 05/22/c_1686402318492248.htm?eqid=f94447d600003c3500000003646d59b5#.

㊾《个人信息保护法》第3条、第38～43条、第66～71条;《数据安全法》第2条、第31条、第36条、第44～52条。

㊿习近平.高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告[EB/OL].http://www.news.cn/politics/cpc20/2022-10/25/c_1129079429.htm.

(51)赵精武.论数据出境评估、合同与认证规则的体系化[J].行政法学研究,2023,(1).

(52)国际礼让原则是国际私法领域的一项基本原则,但其内涵具有灵活性和不确定性。一般是指一国对外国政府行为的认可,和一国主动限制国内法的域外适用以尊重他国主权利益。国际礼让原则的适用主要体现为承认外国国家主权豁免、承认与执行外国法院的判决等。一国法院适用国际礼让原则时会对本国利益与外国利益进行权衡判断。参见曹亚伟.国内法域外适用的冲突及应对——基于国际造法的国家本位解释[J].河北法学,2020,(12).

(53)张新民,张稷锋.网络法域外适用的法理阐释:概念、逻辑与原则[J].太平洋学报,2022,(12).

(54)中国与东盟国家已建立起警务合作机制共同打击跨境电信网络诈骗犯罪。参见王立梅.论跨境电子证据司法协助简易程序的构建[J].法学杂志,2020,(3);梁坤.我国跨境刑事电子取证制度新发展与前瞻[J].中国信息安全,2021,(5).

(55)霍政欣.论全球治理体系中的国内法院[J].中国法学,2018,(3).

(56)王雪,石巍.个人数据域外管辖权的扩张及中国进取型路径的构建[J].河南社会科学,2022,(5).

(57)谭观福.数字贸易中跨境数据流动的国际法规制[J].比较法研究,2022,(3).

(58)石静霞.世界贸易组织谈判功能重振中的“联合声明倡议”开放式新诸边模式[J].法商研究,2022,(5).

(59)习近平.高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告[EB/OL].http://www.news.cn/politics/cpc20/2022-10/25/c_1129079429.htm.

(60)Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security[EB/OL]. https://front.un- arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf;Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security[EB/OL]. https://front.un-arm.org/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.