欧盟 GDPR 域外管辖冲突下的中国应对路径

吴诗怡[1]，刘梓峥[2]

1 澳门科技大学法学院，787383247@qq.com
2 澳门科技大学法学院，juzi96180@gmail.com

摘要：当前，数据立法呈现出显著的域外适用趋势，成为各国扩张网络主权、争夺数据治理话语权的核心手段。然而，这种管辖权的域外扩张难免触及他国主权边界，引发国家间在立法、执法及司法层面产生冲突风险。欧盟 GDPR 以“功能住所”和“主观意图”为核心的域外管辖标准不仅给中国出海企业带来双重合规困境，更对中国的网络主权构成了直接挑战。冲突的根源在于，传统管辖权理论的失灵、国际法协调机制的缺位以及各国数据主权模式异化。为此，中国亟须构建“能动回应型”的数据立法域外适用体系。在强化外国法不当域外适用的阻断机制的同时，应完善国内法与国际法的转化和衔接，以维护国家主权、安全和发展利益。

关键词：域外数据管辖，域外适用，GDPR，网络主权

1 引言

随着全球数据跨境治理格局以碎片化态势发展，网络空间已成为与大国多元化博弈的重要领域，习近平总书记多次强调“尊重网络主权”。当前，欧盟 GDPR 不断拓展的域外管辖边界，对中国网络空间的主权安全及企业“走出去”形成了挑战。面对欧盟 GDPR 可能造成的现实冲击，国内研究普遍认为，我国应完善数据立法，加强数据主权治理[4]。此外，还有学者建议我国推动双多边数据跨境流动条约的制定与谈判[5]。然而，现有研究鲜少关注我国数据法域外管辖体系的不足与完善。

党的二十届四中全会通过的《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》指出，深化网络空间安全综合治理，加快国家网络安全防御体系建设。基于此，在网络主权冲突日益加剧的背景下，探讨中国现有的数据管辖规则如何应对欧盟数据立法域外适用的扩张具有重要意义。鉴于此，本文剖析中国与欧盟因域外数据管辖模式差异引发的法律冲突及成因，立足于国家安全观提出应对域外数据管辖冲突的中国方案，以期为全球数据跨境流动治理提供中国范式。

2 中欧域外数据管辖的冲突问题

当前，欧盟与中国均确立了各自的数据法域外适用机制。欧盟 GDPR 第 3 条确立了其对特定数据处理活动的管辖权，GDPR 第 48 条通过控制数据跨境传输渠道，间接约束第三国数据接收。中国通过出台《中华人民共和国个人信息保护法》（以下简称“个保法”）《中华人民共和国网络安全法》（以下简称“网安法”）《中华人民共和国数据安全法》（以下简称“数据安全法”），实现了对跨境数据法律适用体系的初步构建。虽然中国与欧盟在数据法制度设计上总体有相似之处，但在管辖依据、执法方式和合规路径层面仍存在显著差异，这将造成法律适用冲突。

作者简介：吴诗怡，澳门科技大学法学院博士研究生，研究方向为国际法。
刘梓峥，澳门科技大学法学院，研究方向为国际法。

2.1 管辖依据比较：法人住所 vs 功能住所

首先是连结点认定的不同：GDPR 第 3 条明确只要数据控制者在欧盟境内的办事机构存在某种稳定的、真实的商业活动，即便其注册地在域外，欧盟法亦可适用。可见，此种标准的认定极具柔性：既不以法律人格为前提，亦不以注册为要件。相较于欧盟，中国对数据处理行为发生地的连接点认定具有强地域性特征，其以注册地、办事机构所在地为主。这延续了中国传统民商法“法人住所”理论，根据《民法典》第六十三条及相关商事法律，法人的住所地为其主要办事机构所在地，注册地是确立管辖的首要形式标准。这意味着，只要企业在中国注册，即无条件受辖。而欧盟的连接点彰显“功能住所（Functional Domicile）”理论特色，针对数据控制者的监管需要穿透公司法的注册面纱，公司住所是否处于欧盟领土内不是构成连接点之必要，决定性因素在于是否有通过稳定安排进行的“真实有效活动”。上述两种连接点认定的差异必然导致中欧数据管辖权产生冲突。

其次是管辖触发条件的不同：欧盟 GDPR 第 3 条采用主观意图标准，规定境外控制者或处理者存在向欧盟数据主体提供商品或服务的主观意图或监控其行为的，即受 GDPR 管辖[1]。这本质上是将服务自由的市场准入逻辑延伸至跨境数据流动领域，欧盟法的管辖范围取决于行为人在客观上是否呈现出服务欧盟市场的主观意愿，例如使用欧盟语言。《个保法》第三条采用了与 GDPR 相似的表述：“以向境内自然人提供产品或者服务为目的的数据处理活动适用本法”。但从司法实践来看，《个保法》注重客观结果，无需主观意图。以 2023 年广州互联网法院审理的“万豪酒店集团个人信息跨境传输案”为例：法国总部酒店集团通过 App 向中国用户提供服务，收集并跨境传输个人信息用于全球营销。中国原告起诉侵权，法院认定该行为因客观上发生了“向境内自然人提供服务”的行为事实，且产生了隐私侵害效果，故依照《个保法》规定判决被告赔偿并删除数据。由此观之，中国数据法的管辖模式彰显“效果原则”的色彩，即境外处理若在中国境内产生实质效果或影响，则触发中国法管辖。

GDPR 第 3 条第 1 款通过借助属人原则的解释弹性，将“最低限度联系”无限扩大，弥补传统属地原则在数据跨境场景下的适用短板。GDPR 第 3 条第 2 款则使管辖权连接点不再局限于欧盟境内的实体，而是直接延伸至各类第三国在线服务提供者，包括电子邮件服务商、搜索引擎及网络平台等，从而实现数据管辖权的域外扩张。实践中，同一处理行为可能同时落入 GDPR 与《个保法》适用范围。一方面，中国监管机构倾向于限制数据的自由出境，强调数据主权与国家安全，要求部分数据必须存储于境内或通过严格审批才可流出；另一方面，欧盟则通过高标准的权利保护机制限制数据向未被认定为具有“充分保护”的第三国传输，尤其关注个人数据权利是否能够在接收国得到有效实现。企业因此陷入一种“合规悖论”境地：将欧盟数据传回中国，可能违反 GDPR 对数据传输的限制；把在中国收集的必要数据留存于欧洲，又可能抵触中国的数据本地化要求。更严峻的是，欧盟监管机构在实践中可能进一步质疑中国现行法律体系对隐私和人权的保护程度，从而直接援引 GDPR 中的阻断条款禁止数据向中国流动。

2.2 合规路径比较：国际协议优先 vs.行政审批优先

为限制第三国公权力行为的过度域外适用，GDPR 第 48 条规定，第三国只有基于欧盟或成员国与该第三国之间生效的国际协议，才能要求欧盟境内的数据控制者披露数据，但这不妨碍 GDPR 中针对数据传输的充分性认定、适当保障措施、特定情况例外等监管要求的适用。这条规定为欧盟拒绝承认与执行外国法院或行政机关的数据调取令提供了明确的合规依据，有利于避免受 GDPR 第 3 条管辖的企业盲目遵守外国法律义务而损害欧盟数据主权。实践中，当一个跨国企业同时受到来自欧盟和母国的数据法双重管辖时，第 48 条通过阻隔企业向其母国政府无条件传输数据的路径，迫使这些企业成为游说力量，推动其母国政府与欧盟签订双边或多边协议来解决数据共享问题。在地缘政治博弈加剧的背景下，GDPR 第 48 条明确否认了非欧盟司法裁决或行政决定在欧盟境内的适用，强调通过国家外交取得的协议在跨境数据传输中的优先性，实际上

与第 3 条协同形成了一种阻断路径，使得欧盟能够有效抵御美国的《云法案》，重塑全球建立一种基于相互承认和国际条约的数据调取新秩序。

相较于 GDPR 的依赖国际协议路径的自动排他性模式，中国企业执行外国数据调取令的合规路径为取得主管机关的行政许可。《数据安全法》第三十六条规定，中国境内的组织、个人在执行外国司法或者执法机构的调取令前，必须经过中国主管机关根据相关法律、国际条约或平等互惠原则批准。换言之，发布数据调取令的外国政府即便与中国不存在双边或多边条约，只要获得中国网信办审批也可执行数据传输。这种行政审批优先的模式核心在于将数据出境的决策权从“企业自决”上升至“国家管控”，体现了我国对企业向境外提供数据的风险防护，同时也给企业留出了灵活操作的合规空间。与欧盟直接通过立法排除非协议国数据调取令效力的模式不同，我国没有直接一概否定外国数据调取令的效力，而是将合规裁量权交给主管机关，根据案件具体事实结合国际法原则逐一审查，有利于满足我国总体国家安全观的实际需求。

2.3 执法方式比较：“一站式”投诉机制 vs.阶次式处罚

针对跨境数据处理活动，GDPR 为数据主体建立了“一站式”的救济程序。首先，GDPR 要求各欧盟成员国设立独立的数据保护监管机构以负责在本国执行 GDPR。为更好地保障人权，当数据控制者不当处理欧盟公民的个人数据时，数据主体可直接向其居住地所在国的数据保护监管机构投诉。居住国数据监管机构作为主导机关负责统筹调查与沟通，其可要求数据控制者所在国的数据保护监管机构参与调查并提出意见，最后双方针对投诉共同做出解决方案。若各国监管机构对解决方案存在分歧，欧洲数据保护委员会介入协调并作出有约束力决定。最后，由主导机关发布终局决定，确保该决定在相关成员国得到统一适用与执行。GDPR 对数据主体的救济保障依赖于多方监管机构之间的密切协作，一站式机制具有清晰的递进式监督层级。

中国当前在数据处理活动采取以国家网信办牵头，网信办与公安协同配合的分级同步执法模式。对于在我国境内没有设立机构的数据处理主体，我国规定其应当在境内设立专门代表机构或者委托境内相关机构代为承担合规义务，配合我国监管部门开展调查。针对不正当的数据处理活动，与欧盟强硬的直接罚款手段相比，中国的执法更为柔性与具备可预期性。根据 2025 年国家互联网信息办公室出台的《网信部门行政处罚裁量权基准适用规定》，网信部门行政处罚裁量基准划分为不予处罚、减轻处罚、从轻处罚、一般处罚、从重处罚等裁量阶次，明确了各阶次处罚的具体适用情形。在对个人信息处理者作出行政处罚之前，会先进行约谈整改等行政指导。若整改不到位，网信部门应根据网络运行安全、网络信息安全等不同类型违法行为向个人信息处理者问责，其中可处以没收违法所得、最高一千万元人民币罚款；情节严重的，还可责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。相比之下，GDPR 对违规行为处罚力度更大。欧盟国家数据保护监管机构可对违反 GDPR 的数据控制者处以最高可达 2000 万欧元或上一财政年度全球营业额 4%的罚款，且无需经过约谈整改的前置程序即可直接启动处罚程序，整体执法更侧重威慑力。这种差异的本质，源于中欧对数据监管价值目标的不同定位：欧盟侧重通过刚性统一执法打造欧盟单一数据空间，保护公民数字人权；中国则以合规引导为优先，在维护数据安全与个人信息权益的同时，也通过前置约谈整改程序给企业经济发展留了空间。

3 域外数据管辖权的冲突根源

3.1传统属地管辖的失灵

传统国家管辖原则由属地、属人、保护及普遍管辖共同构成，其中属地管辖原则居于重要地位，即各国一般依托物理空间的地域关联来划定其国内法的效力边界。然而，数据作为数字时代的核心生产要素，其具有区别于传统规制对象的独特属性。首先，数据的无形性与可复制性使其无需依附于特定物理载体，可在瞬间被无限复制并横跨多个法域[2][20]；其次，跨境数据流动的即时性使网络传输可在毫秒间逾越国界，传统边境管控手段难以有效拦截[3]；最后，云计算技术使

数据的实际存储地、处理地与其控制者所在地经常处于相互分离状态。

数据的“去地域性”极大地削弱了数据物理位置的稳定性。若沿用传统理论——即以物理在领土内具有稳定且可识别的物理节点作为管辖基础,那么数据的存储或处理地往往并非与数据侵权行为或数据传输合同存在最密切联系的地域。尤其是在侵害中国公民个人信息权益的行为或损害中国数据安全的数据处理活动发生于境外的情形下,若固守严苛的属地管辖,将导致主权国家无法对其利益实现有效保护。

在此背景下,数据流动的弥散性决定了法律适用存在不确定性,理论上数据流动过程中途经的任一节点国家都可主张管辖权。由此,各国开始在传统管辖理论基础上,通过强化数据出境监管,衍生出一种更具进取性的管辖权体系[6]。近年来西方国家单方扩张其数据立法适用范围,不仅加剧了国家间的不信任,还诱发了各国的“跟风立法”,进而造成了全球范围内管辖权冲突的泛滥。

3.2 数据主权模式差异

在数字经济时代背景下,各国依据其自身的治理方针、价值观及政策偏好对数据主权边界及行使路径作出不同主张,使得跨境活动中同一份数据往往同时承载着多重主权意志,进而演变为一场关于网络空间控制权的竞争。中欧域外数据管辖权冲突根源之一在于数字经济时代背景下国家之间不同主权模式的相互博弈。

3.2.1 欧盟:基于人权的“规范壁垒”模式

欧盟率先进行数据保护立法,其目标在于把 GDPR 中的“域外适用”“充分性认定”等新型制度设计“外溢”为国际规则,将其数字人权理念和人格尊严法理嵌入国际规范框架,形成“布鲁塞尔效应”。GDPR 通过广泛的域外管辖将欧盟的数据保护标准向全球输出,迫使外资企业在进入欧盟市场时必须按照 GDPR 的要求调整自身的处理规则。这种模式突破了传统领土主权的管辖边界,试图在全球范围内建立一套以欧盟规则为核心的数据治理秩序,从而塑造他国政府与企业的行为选择。当面对来自外国当局的数据调取压力时,欧盟不仅依靠 GDPR 第 48 条等禁令机制限制数据出境,更通过《阻断条例》强制要求境内主体抵制外部法律的单边适用[19]。近年来,欧盟还通过《数字服务法案》和《数字市场法》扩张对数字平台的监管,进一步使欧洲规范外溢为制度力量。

3.2.2 中国:国家安全观的“消极型防御”模式:

中国是严格的数据主权国家,其以国家安全与发展为导向,通过《数据安全法》《个保法》为产生损害中国境内安全效果的境外数据活动提供了保护性管辖权基础。中国主张与公民相关的所有数据都须存储于境内的服务器,这一模式要求在境内的大部分数据需满足出境安全评估才能向境外流动,并加以《阻断外国法律与措施不当域外适用办法》(以下简称“阻断办法”)来应对外国法不当域外适用。中国数据治理对内实施中央集权式监管,由网信办统筹,多部门协同执法;对外推行《全球数据安全倡议》,主张各国不干涉他国数字治理事务,反对滥用技术手段进行数据获取与监控。通过“一带一路”合作机制,中国协助沿线国家建立本地数据中心、提供云计算基础设施,并输出其推动“数据本地化”的基本立场[22]。与欧盟不同,中国的防御性管辖体系不主动谋求对境外数据处理活动的管辖,有利于捍卫国家数据安全与个人信息权利,但在促进数据流动经济发展和对他国友好程度方面有待优化。

3.3 国际法协调工具的缺失

依据 1927 年“荷花号案”判决,只要国际法未明确禁止,国家便拥有以其意志发展国内法域外适用规则的自由。然而,这种主权扩张并非毫无节制,国内法的域外适用理应考虑到实际联

系原则、反域外适用推定原则以及国际礼让原则[20]。尽管联合国相关专家组的报告亦已明确《联合国宪章》对网络空间的适用性[23]，但在各国数据立法竞相扩张且冲突频发的背景下，当前国际层面缺乏具有协调作用的专门性条约，构成了数据法域外适用冲突的核心诱因之一。

除国际条约缺失之外，当前数字贸易国际规则也呈区域化发展。现有数字贸易协定多呈现出区域性特征，这与数据本身的“去地域性”存在天然冲突。虽然 USMCA、CPTPP、RCEP 等区域性协定普遍确立了以数据跨境自由流动为原则、本地化为例外的规制进路，但在关键议题上缺乏一致的共识。以政府跨境数据调取为例，RCEP 第 8.2 条以宽泛的“安全例外”条款允许成员国对数据流动施加限制；CPTPP 第 14.11 条规定成员国可在遵守透明度与比例性原则的前提下实施数据本地化措施。这种“以区域规则治理全球数据”的趋势，非但未能建立起统一的国际秩序，反而增长了数据保护主义的扩张空间[21]。

同样的局限性也体现在多边贸易体制中。WTO 在 2026 年喀麦隆举行的第 14 届部长级会议上达成的《电子商务协议》（E-Commerce Agreement）中，首次推出了数据跨境流动的国际标准，并提出建立跨境消费争议解决机制与强制披露数字贸易监管措施。其中第 19 条虽禁止将计算设施本地化作为市场准入条件，但对“变相本地化措施”未作解释，实质上允许成员国以“国家安全”为由实施缺乏透明度的数据出境审查限制，这极易形成规则漏洞[9]。在大国数据主权博弈加剧的局势下，协议的执行机制因美国、印度等关键经济体的缺席面临停摆风险。更为根本的是，WTO 规则对数据主权的约束力本身有限：数据跨境流动虽被纳入服务贸易总协定（GATS）框架下“电信服务”或“计算及相关服务”范畴，但 GATS 第 14 条之二（安全例外）与第 14 条（一般例外）均允许成员基于“公共秩序”“国家安全”例外条款来实施限制性措施，从而扩张域外数据管辖，阻碍数据跨境贸易自由的实现。

4 数据管辖冲突下的中国制度反思

近年来，为应对外国数据立法域外适用扩张，中国已构建起以《个保法》《网安法》《数据安全法》为核心，以《阻断办法》等配套规则为补充的数据治理框架。然而，面对欧盟 GDPR 适用的扩张态势，中国现有数据法律体系短板逐渐显现，具体有以下表现：

4.1 数据域外管辖标准不一致

中国域外数据管辖权的体系构建已有雏形，但数据管辖规则内部存在逻辑矛盾。《个保法》第三条第 2 款采用“目的导向型管辖”，以“向境内自然人提供产品或服务”或“分析评估境内自然人行为”作为域外适用的实质连结点；而《数据安全法》第二条则采“效果导向型管辖”，聚焦数据活动对国家安全和公共利益的“实质影响”。两者分别确立的“境外处理境内数据”与“境外活动影响境内”域外适用标准，实质构成域外管辖权行使的双重路径依赖，造成“意图标准”与“效果原则”的体系性冲突[9]。

其次，《网安法》第二条采用“建设、运营、维护和使用网络”的概括性表述与《个保法》第三条第 2 项的清单式规范形成鲜明对比，加剧了法律适用的不确定性。实践中，这一差异将迫使企业在跨境数据事务中需依照两部法律预备不同的合规方案，无形中给企业合规造成双重负担[10]。此外，《个保法》第三条第 2 项为兜底条款，赋予立法机关灵活调整空间。此标准的优势在于主动防范境外数据滥用，保护公民隐私权，但也可能引发与 GDPR 的适用摩擦，需要通过双边协议缓解。

最后，中国数据法在关键概念的界定上仍有欠缺。不同于 GDPR 将数据处理主体分为数据控制者与数据处理者来便于分配法律责任，《个保法》没有针对“个人信息处理者”做出类型化区分，且“自主决定处理目的、方式”的界定标准缺乏操作性指引。界定不明易引发角色混同，可能致使平台内第三方开发者、数据清洗服务商等边缘主体均被不当纳入责任范围。加之目前司法实践中存在个人信息与数据概念混淆的现象，个人信息的泛化保护加剧个人信息处理者受到宽

泛解释，从而给企业造成连带问责的滥化，阻碍企业行使数据权益[11]。

此外，《个保法》第三条中的“境内自然人”是否包含偶然出现在我国境内的自然人，即“偶发性存在”（fortuitous presence）是否构成管辖基础，如短期入境旅客的数据处理是否适用本法。作为兜底条款的“其他情形”应当符合哪些具体条件未详细说明，该条款潜在被行政机关在数据出境审查中滥用的风险。《数安法》第二条中“国家安全”概念的范围不明易引发外国对中国援引“国家安全”例外条款正当性的质疑。

4.2 国际法的转化不足

当前中国数据法制度设计主要着眼于对境内数据的治理和监管，而相对忽视对国际公法的转化和援引。中国作为《维也纳条约法公约》与《数字经济伙伴关系协定》（DEPA）的缔约国，应当严格遵循《维也纳条约法公约》所确立的条约法规则，切实履行 DEPA 项下的条款义务[11]。然而，当前中国数据保护法律文本中尚未援引《维也纳条约法公约》第二十七条所明确的“条约必须遵守”原则，也缺乏类似 GDPR 序言第 23 段对履行国际条约义务作出清晰的承诺。这可能导致中国在主张数据法域外效力数据法时，因为缺乏对条约义务的转化而遭受国际社会的质疑，从而得不到其他国家的认可和执行[12]。

DEPA 与中国现行数据立法存在规范张力。DEPA 第 4.4 条规定成员国有权制定本国的数据监管要求，但禁止成员国强制要求企业把服务器或数据计算设施设置于本地。中国虽未在法律文本上明确对立 DEPA 的“禁止强制本地化”原则，但《个保法》第三条通过“效果管辖”将境外企业向中国公民提供服务为目的处理境内个人信息的行为纳入规制范围，这可能迫使企业为满足合规要求而主动在境内增设服务器或数据中心，形成与 DEPA 规则冲突的“间接本地化”效果。

在《区域全面经济伙伴关系协定》（RCEP）框架下，成员国不得以计算设施本地化作为市场准入条件。这与《网安法》第三十七条明确关键信息基础设施运营者的重要数据需境内存储的要求构成冲突。即使中国可援引 RCEP 框架下的“安全例外”条款为本地化措施抗辩，但由于该条款的适用标准极为严格，要求相关措施必须符合保护其基本安全利益所必要，且不得构成任意或不合理的歧视或变相贸易限制[13]。在实践中，中国对关键信息基础设施的宽泛界定易被质疑为“过度限制数据流动”，构成变相贸易壁垒。

从争端解决机制角度分析，DEPA 虽构建了完整的争端解决程序，包括磋商、专家组裁决和上诉审议等环节，但在当前地缘政治风险加剧背景下，中国通过 DEPA 争端解决机制解决数据监管冲突仍受制于多方因素：一是 DEP 成员数量有限，不足以覆盖中国主要的数据贸易伙伴；二是争端解决机制的裁决执行依赖成员国的政治意愿，各成员国往往难以达成共识。相较之下，RCEP 争端解决机制虽覆盖范围更广，但其裁决面临上述同样的执行困境，尤其是涉及“安全例外”条款的争议往往被提交至专家组裁决，效率较低且成本高昂。

4.3 阻断机制效力有限

中国为企业拒绝向外国提供数据提供了《阻断办法》作为合法依据，但阻断机制在实践中的效力却仍受到多重因素制约[7]。首先，《阻断办法》为部门规章，法律位阶低且关于“禁令”适用情形及约束对象的程序规则与执法案例不足[14][10]。在合规判断标准上，缺乏对“不遵守”外国制裁的界定标准。从企业救济机制来看，豁免与索赔制度仅具框架性，申请渠道、评估标准、管辖安排等关键规则有待细化[2]。中国《反外国制裁法》为应对单边制裁提供了反制工具，但其更多侧重于政治外交层面的宏观反击，缺乏与日常数据监管执法的微观衔接。例如，网信部门在处理跨境数据违规时，能否直接援引该法进行反制？需要哪个层级的审批？与《数据安全法》的关系如何协调？与《阻断办法》的反制规定如何衔接？这些操作性问题均未解决[15]。此外，《阻断办法》与《反外国制裁法》都具备阻断条款，二者为上下位法关系，可能存在衔接不畅的问题。

《阻断办法》超出《反外国制裁法》范围规定的豁免制度，能否解释为《反外国制裁法》第十三条中的“其他必要的反制措施”尚存疑问[16]。

5 中国应对数据域外管辖冲突的完善路径

5.1 重塑能动回应型的数据管辖体系

为有效应对外国数据治理规制的挑战，中国亟须基于数据主权理论，构建出一套兼具制度弹性和价值理性的“能动回应型”数据管辖体系。

在立法层面上，中国首先应当针对《数安法》《个保法》《网安法》的适用条款展开相应的修法工作，以确立统一的数据域外管辖标准。具体而言，应引入实质联系原则、效果原则及比例原则作为核心管辖标准。其中，实质联系原则强调数据处理活动与中国境内有实质性的直接客观联系，对此，可对实质联系测试采用量化标准，如数据处理行为与境内实体间的经济利益关联度、数据跨境转移频次等。效果原则则关注数据处理活动对中国境内产生的实际影响，建议为之建立负面影响的定量评估模型。其次，明确管辖权应优先归属于与数据之间具有最密切联系国家的。通过综合考量数据主体在境内的机构设置、用户规模、特性数据活动强度以及境内用户访问数的可及性等因素，运用比较分析法识别出与数据流动行为具有最显著利益关联的法律来予以适用[10]。

在行政层面上，主管部门应进一步规范跨境数据的监管细则。首先，由中国网信办及地方政府加快制定细化数据域外管辖各执行环节的具体期限和技术办法。例如，明确执法机构的职能权限、执行期限与技术标准的配套细则。其次，针对“境外数据控制者”与“国家安全”等关键概念界定问题，国家互联网信息办公室应通过制定《个人信息处理者识别指南》来对境外个人信息处理者的数据控制权进行规范引导，同时出台《国家安全影响评估技术规范》等标准明晰国家安全的涵盖范围。最后，政府机关应增设数据跨境业务的系统化合规培训与政企协同机制，具体可邀请熟悉数据法律法规的商务部、外交部专家和从事涉外合规业务的律师定期开展讲座，引导民营企业及科研机构深化对数据出境合规的认知，协助企业降低因触发多重数据管辖权带来的合规成本与风险。

在司法层面上，我国应积极推进国际司法协助合作。在设立“数据主权豁免”机制的基础上，个案审查外国政府机关基于司法管辖权提出的数据调取请求，对不实质侵犯数据主权的数据调取予以原则性认可。同时，大力发展联邦学习、区块链技术等新兴技术在跨境数据传输中的安全保障作用，与外国政府共同构建可信的跨境数据访问平台，以实现数字化司法证据在跨境调取中的互认互信[8]。

5.2 增强外国法不当域外适用的阻断机制

为化解他国法律不当域外适用给企业带来的合规困境，中国亟须从立法上加强对他国单边调取数据行为的防御性阻断，拓展企业救济途径[17]。

首先，中国应尽快出台最高法层级的《阻断法》，提高阻断机制的法律位阶。该法应明确将外国数据法不当域外适用所涉及的证据开示纳入阻断范畴，并借鉴欧盟《阻断条例》中第 5 条赋予企业起诉追偿权、第 6 条设置“合规冲突豁免”程序的相关规定[11]。在《阻断法》中确立“追偿条款（Clawback Clauses）”，准许因外国滥用数据法域外效力规则而遭受损失的中国自然人、法人或者其他组织在国内法院起诉并要求赔偿，并为被迫合规的企业设定明确的行政豁免机制[12]。为确保阻断机制的高效落地，中国应进一步细化阻断机制的实施细则。具体可构建“禁令发布 – 企业申报 – 部门审查 – 司法确认”的全链条工作流程，限定商务部门需在 30 日内作出初步裁定；设置梯度化处罚标准，对故意违反阻断令的企业处上年度营业额 20%罚款，对被迫合规企业则适用合规承诺制度。此等制度设计既可对接 CPTPP 关于“监管一致性”的要求，亦符合《维也纳条约法公约》第二十六条“善意履行”原则的规范期待。此外，还应强化阻断机制与

司法程序的衔接，赋予法院依职权启动阻断审查的权力，并配套《民事诉讼法》下的临时禁令措施[11]。

在数据领域司法协助层面，中国应基于国家主权平等原则，为友好国家搭建跨境数据调取的“绿色通道”。根据不同数据种类的敏感程度，探索类型化的调取路径。在严格监督企业落实数据安全合规的同时，适度放开对非敏感数据的跨境调取监管，着重加强对敏感数据、重要数据及核心数据跨境调取行为的安全监测和把控。另一方面，应基于多双边条约或互惠原则，合理承认与执行外国法院依据其数据立法作出的判决。但在执行过程中，必须坚守管辖权审查和公共政策审查底线，对他国不当的执法行为实施精准阻却[8]。

5.3 强化国际规则适配

数据域外管辖的实现仍需高度重视国内法与国际法范式的转化与协同。我国现阶段数据法域外适用体系缺乏对“国际礼让原则”“合理管辖”“比例原则”的规范体现，以及我国“数据本地化存储”的法律框架如何与所签订的 DECA、RCEP 等区域贸易协定实现衔接尚未有明确的规范回应[3]。具体制度的完善可循以下三条路径展开：首先，参考欧盟 GDPR 第 48 条的“国际礼让分析”（comity analysis）机制，引入国际礼让原则并明确在不损害我国及他国主权安全与平等的前提下，允许满足利益衡量测试基准的外国政府或个人请求调取存储在我国的数据。其次，为数据本地化政策提供更为灵活的机制安排，建议立法把“合理管辖”“比例原则”转化进数据域外管辖及出境安全评估条款中并制定量化适用标准。对此，可进一步根据重点行业类型细化不同数据的出境审查程序予以差异化管辖，避免“一刀切”的监管困境[18]。再者，我国应探索“数据主权豁免”抗辩机制，以便为应对涉及数据争议的国际纠纷提供正当性基础。对此，可借鉴《承认及执行外国仲裁裁决公约》第五条的“公共政策保留”条款，秉持审慎务实的原则，制定数据主权豁免的司法审查标准。

最后，中国应重视国内跨境数据流动监管措施与区域贸易协定的适配，应保证数据本地存储要求和数据出境监管的实施须与区域贸易协定相协调。对此，中国可依据 RCEP 和 DEPA 协定下的标准订立数据出境负面清单，规定透明度条款、非歧视条款，并明确安全例外条款的适用范围[7]。在国际法层面上，中国可积极推动 WTO 组织成员国就跨境电子商务协议达成更多共识。在参与国际数字经贸协定的谈判工作中，应就例外条款的适用范围、数据跨境流动规制措施的豁免条款及跨境数据合作执行等议题进行积极推动，致力于促进数据流动规制的国际协调[6]。

6 结语

面对欧盟数据域外管辖权扩张带来的挑战，我国的数据立法域外适用效力相对有限，容易因跨境数据传输与欧盟成员国发生主权冲突。数据跨境流动领域的主权竞争，既是技术层面的较量，也是制度的博弈。针对跨境数据流动安全问题，我国首先应继续秉持开放思维，大力发展联邦学习、人工智能大模型、区块链等技术在数据跨境传输中的应用。其次，出台更多数据相关立法、司法及行政实践，以期引导“走出去”企业依法经营、防范风险。最后，我国应积极推动制定中欧数据双边协议以及国际倡议等多边机制，创新数据跨境治理范式。

参考文献：

[1] 马光.我国跨境数据传输规则与国际规则的协调研究[J].中国政法大学学报,2024,(02):227-239.
[2] 马光,毛启扬.单边制裁与阻断立法下中国企业的合规困境与应对策略[J].武大国际法评论,2023,7(02):17-37.
[3] 马新民.中国条约法律制度与法律外交实践[J].国际法研究,2025,(06):3.

[4] 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, 41 (8): 76-88.
[5] 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): 187-200.
[6] 文淑.数据立法域外适用引发的法律冲突与中国解决方案[J].云南师范大学学报（哲学社会科学版）,2023(06):97.
[7] 安子健.数据法律冲突中适用国际礼让原则的理论基础、实践应用与中国镜鉴[J].河北法学,2024,42(05):164-182.
[8] 刘晗.何谓数据主权?——全球数字规则博弈中的弹性主权视角[J].北京大学学报(哲学社会科学版),2025,62(06):115-126.
[9] 刘晓春.阻断外国法律域外适用的中国实践[J].法学家,2020,(03):56.
[10] 宋云博.DEPA 个人信息跨境流动的规则检视与中国法调适[J].法律科学(西北政法大学学报),2024,42(01):135-144.
[11] 陈东阳.论单边跨境数据调取中的管辖权冲突[J].南大法学,2023,(02):103-117.
[12] 张鹏.我国阻断法的适用难点与完善路径[J].法治现代化研究,2024,8(06):63-77.
[13] 林福辰.外国数据法效力的域外扩张与中国范式研究[J].四川师范大学学报(社会科学版),2024,51(05):59-68+201-202.
[14] 贺嘉.我国数据立法中域外效力条款之解构[J].上海法学研究,2022,22:21.
[15] 赵自轩,杨泓桢.企业数据保护之不足与完善——以《深圳经济特区数据条例》为例[J].民商法争鸣,2024,(23):51.
[16] 高智华,李启文.美国法不当域外适用的中国应对策略探索[J].西南石油大学学报(社会科学版),2024,26(02):114-122.
[17] 袁康,赵宛如.跨境数据流动中的管辖权冲突及其协调[J].重庆邮电大学学报(社会科学版),2024,36(02):66-76.
[18] 梅傲,李淮俊.论《数据出境安全评估办法》与 DEPA 中数据跨境流动规则的衔接[J].上海对外经贸大学学报,2023,30(02):62-72.
[19] 廖斌,刘敏娴.数据主权冲突下的跨境电子数据取证研究[J].法学杂志,2021,42(08):147-161.
[20] EICHENSEHR K E.Data Extraterritoriality[J].Texas Law Review,2017,95:145-160.
[21] JOHNSON D R,POST D.Law and Borders--The Rise of Law in Cyberspace[J].Stanford Law Review,1996,48(5):1367-1402.
[22] RYNGAERT C,TAYLOR M.The GDPR as global data protection regulation?[J].AJIL UNBOUND,2020,114:6-9.
[23] WATT H M.Private International Law Beyond the Schism[J].Transnational Legal Theory,2016,2(3):347-427.

China's Response Path under the EU GDPR Extraterritorial Jurisdiction Conflict

Wu Shiyi[1], Liu Zizheng[2]

1 Faculty of Law, Macau University of Science and Technology, 787383247@qq.com

2 Faculty of Law, Macau University of Science and Technology, juzi96180@gmail.com

Abstract: Currently, data legislation exhibits a significant trend of extraterritorial application, becoming a core tool for countries to expand cyber sovereignty and compete for discourse power in data governance. However, such extraterritorial expansion of jurisdiction inevitably touches upon the sovereign boundaries of other nations, triggering risks of conflicts between states at the legislative, enforcement, and judicial levels. The EU GDPR's extraterritorial jurisdiction standards centered on "functional domicile" and "subjective intent" not only impose dual compliance dilemmas on Chinese enterprises operating overseas but also pose direct challenges to China's cyber sovereignty. The root cause of these conflicts lies in the failure of traditional jurisdictional theories, the absence of international law coordination mechanisms, and the divergence of data sovereignty models among countries. To address this, China urgently needs to establish an "active-response-oriented" extraterritorial application system for data legislation. While strengthening mechanisms to block improper extraterritorial application of foreign law, it is essential to improve the transformation and alignment of domestic and international laws to safeguard national sovereignty, security, and development interests.

Keywords: Extraterritorial Data Jurisdiction, Extraterritorial Application, GDPR, Cyber Sovereignty