DOI：10. 13766/j. bhsk. 1008−2204. 2023. 2035

● 数字经济环境下安全制度革新与权利理念审视研究专题

主持人语：全球数字经济发展离不开数据资源的自由流动和对数字资源的充分利用，世界各国针对数据资源的开发利用也纷纷制定了不同层面的法律制度和监管政策。但是，在数据资源的商业化使用过程中，仍然存在着数据安全、数据歧视等问题，严重影响了数据资源经济价值的开发利用。尤其在数据分析技术高速发展的当下，唯数据主义更是有可能对传统法律价值、科技伦理等造成严重侵蚀。针对这一现状，本专题刊发的三篇文章分别从不同的研究视角重新审视和解构了现有的商业实践和制度体系：其一，以数据跨境传输制度体系化为立足点，考察国内规则与国际规则之间的适用衔接问题，提出以数据主权为基础的制度完善建议；其二，主张从人权本原、人权解构、人权话语等多元视角考察数字科技与人权的复杂关系，并对“数字人权”的学术论争进行了系统性梳理和总结；其三，从身份、概念、功能、价值四个方面整合“数字人权”概念，区隔出四象限结构。

——赵精武（北京航空航天大学法学院副教授、北京科技创新中心研究基地副主任）

论中国数据跨境制度的现状、问题与纾困路径

叶传星，闫文光

（中国人民大学 法学院，北京 100872）

摘　要：中国已经建立了以“安全评估、标准合同、保护认证”为核心、以行业规定为配套的数据跨境制度体系，形成了既保安全又促发展的中国方案。但在具体立法中，该制度在理论与实践上存在双重失衡，在理论上缺乏完善的基础理论支撑，在实践中未能形成系统完整的制度体系，且其在适用关系上出现龃龉，与国际规则之间也存在割裂导致难以衔接，致使数据处理者在合规实践中面临较大成本，难以获得预期成效。不同于美国的“市场话语”和欧盟“权利本位”的数据跨境理论基础，中国应当基于国情明确利益平衡体系下的数据主权理论建构数据出境制度体系，矫正实践中过度保障安全的规制思路，通过单列安全评估、制定行业性与地方性特殊制度等措施，完善相关制度之间、国内法与国际规则之间的适用衔接，着力降低合规成本，保障制度落到实处。

关键词：数据跨境；安全评估；标准合同；保护认证；数据主权理论；合规成本

中图分类号：DF49; DF12　　**文献标志码：**A　　**文章编号：**1008−2204（2024）01−0057−15

Current Situation, Problems, and Relief Path of China’s Cross-Border Data System

YE Chuanxing，*YAN Wenguang*

（Law School, Renmin University of China, Beijing 100872, China）

Abstract: China has established a cross-border data system with “security assessment, standard contract, protection and certification” as its core and industry regulations as its supporting mechanism, which has resulted in a Chinese program that ensures security and promotes development. However, in the specific legislation, the system is unbalanced both in theory and practice. In theory, it lacks perfect basic theory support, and in practice, it has not formed a systematic and complete system. In addition, there is disagreement in the application relationship between the systems, and it is difficult to connect the systems with the international rules due to their separation from the international rules. Data processors face higher costs in compliance practices, making it difficult to achieve the desired results. Unlike

收稿日期：2023−12−11

基金项目：国家人权教育与培训基地重大项目（16JJD820029）

作者简介：叶传星（1968—），男，山东菏泽人，教授，博士，研究方向为法理学.

various theoretical foundations of cross-border data, such as the “market discourse” of the United States and the “rights-centeredness” of the European Union, China should construct a data outbound transfer system based on its national conditions and the theory of data sovereignty under the system of clear balance of interests, and rectify the regulatory ideas of excessive security protection in practice. China also needs to improve the connection between the relevant systems and between domestic laws and international rules through measures such as separate security assessments, formulation of special industrial and local systems, and endeavor to reduce the compliance costs and ensure the implementation of the system.

Keywords: cross-border data; security assessment; standard contract; protection and certification; data sovereignty theory; compliance cost

一、问题的提出

2023 年 2 月，《个人信息出境标准合同办法》正式发布，加上此前业已发布的《数据出境安全评估办法》《关于实施个人信息保护认证的公告》等政策法规，标志着《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》）第 38 条所明确的个人信息跨境提供三大机制全面落地。在上位法依据方面，《中华人民共和国网络安全法》（以下简称《网络安全法》）首先对特定主体的数据出境活动进行了探索，其第 37 条规定“关键基础设施运营者”向境外提供个人信息和重要数据的，除法律、行政法规另有规定外，应当进行安全评估。《中华人民共和国数据安全法》（以下简称《数据安全法》）第 31 条进一步区分了“关键基础设施运营者”和“其他数据处理者”两个主体，补充了“其他数据处理者”的相关规定，细化、完善了数据跨境流动的主体治理范围。《个人信息保护法》继续在上述二者的基础上通过专章对个人信息跨境规则进行了顶层设计，其第 3 章专门规定了“个人信息处理者”进行个人信息跨境时应满足的条件和履行的义务，并将个人信息跨境提供划分为三类场景：一是个人信息处理者的业务需要；二是中国参加的国际条约、协定对个人信息跨境有规定；三是外国司法或者执法机构提出请求。这三类场景各自遵循不同的监管规则，在一定程度上覆盖了当前实践中个人信息跨境的各类需求。此外，新修订的《网络安全审查办法》、《中华人民共和国人类遗传资源管理条例》（以下简称《人类遗传资源管理条例》）、《人口健康信息管理办法 (试行)》、《银行业金融机构反洗钱和反恐怖融资管理办法》、《中国人民银行金融消费者权益保护实施办法》、《商业银行互联网贷款管理暂行办法》等都对具体场景下的数据出境提出了要求，逐步建立起了一套数据出境监管制度体系。

但是，由于起步较晚，“针对中国网民规模巨大、企业平台众多、产品业态丰富的实际情况，适应法律主体多元、法律关系多样、法律适用场景多变的特点”[1]，中国的数据跨境流动无论在理论上还是在实践中，均出现了一些问题与缺陷，尚待进一步完善。在理论上，中国的数据出境监管制度缺乏成熟的基础理论依据作为指导，导致虽然在总体思路上秉承着平衡安全与发展的大方向，但是在具体制度设计时尚未形成科学的、系统的以及一以贯之的规制路径，难以准确掌握安全与发展的边界，制度之间存在空白重叠且无法有效协调适用；在实践中，缺乏基础理论的指导导致了制度层面的混乱，尤以因过度注重安全而进行“一刀切”的做法最为显著，“安全”的边界不断扩张和泛化，从而导致一方面在国际上难以与现有规则体系相衔接，另一方面在国内使得产业界背负巨大的合规压力，反噬并扼杀了数据的创新性利用。

数据已经成为继土地、劳动力、资本、技术之后的第五大生产要素，其价值在于流动，只有动态的数据流汇聚而成的大数据才能充分体现数据的经济价值，释放数字经济的活力。数据跨境流动推动了全球数字经济的发展和创新，其治理水平已成为衡量一个国家综合实力的重要参考标准之一，也是未来大国战略博弈的要点之一[2]。作为世界第二大经济体，数字经济的繁荣与否对中国而言同样至关重要，中国的跨境贸易、技术合作、企业出海、网络平台发展、科学研究等活动对数据出境的需求日益强烈，越来越多的企业、机构和个人需要进行跨境数据传输，以实现更好的经济、社会和文化交流，而当前数据跨境监管体系在理论上的缺失和在实践中的混乱已经严重阻碍了数据的有序流动，高昂的合规成本和模糊的监管方向使得产业界难以形成合理的稳定预期，许多企业纷纷停止其数据跨境业务并保持观望态度，严重影响了数字经济的健康发展。因此，笔者拟梳理分析中国数据跨境流动制度的现状，并根据

实践经验总结存在的难点与痛点，以期能为中国数据跨境制度体系的建立找寻到基础理论的支撑，提出相适应的解决之策。

二、中国数据跨境制度的现状及其困境

截至目前，各界普遍认为中国数据出境的路径包括三类：安全评估、标准合同和保护认证。三者互为补充、相互支撑，共同构建了中国数据出境的制度体系。其中，安全评估由国家互联网信息办公室（以下简称“国家网信办”）于 2022 年 7 月 7 日发布的《数据出境安全评估办法》作出具体规定，并提供了详细的申报指南，旨在通过行政许可的方式[3] 重点评估拟出境的重要数据，关键信息基础设施运营者处理的个人信息，大规模的个人信息对维护国家安全、社会公共利益、个人信息权益等的影响，以判断其出境的风险性。对于非重要数据、非关键信息基础设施运营者处理的个人信息和中小规模个人信息的出境需求，则由《个人信息出境标准合同办法》和《个人信息保护认证实施规则》作出规范。前者采用私主体商事行为+行政备案[4]78-94 的方式，仅要求符合条件的个人信息处理者与境外接收方按照给定的模板签订个人信息出境标准合同并进行备案，在此基础上即可实现个人信息出境，最大限度地促进和保障个人信息依法有序自由流动；后者则是将个人信息保护认证和个人信息跨境认证“合二为一”的第三方规制行为，相较于企业的自我规制和政府的行政规制，可以有效克服市场与政府的“双重失灵”[5]，从而通过独立于被规制对象的专业机构依据一定的标准和技术规范形成个人信息保护社会化服务体系[6]。整体来看，上述规定更加希望通过限制数据的跨境来保障安全，这一思路贯穿了中国近年来的数据相关立法，与之相对应的是国家网信办于 2023 年 9 月 28 日发布的《规范和促进数据跨境流动规定（征求意见稿）》，实现了中国数据相关立法思路的重大转向，在申报数据出境安全评估的条件、评估内容等方面做了较多豁免，从而有利于开展数据跨境流动。

总体来看，中国数据出境制度表现为《网络安全法》《数据安全法》《个人信息保护法》层面的宏观设计和《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息保护认证实施规则》层面的具体落实，安全评估反映出中国在数据出境方面聚焦风险规制，且并未严格区分不同数据类型，都由网信部门从风险的角度对数据出境活动进行一体评估[7]62-77；标准合同一直被认为是数据跨境传输领域的有效监管工具，欧盟《通用数据保护条例》（GDPR）将标准化合同条款（SCC）嵌入跨境数据流动的全过程，原因在于，该项机制既能实现监管者对于数据跨境传输重要事项的直接审核，也能基于违约责任督促数据处理者积极履行数据安全保护义务[8]；保护认证则是通过将行政成本转移为市场成本来实现更加灵活的数据出境，增强用户对中小微互联网企业和新兴数字产业的信任感并增加中小微互联网企业的交易机会[9]，避免因盲目追求安全而妨碍正常的数据出境流动。

安全评估、标准合同和保护认证三者看似相互补充并组成了一个完整的制度框架，但在实践中则“碎片化”严重，相互之间缺乏科学的逻辑设计，暴露出中国数据出境制度在系统性、国际性、可操作性方面存在的短板和待完善之处。

（一）系统性：未形成完整科学的体系

1. 存在监管空白

从规制对象上来看，安全评估涵盖的范围是对重要数据和大规模个人信息的处理，标准合同针对的是中小规模的个人信息处理活动，保护认证面向的也是个人信息处理活动。由此可以看出，对于既非个人信息又非重要数据的其他类型数据，目前均尚未有应当遵守的出境制度予以规范，处于监管真空状态。究其原因，难道是这些类型的数据并不重要以至于不值得对其出境活动进行监管吗？实践中显然并非如此。例如：在医疗卫生行业，其基础资源数据与业务资源数据包括医疗卫生机构的人员配置数据、重要医疗设备和信息平台的安保数据、特定药品的供应与规划数据、重要科研成果数据等，通过大数据技术对上述数据进行分析，就能够较为容易地获得一个国家的医疗政策和医疗能力变化情况；在贸易领域，通过一个地方的商品类型、快递物流信息等供应链数据就可以判断出当地的支柱性产业、产品销量、上下游合作方等信息，并可以较为容易地评估当地的经济状况、劳动力状况、产业结构，从而发起精准的经济制裁和封锁，美国早在 2019 年就已经注意到了供应链数据的重要性及其对国家安全的影响，并采取了一系列保护措施[10-11]；在金融领域，Swift 系统对接全球超过 11 000 家银行、证券机构、市场基础设施和企业，覆盖 200 多个国家和地区，年处理金融数据数十亿条[12]，近年来更是被美国用于制裁伊朗和俄罗斯，对伊朗和俄罗斯的金融数据安全乃至国家安全产生了巨大影响。

此类现象产生的原因源于两类法规之间的衔接不畅：一方面，数据出境主要制度之间存在空白，安全评估、标准合同和保护认证仅针对重要数据和个人信息作出了规定。另一方面，行业主管部门和配套法规制度未能及时跟进，未能发挥“配套”作用，突出表现为目前国内对重要数据和核心数据缺乏明确且详细的界定，在分类分级上也存在较多的模糊之处，使得作为数据出境制度选择适用起点的数据资产梳理难以有效开展，多数数据处理者无法确定自身业务中是否涉及对重要数据的处理，导致数据处理者在安全评估申报上进退两难。一是基于其自身对业务的了解，认为某些数据的出境将影响数据安全，尤其是“量变引起质变”后，一旦操作不慎将需要承担法律责任；二是因为安全自评估和申报的成本较大、流程烦琐，如果没有申报的必要反而会浪费大量的人力和物力。

2. 存在交叉重叠

从制度内容上看，安全评估与标准合同在内容上多有重合，二者都规定了安全自评估，且评估内容基本相同。安全评估与标准合同都关注数据出境和境外接收方的处理目的、范围、方式等的合法性、正当性、必要性，都要求说明数据的规模、范围种类和敏感程度，安全保障措施、应急预案和境外接收方的政策法规情况皆是二者的评估对象。同时，安全评估中要求双方签订的具有法律效力的文件在内容上也与标准合同模板相似，实践中申请安全评估的主体多参照标准合同模板制定或修改双方的法律文件。《个人信息出境标准合同办法》和《数据出境安全评估办法》评估内容对比，如表 1 所示。

表 1 《个人信息出境标准合同办法》和《数据出境安全评估办法》评估内容对比

评估事项	《个人信息出境标准合同办法》自评估	《数据出境安全评估办法》自评估	《数据出境安全评估办法》主管部门评估
数据出境的合法性、正当性、必要性评估	个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性	数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性	数据出境的目的、范围、方式等的合法性、正当性、必要性
出境数据的风险评估	出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能给个人信息权益带来的风险	出境数据的规模、范围、种类、敏感程度，数据出境可能给国家安全、公共利益、个人或者组织合法权益带来的风险	出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险
境外接收方评估	境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全	境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全	境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平能否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求
出境后安全评估	个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等	数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等	数据安全和个人信息权益是否能够得到充分有效保障
法律文件评估	境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响	与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务	数据处理者与境外接收方拟订立的具有法律效力的文件中是否充分约定了数据安全保护责任义务
其他事项评估	其他可能影响个人信息出境安全的事项	其他可能影响数据出境安全的事项	国家网信部门认为需要评估的其他事项
遵守中国法规情况评估			遵守中国法律、行政法规、部门规章情况

从法理逻辑上看，安全评估与标准合同的评估内容应当有所区别。由于安全评估针对的是重要数据和大规模个人信息出境对国家安全以及社会公共利益所产生的风险，其重点关注的是数据出境活动的安全面向，需要国家公权力的介入并进行实质审查，通过外部审批和问责的方式确保将风险降到最低，数据出境的实现需要让位于国家安全的保障；标准合同的立法目的在于保护个人权益，通过明确合同义务履行方式和违约责任承担方式[4]78-94 为个人信息出境提供便捷渠道，这也是为什么标准合同虽然要求自主缔约与备案管理相结合，但是并不以备案为前置条件的原因，以合同生效为出境条件的制度设计代表的是通过内在的诚实信用降低风险，因而在此语境下数据出境活动的实现更具重要性。但是，安全评估与标准合同的评估内容基本相同，导致二者在立法目的上的区分变得模糊，中小规模的个人信息处理者仍然需要按照重要数据和大规模个人信息处理者的标准开展自评估，这无疑会提升其在技术、管理、法律、资金等方面的成本，提高中小规模个人信息的出境门槛，原本为“优先促发展”而设

计的个人信息出境制度并没有发挥应有的作用，反而又回到了“优先保安全”的框架内。

（二）协调性：制度之间适用关系存疑

从上述现状可知，中国目前的数据出境制度是以《网络安全法》《数据安全法》《个人信息保护法》为总体框架，以《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息保护认证实施规则》为具体实施路径，以行业具体场景下的规定为配套措施，形成的“框架+路径+场景”的数据出境制度集成模块。但是，这个集成模块涉及文件的层级跨度较大，既包括法律也包括部门规章和规范性文件，在适用关系上存在较大疑问：一方面，在安全评估、标准合同、保护认证之间缺乏明确且清晰的适用逻辑安排，导致三者的适用顺序出现混乱；另一方面，行业场景制度由于出台时间跨度较大，且政出多门，即由不同的国家机关起草或出台，背后自然承载了各自不同的利益考量，因而在适用上多有龃龉。

第一，实践中，标准合同与保护认证在一定程度上被安全评估所架空。就安全评估、标准合同、保护认证的适用关系而言，安全评估将申报主体限定为“处理 100 万人以上个人信息的数据处理者、自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者”。但根据笔者的调研结果，能够满足上述要求而必须申请安全评估的主体数量较大，截至 2023 年 8 月，国家网信办和各省级网信办已受理的数据出境安全评估申报已达千余件。具体到健康医疗行业，根据对医院的调研结果，中国几乎每家三甲医院累计处理的个人信息数量均已超过 100 万人，且目前全国的三甲医院超过。1 600 余家[13] 这就导致大部分具有数据出境需求的主体落入了安全评估的范围内，将产生巨大的安全评估工作量，且从行业实践来看，有些主体即使不符合安全评估的申报标准，但为了规避可能产生的风险和法律责任，也会主动选择向网信部门提起安全评估申请，此类现象极大地架空了标准合同和保护认证的路径，灵活便捷出境的适用主体范围被限缩。

第二，理论上，安全评估与标准合同在一定程度上被保护认证所架空。《个人信息保护法》第 38 条规定，个人信息处理者向境外提供个人信息的应当满足安全评估、标准合同、保护认证三个条件之一，即可以根据自身条件择一适用，但保护认证的适用条件相当宽泛，可以同时适用于安全评估和标准合同的适用主体。此外，虽然《数据安全法》第 30 条规定了重要数据的处理者要定期开展数据安全评估，但此安全评估并非数据出境安全评估，而是一种定期评估的义务，这就造成了在制度适用上的混淆，也即满足安全评估和标准合同主体标准的数据处理者在出境个人信息时，按照上位法《个人信息保护法》第 38 条的规定，是可以绕开数据出境安全评估和标准合同而选择更加便利的个人信息保护认证途径的。虽然在实践中由于“保安全”之达摩克利斯之剑的存在，绕开安全评估和标准合同的行为几乎不会发生，但是在理论上却存在一定的漏洞，暴露出上位法依据不清或缺失所导致的协调性失衡，进而导致制度的适用关系不清。

第三，通用性制度、行业性制度之间衔接不畅。由于中国的数据出境通用性制度起步较晚，先前有关数据出境的要求多散见于各行业主管部门制定的法规中。由于制定时间各不相同，受当时国际环境、行业发展态势、数据安全意识、技术先进程度、部门职责利益等因素的影响，各行业主管部门制定的法规在禁止出境或限制出境的尺度把握上与当前新制定的通用性制度之间存在差异。按照《数据安全法》《个人信息保护法》《数据出境安全评估办法》《个人信息出境标准合同办法》的立法精神和立法目的，对于没有风险的数据原则上应当鼓励数据流动，对于可能会带来风险的重要数据以及大规模的个人信息在经过安全评估后仍然可以出境，但是目前有不少行业规定是严格限制甚至禁止某些数据出境的。例如：《人类遗传资源管理条例》第 7 条明确，外国组织、个人及其设立或者实际控制的机构不得向境外提供中国人类遗传资源；《人口健康信息管理办法（试行）》第 10 条规定，不得将人口健康信息在境外的服务器中存储；《商业银行互联网贷款管理暂行办法》第 34 条规定，用户的风险数据原则上不得出境。

其中，最具代表性的是人类遗传资源信息的出境，根据《人类遗传资源管理条例》，人类遗传资源包括人类遗传资源材料和人类遗传资源信息。人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料，人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。按照该条例第 27 条和第 28 条的规定，人类遗传资源材料出境需要取得科技部出具的人类遗传资源材料出境证明，而向境外提供人类遗传资源信息应当向科技部备案并提交信息备份。目前，中国对人类遗传资源信息出境的主管部门为科技部。由此产生的问题是，人类遗传资源信息大部分能够识别到个人层面，因而其应属于个人信息甚至是敏感个人信息，那么对于属于个人信息的人类遗传资源信息出境，应当选择科技部路径还是国家网信办路径就

成为摆在数据处理者面前的难题，二者之间所需条件、程序以及相关责任完全不同，且二者之间亦未做好协调。

第四，安全评估与安全审查如何适用尚不明确。目前，除安全评估外，重点关注与防范数据出境安全风险的制度还包括安全审查，如网络安全审查、数据安全审查、人类遗传资源出境的科技部审查等。2022 年 1 月 4 日，经国家网信办等 13 部门联合修订的《网络安全审查办法》发布，其适用范围在“关键信息基础设施运营者采购网络产品和服务”的基础上增加了“网络平台运营者开展数据处理活动”，包括掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，显然存在数据安全风险的数据出境活动也在网络安全审查范围内，且该办法第 10 条规定的审查内容与安全评估的内容具有一定的相似性。作为同样关注数据出境引发的国家安全、数据安全等问题的制度，安全审查与安全评估之间的关系如何、是否平行适用、在机制上如何配合等问题目前尚不明确。例如，经过网络安全审查或科技部审查的数据出境，是否还需要再申报安全评估？审查内容或评估内容是否在一定程度上重复并增加了数据处理者的合规成本？上述问题还需要进一步予以明确，以便为数据处理者提供更加清晰的指引，从而既有利于其高效率、高质量地合规，也有利于及时有效地保障中国的国家安全与数据安全。

第五，《规范和促进数据跨境流动规定（征求意见稿）》与《数据出境安全评估办法》在一定程度上相互冲突。根据《规范和促进数据跨境流动的规定（征求意见稿）》第 5 部分和第 6 部分的规定，预计一年内向境外提供不满 1 万人个人信息的，不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。预计一年内向境外提供 1 万人以上、不满 100 万人个人信息，与境外接收方订立个人信息出境标准合同并向省级网信部门备案或者通过个人信息保护认证的，可以不申报数据出境安全评估；向境外提供 100 万人以上个人信息的，应当申报数据出境安全评估。由此可以看出，只有当预计向境外提供 100 万人以上个人信息时，才必须通过安全评估的路径，而《数据出境安全评估办法》则规定了处理 100 万人以上个人信息、自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息都需要申请安全评估。综上所述，二者在两处产生了一定程度上的冲突：一是“历史出境数据”和“未来出境数据”的冲突，《数据出境安全评估办法》关注的是数据处理者历史上处理个人信息的体量，从而判断其出境数据是否会产生安全风险，而《规范和促进数据跨境流动规定（征求意见稿）》关注的是数据处理者未来将要出境数据的体量，从而判断其可能产生的安全风险，从实践情况来看，后者显然更加科学和有利于数据处理者；二是《规范和促进数据跨境流动规定（征求意见稿）》没有再区分个人信息和敏感个人信息的不同体量，统一将出境数据的数量提升至 100 万人，有利于方便数据出境业务的开展。

（三）国际性：难与国际规则相衔接

数据跨境是数字经济全球化背景下的产物，需要世界各国之间相互协作才能产生巨大价值，这就决定了数据能否实现高效、自由的流动不能仅仅依靠各个国家或地区的法规政策，还与区域性或全球性的国际规则和协定息息相关。近年来，数据跨境流动不仅成为国际数字贸易规则的核心议题，也成为各国争夺数字产业、数字治理话语权的关键领域[14]，美国、欧盟、中国等为促进自身数字经济发展，促进数据自由流动，积极主导制定或参与制定国际协议，输出自身的数据跨境流动规则与标准，形成了一系列成果[15]。自 2004 年以来，美国先后主导制定了《美国—智利自由贸易协定》、《美国—韩国自由贸易协定》、《跨太平洋伙伴关系协定》（TPP）、《美墨加协定》（USMCA）等，并通过亚太经合组织（APEC）积极推进《跨境隐私规则体系》（CBPRs）[16]，倡导自由的跨境数据传输，要求各国政府不得以数据保护为由限制数据的跨境流动。在美国于 2017 年宣布退出 TPP 后，原 11 个成员国宣布将 TPP 改名为《全面与进步跨太平洋伙伴关系协定》（CPTPP），保留了原 TPP 的大部分内容，同样支持跨境数据流动、反对数据本地化。

2020 年 11 月 15 日，中国同东盟十国、日本、韩国、澳大利亚、新西兰正式签署《区域全面经济伙伴关系协定》（RCEP），达成了亚太地区规模最大的自由贸易协定，中国首次在自由贸易协定中明确表示支持数据跨境自由流动和禁止数据本地化。2020 年 11 月 20 日，习近平在亚太经合组织第二十七次领导人非正式会议上发表讲话指出，中国“将积极考虑加入全面与进步跨太平洋伙伴关系协定”[17]。2021 年 11 月，中国正式提出申请加入《数字经济伙伴关系协定》（DEPA）。通过加入 CPTPP、DEPA、RCEP 等国际规则，表明了中国政府加快推动数据跨境流动、促进数字经济贸易全面发展、实现数据要素高水平开放的决心，跨境数据流动贸易规制提供了国际合作的基本制度框架，确认了跨境数据自由流动的共同

发展方向[18]。

但是，参与制定或者申请加入国际规则的必备条件之一是需要使国内制度与国际规则相衔接，满足相关国际规则的要求和标准，否则将很难实现标准输出与全面开放的目的。例如，《关于 CPTPP 加入程序的决定》明确要求申请加入方采取国内行动措施，即完成国内相关改革和法律修改，证明其将遵守 CPTPP 的现行规则。就中国目前申请加入的 CPTPP 和《数字经济伙伴关系协定》（DECP）而言，在数据跨境流动的促进与限制方面与中国国内目前的制度之间存在着较大的原则性分歧。根据 CPTPP 第 14.11 条规定，每一缔约方应当允许通过电子方式跨境传输信息，除非为了实现合法的公共政策目标方能施加限制性措施，但是这种限制性措施不以构成任意或不合理歧视或对贸易构成变相限制的方式适用，以及不对数据传输施加超出实现目标所需限度的限制。在这一方面，DECP 采用了基本相同的条款表述。

可以看出，CPTPP 和 DECP 规定了较高水平的数据跨境流动措施，同时对限制数据跨境的行为设定了极为严苛的条件。一方面，CPTPP 虽然未明确“合法的公共政策目标”的具体内容，但是也并没有授权各成员国自行确定，而在中国目前的国内制度中，安全评估、标准合同和保护认证都是对数据出境的限制措施，实施目的仅规定了较为模糊的“为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益”，没有规定明确的公共政策目标且无法说明此类限制的必要性，而金融、医疗等行业中规定的禁止数据出境条款更是在公共政策目标、歧视性限制和必要性方面缺乏具有足够说服力的解释，未来在与 CPTPP 的衔接中将存在巨大的挑战。另一方面，从 CPTPP 条款内容设置来看，其遵循的逻辑是“应当允许”出境为原则，“施加限制”出境为例外，而中国目前的制度设计则是以安全评估、标准合同和保护认证为主体，尤其是个人信息的出境条件必须满足上述三者之一，表现出了以限制为原则的逻辑思路，未来其他成员国如果将 CPTPP 第 14.11 条“应当允许”解释为等同于 USMCA 使用的“不得禁止或限制”的含义[19]，则中国的国内制度与国际规则之间则面临着完全相反的逻辑设计的困境。

（四）可操作性：成效难达预期

徒法不足以自行，即使再好的制度设计也需要得到实践的检验。除上述制度设计上存在的问题与短板外，在实际操作中，中国数据出境制度同样存在较多的痛点与难点，这极大地提升了数据处理者的合规成本，也给监管部门带来了巨大的监管阻碍。

1. 部门协调成本较高

无论是安全评估还是标准合同，都需要数据处理者首先进行自评估，这就要求对数据出境涉及的业务、数据链路等内容进行梳理和评估，而一项数据出境业务往往涉及技术、法务、管理、业务、营销等多个部门，有的数据处理者也会有多个业务场景需要进行数据出境，这就使得多部门协同配合成为数据出境安全评估申报的重中之重，其配合程度与效率高低将直接决定自评估能否顺利进行。但是，实践中往往只有法务部门能够重视这项工作，其他部门由于职责范围不包括这一内容而难以对其给予足够高的重视，部门之间协调困难成为安全评估的阻碍因素之一。例如，从笔者对北京地区具有数据出境需求的医院进行调研的结果来看，目前排名前三的医疗数据出境目的为国际合作临床试验和文章发表、国家药物临床试验以及人类遗传资源信息对外提供或开放使用，占比依次为 29%、18% 和 12%，而医院等医疗机构中往往是以课题组或研究团队为单位进行数据跨境流动，不同课题组对出境数据的字段、境外接收方、数据量、处理方式等条件具有不同的需求，因而，除本项目组外，其他部门对数据出境的驱动力并不强，配合程序和效率上往往存在滞后性。

2. 境内外配合难度高

安全评估中，境内数据处理者需要明确境外数据接收方的境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性，与其订立数据出境相关合同或者其他具有法律效力的文件，充分约定数据安全保护责任义务以及履行责任义务的管理和技术措施、能力等，保障出境数据的安全。对于一些已出境及在持续出境的数据，需要境外接收方同步配合对其开展大量的整改工作，加上安全评估为中国独具特色的数据出境制度，实践中存在部分境外数据接收者拒不配合甚至威胁反制的情况，因而境内与境外的沟通也是重点和难点之一。

3. 人力物力不足

一方面，在合规侧，数据资产梳理与自评估包含了巨大的工作量，需要耗费较多的人力和物力。然而，根据笔者的调研结果，目前实践中数据处理者主要采用 Excel 工作表的形式进行梳理总结并依靠专业人员进行主观评价，效率低、数量大、类别杂，缺少自动化技术手段，且专业人员不仅需要对相关法律法规了如指掌，还需要懂得技术与业务，否则将会

很容易出现“鸡同鸭讲”“隔行如隔山”的情况，一般的中小企业往往难以负担如此高昂的成本，也缺乏有效完成自评估的能力和现实条件，最终只能放弃申报数据出境而选择暂停业务，更有甚者则选择铤而走险，在未作申报的情况下仍继续开展数据出境活动。另一方面，在监管侧，根据《数据出境安全评估办法》，所有申报数据出境安全评估的审查材料都将汇聚到国家网信办进行评估，但是全国数据出境安全评估申报主体数量如此之多，每个申报主体的申报材料内容又十分繁杂，以国家网信办的人员数量要想快速完成如此之大的工作量，十分困难，且国家网信办并非行业主管部门，对于来自各行各业的数据出境业务必定无法全面掌握，在评估目的性、必要性等与业务场景紧密结合的内容时难免在专业性上捉襟见肘，这将极大地延缓审查速度。实践中，虽然大部分申报主体在国家网信办进行审核评估期间仍能继续进行数据出境活动，国家网信办对此也予以默认许可，但是这种“潜规则”的方式缺乏稳定性和可预期性，不利于市场主体正常开展业务。

三、数据跨境规制的理论逻辑

总体而言，中国目前的数据出境制度呈现出“以通用规则为主体，以行业规则为补充”的思路和格局。虽然在总体方向上强调兼顾经济发展与数据利用，在保障安全作为红线与底线的前提下促进数据的跨境流动，统筹兼顾不同领域对数据跨境的不同关切面向，但是在具体制度设计及实践中，中国的数据出境制度却出现了混乱情形，难以在实际操作层面真正实现“平衡安全与发展”的规制导向，尤以过度注重安全而“一刀切”的做法最为显著，“安全大于天”的红线使得“保安全”的边界不断扩张和泛化，甚至可以压倒一切，反噬并扼杀了数据的创新性利用，从而导致了上文所述的系统性、协调性、国际性和可操作性层面的重重问题。

究其原因，必然是政治、经济、文化、社会、舆论环境、立法技术等多种因素共同影响的结果。但其中最本质的因素是，尚未明确能够形塑监管体系的数据出境规制理论或政治道德哲学，从而难以一以贯之地形成稳定、科学和完善的数据出境监管体系[20]。一方面，数据跨境规制理论能够间接反映政治、经济、技术、社会等其他因素，是其他因素集中作用和影响的载体；另一方面，全世界各地的数据立法体系复杂庞大，不仅数量较多，而且法律、政策、指南、标准等各类文件纵横交叉，立法、执法、司法相互独立，美国的联邦立法与各州立法、欧盟的立法与各成员国立法相互作用，如果仅从制度层面借鉴分析而不深究其背后的理论逻辑，则往往会以偏概全甚至得出相互矛盾的经验总结。综合来看，当前主流的数据跨境规制理论包括数据自由贸易、数据权利保护、数据主权等[7]62-77。

（一）市场话语体系下的数据自由贸易理论

数据自由贸易理论以美国为典型代表，其建构基础来自市场话语体系。在美国，长期以来的冒险精神使得不论政府还是公民都倾向通过多元、宽松的手段追求经济的发展，虽然存在一定的安全风险，但是绝不能为了实现零风险而极大地阻碍甚至扼杀市场经济、科技创新以及全球化竞争。因此，美国倾向通过事后救济的方式来进行风险规制[21]，并将自由贸易认定为国家和社会发展的主要目标之一，在社会中已经形成了较为广泛的市场话语体系[22]。

在这种文化背景下，全球被美国视为一个开展自由贸易的大市场，数据是全球市场上的一种商品，而数据自由跨境流动则被视为自由贸易的重要前提条件。因而，美国鼓励全球数据自由流动，要求其他国家和地区降低数据跨境门槛，弱化监管和司法限制，并提出公平信息实践理论。自 2011 年 11 月 13 日起，美国开始不断推进并主导 APEC 的 CBPRs，旨在通过区域规则要求缔约方确保数据跨境的自由流动[23]。同时，在美国国内的相关数据隐私法规中，也未采取如欧盟等地区般严格执行的知情同意等数据授权原则，美国各方可以未经同意收集和使用个人数据，只需要遵守一些其他相关法规即可[24-25]。

但是，在自由贸易的背后，美国单边主义的霸权文化在数据跨境流动领域内不断扩张[26]，其同样关注通过数据实现其全球霸权的延续，打造新的“数据霸权”，保障对其他国家相关主体的“长臂管辖”。因此，虽然美国联邦层面在数据出境上的整体政策较为宽松，但是美国也并未放松对一些重要数据的管制，对于数据安全问题极为重视。例如：2018 年通过的《澄清域外合法使用数据法案》（CLOUD），针对危害国家安全和重大犯罪的行为规定了较为强势的跨境数据调取规则；《2022 年保护美国人数据免受外国监视法案》（Protecting Americans’ Data from Foreign Surveillance Act of 2022），旨在防止美国公民敏感的个人数据流入恶意的外国实体①。

美国拥有全球数量最多、规模最大、国际化程度最高的互联网企业和科技企业，其在数据的产生、收集、分析、利用等方面具有无可比拟的优势，多年来汇聚收集了全世界的海量数据，为其“世界警察”

角色提供了强力支撑。一方面，表现为经济红利的增长。例如，谷歌公司、苹果公司的海外市场收入占比常年保持在它们总营收的 50% 甚至更高，亚马逊公司也有差不多 1/3 的收入来自海外[27]。另一方面，表现在国家安全和政治安全上。多年来，美国利用自身数据和算法的优势，长期对其他国家政府进行类似“棱镜门”的监视，根据他国贸易数据、供应链数据发起精准的贸易战和经济制裁，甚至扰乱他国社会稳定。所以，这也从侧面反映出，数据是新时代的石油或原材料，如果主权国家没有权利管理自身主权范围内的数据，那么数据就会源源不断地流向数字经济发达的国家和地区，数字落后的国家和地区则无法从中获得好处[28]，甚至导致数据殖民主义[29]的产生。

（二）权利本位体系下的数据权利保护理论

权利本位体系下的数据权利保护理论以欧盟为典型代表。与美国相反，欧盟走上了一条权利本位的话语体系之路，将数据视为公民尊严、人格、自由等基本权利的载体和映射，事关公民的身份、隐私等人权能否得到充分的保护，神圣不可侵犯。基本权利保障是第二次世界大战后欧洲国家创造欧洲公民身份计划的重要组成部分，是在法西斯主义和纳粹主义的毁灭性经历中，欧洲国家领会到的保护人类尊严的血泪教训。在第二次世界大战后，欧洲国家逐步建立了一个基本权利的超国家体系，并形成了《欧洲人权公约》和《基本权利宪章》——欧洲基本权利的两大支柱②，由此产生的欧洲数据保护系统以数据主体为权利主体的中心，处理个人数据一直被视为会给人的基本权利带来重大风险的行为，所以欧盟一直以来对于美国法律是否为欧盟公民的个人数据提供足够的保护保留较大质疑[30]。

此外，“国家”安全与利益同样也是欧盟数据跨境制度的重要考量因素之一，第二次世界大战的阴霾使得个人基本权利被欧盟视为“国家”安全与利益的基石，没有对公民基本权利的保护，“国家”安全也将无从谈起。因此，欧盟 GDPR 规定了较为严格的数据跨境流动制度。就个人数据而言，欧盟委员会可以依据 GDPR 法规作出“充分性决定”（adequacy decision）来认定非欧盟国家是否有足够的数据保护水平，该决定将评估个人数据从欧盟流出进入第三国是否需要附加保护措施。如果第三国不在欧盟“充分性决定”范围内，则可以利用具有约束力的公司规则、标准合同条款、认证机制等开展个人数据跨境活动。

由于欧盟 GDPR 具有广泛的域外效力和强有力的执法机制，所有处理欧盟公民信息的个人信息处理者不论其处理行为是否在欧盟境内，都需要遵循欧盟的相关法规，加上欧盟具有拥有巨大潜力和价值的数字市场，导致其他国家涉外企业的跨境合规往往绕不开 GDPR。并且，大多数国家意识到了欧盟数据跨境制度对国家安全和人权的有效保护，往往选择与欧盟进行制度衔接，参考并借鉴欧盟的标准以达到充分性认定水平，这大大促进了欧盟的标准向其他国家的输出，形成了“布鲁塞尔效应”，进一步强化了欧盟的“国家”安全与利益的实现。

但是，与数据自由贸易理论相似，数据权利保护理论同样存在缺陷，主要表现为欧盟认为保障公民的个人数据权利具有极高的价值位阶。虽然极少数的互联网平台巨头已经使欧盟认识到不受阻碍的数字贸易对欧洲十分重要[31]，促进先进技术和相关服务的创新能够带来巨大的利益③，但是数字经济的发展、互联网平台的创新等都需要让步于个人基本权利保护这一红线，当这些其他利益与个人数据权利相冲突时，欧盟法院就会进行比例分析，结果往往是采取更高水平的个人数据保护措施和对数据跨境流动进行更加严格的监管，基于事前预防的基本逻辑充分保障欧盟公民的基本人权。因此，欧盟的数据在内部成员国之间虽可自由流动，但限制了个人数据转移到欧盟境外，采取了多种手段严格控制个人数据的跨境流动，并为此先后通过 Schrems Ⅰ 案和 Schrems Ⅱ 案，使得其与美国之间为促进数据跨境流动而达成的“安全港”和“隐私盾”协议变得无效④。

（三）利益平衡体系下的数据主权理论

美国的数据自由贸易理论虽倾向通过采用事后救济和责任承担的规制进路来促进数字经济的发展，但其背后是以强大的数据霸权和数据殖民主义作为支撑的；欧盟虽倾向采用事前预防的规制进路来保障基本人权，但其代价是数字经济的艰难发展。

显然，数据自由贸易理论与数据权利保护理论并不能有效满足中国现阶段的发展需求。

一方面，中国素无数据霸权的文化传统，反而因为政治、经济、科技实力等原因需要强力保护国家主权与安全，维护公民的相关数据权益。近年来，美国“长臂管辖权”的适用范围不断扩大，从解决美国国内问题发展到介入国际问题、从司法管辖权延伸到立法管辖权和执法管辖权、从民事案件扩张到刑事案件[32]，这种向外扩张的路径难免会与其他国家的利益产生冲突[33]，如美国将中国企业列入“实体清单”试图遏制中国产业发展[34]，如果核心数据、重要数据或大量个人信息被非法出境，将会出现被外

国政府影响、控制、恶意利用的风险。

此外，在第二次世界大战期间，中国遭受了日本帝国主义的人权毁灭，对中国人民的人格尊严与自由等基本权利带来了巨大伤害。改革开放以来，党和国家一直坚持不懈地追求和保障人权，将人民对美好生活的向往作为奋斗目标，不断发展全过程人民民主，推进人权法治保障，坚决维护社会公平正义，促进中国人民的生存权、发展权和其他各项基本权利保障不断向前推进[35]。人权的保障离不开数据主权、国家安全的完整，更需要通过保障公民数据权益来实现，因此，中国的数据出境制度应重点关注安全底线，防范和提前化解可能存在的风险，将数据主权、国家安全、公共利益以及公民权益保障作为数据安全立法的重要原则。

另一方面，中国目前正值数字经济发展的关键期，显然不能因噎废食，以牺牲经济发展为代价。近代以来，清政府采取闭关锁国的政策，几乎断绝了与世界各国之间的大型贸易往来和科技文化交流，以至于错失了工业革命和科技革命，积贫积弱的国力使得中国沦为半殖民地半封建社会，落后就要挨打的历史教训时刻警醒我们必须自立自强。当前，数字经济的快速发展以及百年未有之大变局形势为中国的发展提供了历史机遇，“两个一百年”奋斗目标和中国式现代化的推进需要我们不断做优做强数字经济，数据的跨境流动是数字经济发展的重要内容，只有充分释放数字红利，才能让人民群众真正受益。

因此，相较于美国的数据自由贸易和欧盟的数据权利保护，中国应当基于利益平衡体系下的数据主权理论建构数据跨境制度，强调安全与发展兼顾、“既要又要”的风险规制进路。利益平衡体系下的数据主权理论以维护国家安全为底色，采取因时制宜的数据主权形态，将分级分类保护作为核心机制，具体包括数据保护权与数据参与权。在该理论下，安全评估应当处于单列且优先使用的地位，但其适用需要遵循严格的触发条件，即：只有数据出境行为及境外数据处理活动将对国家安全产生危害时才需要进行安全评估，这种规定是国家主权之自保权的体现，当境外数据处理行为危害到本国国家之安全时，国家有抵御外来侵犯之绝对权利，本国对境外数据威胁行为采取防御、处置措施是国家主权作用的当然结果，此为数据保护权；数据参与权是指当数据出境行为与国家安全、公共利益的关联性相对较弱时，应当采取标准合同与保护认证并行的方式，积极参与国际化数据跨境规则制定和全球经济发展。同时，对内而言，鼓励行业主管部门、自贸区等积极参与数据跨境制度的制定，根据行业特点、地区特点，因时因地制宜地规范数据跨境流动。

“保安全”与“促发展”在数据跨境流动领域并不是相互对立的，而是有机结合以共同致力于使公民的权利和利益得到有效保障。“促发展”并非单纯追求金钱等利益的增长，而是通过数据的流动推进贸易的开展，进而促进数字经济的繁荣发展，让人民群众享受到时代发展的红利，增强国家的经济实力。落后就要挨打的历史教训和改革开放的成功经验告诉我们，经济的发展将为保障国家安全、社会公共利益以及公民权益提供坚实基础，因此，“促发展”可以说是另一种层面上的“保安全”，二者相辅相成、殊途同归，是数字经济发展的鸟之两翼、车之两轮，不应存一废一、偏执一面，而应统筹兼顾，找寻融合与平衡之策。

四、构建数据主权基础上的数据跨境体系

（一）明确安全与发展并重的利益平衡原则

2023 年 7 月 25 日，国务院印发的《关于进一步优化外商投资环境 加大吸引外商投资力度的意见》指出：“探索便利化的数据跨境流动安全管理机制。”2023 年 9 月 28 日，国家网信办发布了《规范和促进数据跨境流动规定（征求意见稿）》，以进一步规范和促进数据依法有序自由流动，同时使得许多数据出境行为豁免于安全评估而可以通过保护认证、签订标准合同等方式出境，降低了门槛和标准，回应了当前国际社会对中国营商环境的质疑，从而极大地便利了数据出境，于经济发展而言是重大利好。

在数据跨境流动的问题上，中国应当明确在数据主权和国家安全视野下最大限度地促进数据自由流动和经济快速发展的基本思路，合理平衡“保安全”与“促发展”理念，防止因“一刀切”式的做法过度扩张安全边界而产生监管异化，从而破坏了科技创新、经济发展和对外开放的良好格局，增加了数据跨境流动的成本，提高了市场主体数据处理和业务开展的成本，打击了通过数据流动进行创新的积极性。

一方面，应当坚持数据主权和国家安全的底线不动摇。数据主权是国家主权的集中体现，是《联合国宪章》中最为核心的原则之一[36]。数据作为有重要经济价值的生产要素，对其占有量的多少和处理能力的大小，是一个国家在全球数字市场中竞争力强弱的外在表现，因而往往会沦为发达国家输出法

律制度及其背后价值观的工具，数据霸权最终会导致数据垄断，数字经济实力弱小的国家将被限制在巨大的“数字鸿沟”之中，因此，当数据状态安全与否威胁到一个国家的生存和独立发展时，该国就有权采取自我保护措施以维护自身数据安全。

另一方面，应当清醒地认识到，安全不是绝对的，风险永远存在。正如习近平所指出的：“网络安全是相对的而不是绝对的。没有绝对安全，要立足基本国情保安全，避免不计成本追求绝对安全，那样不仅会背上沉重负担，甚至可能顾此失彼。”[37] 在当前的实践中，中国的数据出境制度与监管力度过于偏向“保安全”，在具体手段上借鉴了保护“基本权利”的欧盟制度，如安全评估与欧盟 GDPR 的核心机制——充分性认定——相类似，需要评估数据流入国家或国际组织的数据保护水平以及其与欧盟的政治关系、经贸关系、法治水平、人权保护等因素，此外，欧盟 GDPR 也规定了标准合同、第三方认证等制度。

但是，中国与欧盟的法律文化不同，在立法诉求上也存在差异，不能照搬欧盟的制度设计，而是应立足本土法律文化与国情，基于中国当前处于数字经济弯道超车的历史机遇期，明确经济发展的巨大需求。此外，即使是以保护“基本权利”为导向的欧盟，在具体制度开展上也没有过于遏制数据的跨境流动，如“充分性认定”是对一国的状况进行评估，如果达到了欧盟的数据保护标准，则双方之间的数据即可自由流动，不需相关主体再单独申请，且相较于中国“一事一议”的安全评估，更加有利于数据的快速流动。在标准合同方面，欧盟于 2001—2010 年先后发布了三套标准合同（SCC2001C&SCC2001P、SCC2004C、SCC2010P），并于 2021 年再次更新发布了第四套标准合同。总体来看，2021—2010 年发布的三套标准合同降低了企业的合规成本与难度，促进了数据的流动。相较于 2001—2010 年发布的三套标准合同，2021 年更新的第四套标准合同整体上强化了对数据的保护，细化了数据流动的具体场景，体现了不同条件下的规制梯度。此外，前三套标准合同是在执行欧盟《数据保护指令》（Data Protection Directive），第四套标准合同则主要是落实 GDPR 的产物，可以预见，未来欧盟还将继续更新 GDPR 背景下的标准合同，更进一步促进数据的自由流动，为欧盟数字统一市场的建立提供支撑。

因此，未来中国的数据出境制度应当适当更新，探索更加多元化的方式以促进数据的跨境流动，更新和细化不同场景下的制度规定，增加批量评估的占比。

（二）重构制度体系性与协调性

1. 安全评估单列且优先适用

《个人信息保护法》第 38 条规定，个人信息处理者向境外提供个人信息的，应当满足安全评估、标准合同和保护认证三个条件之一。这就导致安全评估与标准合同、安全认证的适用关系出现瑕疵，未来应当基于数据主权理论明确安全评估单列且优先适用的法律地位，且只有在数据出境行为及境外数据处理活动会对国家安全产生危害时才能触发。

在内容优化上，《数据出境安全评估办法》将数据出境安全评估申报的条件落脚在历史上曾经处理过的个人信息数量或出境的个人信息数量上，即根据历史数据处理量来判断该数据处理者的数据出境活动将给国家安全、社会安全和个人信息主体权益可能带来的风险，这虽然具有一定的合理性，但是在实际落地中却暴露出了较大的短板与缺陷。根据笔者对相关具有数据出境需求的机构的调研结果，有些数据处理者虽然已经处理超过 100 万人的个人信息，但是其拟出境的数据量却较小，甚至只有几条或者几十条，其内容也不属于敏感的个人信息，在这种情况下，如果仍然申请数据出境安全评估，将会给其带来较大的负担。例如，在实际的数据出境安全评估申报中，有些餐饮企业和银行拥有超过 100 万名用户，但其需要出境的数据并非其用户的个人信息等业务数据，而是其员工个人信息等管理数据，这种拟出境的数据无论从数量上还是敏感程度上都不满足数据出境安全评估的规制目的。又如，根据上文所述之笔者对国家卫生健康委员会及医院的访谈调研结果，中国 1 600 余家三甲医院中的大部分医院都满足处理超过 100 万人的个人信息的标准，但医院的数据出境需求往往是某一个课题组的研究需要，其与该课题组的专家具有极高的利益相关性，但与医院的利益相关性却较弱，其需要出境的数据体量有时会极小，因而实践中有不少医院认为其不应该作为各课题组数据出境的责任主体，且医院也缺乏能力对众多课题组的数据出境活动进行监管和安全保障，所以只能“一刀切”式地禁止医院内的数据出境活动，这给医学健康研究带来了较大阻碍。

因此，未来的数据出境许可条件的设置应当根据数据处理者的实际情况和合理需求制定标准，从而将监管资源集中于保障真正关系国家安全、社会安全和公民权益的数据出境活动。例如，将《数据出境安全评估办法》第 4 条中的“历史数据处理量”转向“未来数据处理量”，在认定数据出境安全评估主体标准时关注“预计一年内向境外提供”的数据量，

并增加豁免条款，在“为订立、履行个人作为一方当事人的合同所必需、按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理、紧急情况下为保护自然人的生命健康和财产安全、科学研究”等方面减轻或免除安全评估的限制。

2. 明确重要数据范围目录

重要数据在数据跨境监管中占有重要地位，其出境后的安全状态直接关系着中国的国家安全与数据主权，识别重要数据的数量和范围是数据跨境活动开展的前提与基础，如果无法厘清重要数据，则数据跨境规制的安全面向将无从谈起。但是，当前无论理论界还是产业界，均未能明确重要数据的范围、目录以及具备可操作性的识别标准，这也成为目前最重要的行业痛点。例如，在医疗领域，大部分医院尚未建立数据分类分级制度，也未能形成较成体系的数据分类分级方法、策略规则、目录清单等，有些虽进行了数据分类但没有进行数据分级，对于数据资产清单的认识尚不清晰。对此，医院的顾虑在于，健康医疗行业的重要数据定义模糊，国家对医疗领域的分类分级没有明确指导，因此医院内部无法有效区分数据分类分级。

对相关概念的澄清与解释是数据出境制度实施的起点。只有明确了“数据分类分级、一般数据、重要数据以及核心数据”等基础概念，才能为相关主体提供合理预期，便于根据不同类别和重要程度采取不同的出境路径和保护措施。因此，应当尽快完善和明晰数据分类分级制度，通过“列举+兜底”的方式明确一般数据、重要数据和核心数据的边界与范围，从重要数据的识别到对重要数据的管理，从重要数据安全合规使用到重要数据安全保护，所有安全要求都需要有专业化、自动化工具的支持[38]。在重要数据的识别上，应当基于国家数据主权制度的前提和基础，先从类别内容上做出区分再根据重要数据的类别内容做出等级划分[39]，充分考虑各行业场景的共通性与特殊性，通过定量与定性相结合的方式来进行动态识别。

首先，基于数据主权的重要数据识别，应当聚焦国家安全、数据主权面向，明确重要数据与重要的数据之间的关系，避免为了过度追求安全而盲目扩张重要数据的范围。其次，充分考虑行业的安全特性和对数据跨境的正当需求，对于一般数据，原则上应当通过立法明确允许自由流动，提升市场预期和信心。最后，基于定量与定性相结合的方式动态识别重要数据。一方面，要从数据属性、场景、内容等定性的角度评估其对国家安全和数据主权的影响程度，判断其遭遇泄露、非法获取等情况时产生的危害程度；另一方面，要从定量的角度判断危害产生的概率，如虽然一组数据泄露后产生的危害程度为 90%，但这种情况发生的可能性仅为 0.01%，是否应将其纳入重要数据的范围就有待商榷。此外，有些数据在体量较小时无法对国家安全和数据主权产生影响，但经过汇聚形成大数据后极有可能反映出重要信息，因而数据量的大小也是重要数据识别中需要重点考虑的因素。

3. 鼓励地方性、行业性制度

考虑到各行业主管部门的专业性以及部分地方的特殊功能定位，应当鼓励行业主管部门和部分地方积极参与数据跨境制度的制定，并因时因地细化完善相关条件，在部分地区、部分行业、部分场景下的数据出境监管中采取更加便捷、高效、快速的措施，最大限度地满足各类产业的发展需求。

在地方性制度层面，国务院 2023 年 8 月 13 日发布的《关于进一步优化外商投资环境加大吸引外商投资力度的意见》指出：“探索便利化的数据跨境流动安全管理机制。……支持北京、天津、上海、粤港澳大湾区等地在实施数据出境安全评估、个人信息保护认证、个人信息出境标准合同备案等制度过程中，试点探索形成可自由流动的一般数据清单。”2023 年 11 月 26 日，国务院印发的《全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案》指出：“在国家数据跨境传输安全管理制度框架下，允许金融机构向境外传输日常经营所需的数据。涉及金融数据出境的，监管部门可基于国家安全和审慎原则采取监管措施，同时保证重要数据和个人信息安全。”此外，就粤港澳大湾区而言，其横跨“一国、两制、三法域”，内地与港澳之间的数据法存在较大差异，且内地与港澳之间的数据传输属于跨境传输，若采用内地法规则存在较大阻碍，若采用国际公认的保护法规和惯例则难以与内地有关法规完全接轨，这就导致港澳作为国家对外开放桥头堡和远东金融中心的作用被大大限制。为此，国家网信办与香港特别行政区政府创新科技及工业局先后签署了《关于促进粤港澳大湾区数据跨境流动的合作备忘录》和《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》，明确除被认定为重要数据的个人信息外，其他个人信息在广东九市与香港之间的跨境流动都可以通过订立标准合同的方式进行，并减少了个人信息保护影响评估的内容，对标准合同的登记备案手续也予以了简化，更为重要的是，降低了对境外接收方

的义务要求, 极大地促进了数据跨境流动的发展趋势, 为相关主体提供了更多的操作空间和便利。未来, 可以参考此类经验制定一系列规则, 规范和促进数据通过港澳进行跨境传输的相关活动。

在行业性制度层面, 网信部门的数据跨境规则与人类遗传资源信息跨境规则应当相互协调, 进一步明确不同主体、不同数据的适用情形, 合理划分网信部门与人类遗传资源信息主管部门的职责分工和监管范围, 明确人类遗传资源信息出境的监管部门以及所需要采取的程序、标准、要求、安全保障措施等, 为相关数据处理者提供清晰的合规指引。从目前的行业实践情况来看, 人类遗传资源信息出境由人类遗传资源信息主管部门进行监管更加有利于跨国科研等业务的开展。原因有二: 一是该制度更为相关数据处理者所熟悉, 大部分有出境需求的数据处理者更加了解人类遗传资源信息主管部门的数据出境流程, 在实际数据出境时也更多地采取了这一路径, 而对于网信部门的数据出境路径却十分陌生, 学习成本较大; 二是相较于网信部门的数据出境路径, 人类遗传资源信息主管部门的数据出境条件、流程和标准更加便利, 在材料准备方面, 相较于数据出境安全自评估所需成本较小, 而且可以通过统一的信息系统进行流转, 不需要另建系统。

(三) 协调衔接国际规则

2023 年 7 月 10 日, 欧盟和美国达成了继“安全港”和“隐私盾”之后的新的《欧美数据隐私框架》(EU-US Data Privacy Framework), 设立独立法庭以审查美国情报机构数据收集工作, 保障在此框架下个人数据可以自由、安全地流动, 被称为“欧美双方为了维系 7.1 万亿美元的跨大西洋经济关系的重要举措”。2023 年 10 月 21 日, “英美数据桥”(UK-US Data Bridge)生效, 届时将允许组织通过《欧美数据隐私框架》的英国扩展进行美英之间数据跨境传输, 英国的组织将能够将个人数据传输到获得《欧美数据隐私框架》的英国扩展认证的美国组织, 而无需采取进一步的保护措施, 以实现英美相关组织之间的数据自由流动。2023 年 10 月 28 日, 欧盟和日本就跨境数据流达成了协议。该协议明确, 将取消数据本地化要求, 使金融服务、运输、机械、电子商务等多个行业的企业受益, 让它们无需进行烦琐且成本高昂的管理即可处理数据。国际上的数据跨境将迎来新一轮的合作高峰, 从而在全球经济低迷的时代背景下促进国际贸易的复苏, 提升各国经济发展, 同时给中国社会经济的发展带来机遇和启示。

《网络安全法》《数据安全法》《个人信息保护法》都明确了积极“参与数据安全相关国际规则和标准的制定”的开放理念, “推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认”, 以更加自信的形象参与全球数据治理, 发出中国声音, 提出中国方案, 输出中国标准。同时, 国际规则不仅左右各国之间的利益分配, 而且决定一国在国际社会中所能扮演的角色, 并对其国际行为合法性进行评判[40]。因此, 中国能否有效参与国际数字规则制定, 形成符合中国产业利益的方案和主张, 并将其融入规则中, 将直接影响中国数字经济发展和国际地位的提升。

首先, 中国应以更主动进取的姿态参与数据跨境流动国际规则的构建, 在经贸、投资以及其他相关专题谈判中启动数据跨境流动谈判, 做好国内制度与国际规则的衔接工作, 加强国际合作与协调, 促进各国之间的互信和合作。其次, 中国应当合理全面地利用解释手段, 在关键核心问题上通过文义解释、目的解释等方式消除与中国相关制度可能存在的分歧, 逐步实现法律规制的趋同。最后, 利用北京“两区”、上海自贸区、海南自贸港、粤港澳大湾区等区域的制度创新优势, 开展跨境数据流动试点, 形成数据跨境规则的特区或“监管沙盒”, 在容错机制环境下探索建立数据跨境流动的正面清单或负面清单, 既能便利中国企业的数据“走出去”, 也能让外国企业的数据“走进来”。例如, 北京“两区”正在策划建设数字贸易港, 希望实现与欧盟之间数据跨境流动的特殊安排。

(四) 降低合规成本

随着人工智能、大数据等技术的进一步发展, 利用“法律+科技”的手段实现监管与合规的自动化、智能化已经逐渐成为未来的发展趋势。监管部门应持续推进监管科技工具的发展繁荣, 通过智能监管技术实现监管的智慧化、自动化、精细化和全面化, 把日常监管融入个人信息处理者的个人信息出境活动中, 共同推动数字经济健康发展。个人信息处理者应当主动采用智能化合规工具重构合规体系, 通过类似 ChatGPT 的自然语言处理工具构建规则引擎, 对相关法律法规进行自动化分析解构, 通过法律代码化和规则自动化而自动生成符合要求的个人信息出境合同等法律文件, 同时通过技术对数据收集、存储、加工、使用、传输、删除等全生命周期进行可视化管理, 自动分析企业数据资产与合规风险, 根据分类分级等规则自动识别个人信息的数量、范围、类型、敏感程度, 保障个人信息处理目的、范围、方式等的合法性、正当性、必要性, 自动化完成法律法

规要求的自评估等工作，这样既能提高合规的质量与效率，又能降低合规的成本。例如，基于《个人信息保护法》和《数据出境安全评估办法》，设计直观易懂的评估问卷或手册，快速排查具体业务场景的合规风险，自动生成风险矩阵，可视化追踪风险处置进度及持续改进计划，构建发现、评估、整改、优化的管理闭环，自动化生成符合规范要求的数据出境风险自评估报告或个人信息影响评估报告，全方位展示最终评估结果和风险处置过程。

五、结语

一方面，数据的跨境流动能够催生新模式、新业态和新企业，深刻改变国际贸易和分工格局，并借助其公共产品的特性，使国际经济竞争从“零和博弈”转向“帕累托最优”，向自由、开放、合作、共享的方向发展；但另一方面，数据的跨境流动又与数据主权、国家安全、公共利益、个人合法权益等非经济领域密切关联，甚至会威胁到一国的稳定与安全，致使数据安全与数据自由流动之间关系紧张。

目前，世界各国为抢占数字经济繁荣高地，纷纷制定更加宽松开放的数据跨境流动政策法规，力求夺取数字产业发展先机，从激烈的国际竞争中胜出。客观而言，中国现有的数据跨境监管体系暴露出了较多问题，已经对产业的开放发展和数字经济的弯道超车产生了较大阻碍。未来，中国应当对数据跨境制度体系进行转向性调整，依托数据主权基础平衡安全与发展，构建更加开放、动态和稳定的数据跨境监管体系，优化营商环境，提高投资促进工作水平，加大吸引外商投资力度，探索便利化的数据跨境流动安全管理机制，形成可自由流动的一般数据清单。

注释：

① 参见：Protecting Americans' Data from Foreign Surveillance Act of 2022, S.4495, 117th Cong. (2022)。

② 参见：Charter of Fundamental Rights of the European Union, 2000 O.J C 364/10; Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 1, Nov. 4, 1950, 213 U.N.T.S. 222。

③ 参见：Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 60-62 (EU)。

④ 参见：Judgment of 6 October 2015 in Schrems v. Data Protection Commissioner, Case C-362/14, ECLI: EU: C: 2015: 650; Judgment of 16 July 2020 in Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Case 311/18, ECLI: EU: C: 2020: 559。

参考文献：

[1] 新华网. 新时代的中国网络法治建设[EB/OL]. (2023-03-16)[2023-10-21]. http://www.news.cn/politics/2023-03/16/c_1129434612.htm?channel=weixin.

[2] 易永豪, 唐俐. 我国跨境数据流动法律规制的现状、困境与未来进路[J]. 海南大学学报(人文社会科学版), 2022, 40(6): 135—147.

[3] 张凌寒. 论数据出境安全评估的法律性质与救济路径[J]. 行政法学研究, 2023(1): 45—61.

[4] 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): 78—94.

[5] 刘权. 数据安全认证：个人信息保护的第三方规制[J]. 法学评论, 2022, 40(1): 118—130.

[6] 刘懿阳.《个人信息保护认证实施规则》背景下的认证制度实施[J]. 网络安全与数据治理, 2023, 42(1): 61—66.

[7] 丁晓东. 数据跨境流动的法理反思与制度重构——兼评《数据出境安全评估办法》[J]. 行政法学研究, 2023(1): 62—77.

[8] 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[J]. 法律科学(西北政法大学学报), 2022, 40(2): 148—161.

[9] 刘亚平, 游海疆. “第三方规制”：现在与未来[J]. 宏观质量研究, 2017, 5(4): 106—116.

[10] White House. Executive order on securing the information and communications technology and services supply chain [EB/OL]. (2023-04-20)[2023-10-21]. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[11] Federal Register. Securing the information and communications technology and services supply chain [EB/OL]. (2023-04-20)[2023-10-21]. https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

[12] 董少鹏. 该如何看待 SWIFT 系统这张“牌”?[N]. 证券日报, 2022-02-28(A2).

[13] 国家卫生健康委员会. 2021 年我国卫生健康事业发展统计公报 [EB/OL]. (2022-07-12)[2023-10-21]. http://www.nhc.gov.cn/guihuaxxs/s3586s/202207/51b55216c2154332a660157abf28b09d.shtml.

[14] 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(4): 89—103.

[15] BURRI M. Towards a new treaty on digital trade [J]. Journal of World Trade, 2021, 55(1): 77—100.

[16] 王融. 数据跨境流动政策认知与建议——从美欧政策比较及反思视角[J]. 信息安全与通信保密, 2018(3): 41—53.

[17] 习近平. 携手构建亚太命运共同体——在亚太经合组织第二十七次领导人非正式会议上的发言[EB/OL]. (2020-11-20)[2023-10-21]. https://www.gov.cn/gongbao/content/2020/content_5567740.htm.

[18] 杨署东, 谢卓君. 跨境数据流动贸易规制之例外条款：定位、范式与反思[J/OL]. 重庆大学学报(社会科学版), (2021-08-26)[2023-01-02]. https://kns.cnki.net/kcms2/article/abstract?v=vs6GoGUIqCNjhQ-X5l-c4LqSCjkYHzcNHFrMKPi9AurIL3YbkE6ZzmDtRCnhvt1rfw0EMT7XIFXzYeHlHLaT9C5HDg4qUrPxG5oZHfYn58QwdlxbpSllPwkJMeeyrKsjBicL0IrDchw=&uniplatform=NZKPT&language=CHS.

[19] 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(2): 69—87.

[20] DWORKIN R. Law's empire [M]. Cambridge: Harvard University Press, 1986: 176—275.

[21] CITRON D K, SOLOVE D J. Peivacy harms [EB/OL]. (2021-11)[2023-10-21]. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications.

[22] SCHWARTZ P M, PEIFER K N. Transatlantic data privacy law [J]. The Georgetown Law Journal, 2017, 106(115): 120—127.

[23] 宋瑞琛, 冯纯纯. 中美数据跨境流动的国际法规制及中国的因应[J]. 国际贸易, 2022(7): 89—96.

[24] MCGEVERAN W. Friending the privacy regulator [J]. Arizona Law Review, 2016, 58(959): 961—973.

[25] SCHWARTZ P M. The EU-U. S. privacy collision: A turn to institutions and procedures [J]. Harvard Law Review, 2013(126): 1—31.

[26] 许可. 数据主权视野中的 CLOUD 法案[J]. 中国信息安全, 2018(4): 40—42.

[27] 熊鸿儒, 田杰棠. 突出重围：数据跨境流动规则的"中国方案"[J]. 人民论坛·学术前沿, 2021(Z1): 54—62.

[28] PINTO R A. Digital sovereigntyor digital colonialsim [J]. SUR-International Journal on Human Rights, 2018(15): 15—27.

[29] COULDRY N, MEJIAS U A. Data colonialism: Rethinking big data's relation to the contemporary subject [J]. Television & New Media, 2019, 20(4): 336—349.

[30] SCHWARTZ P M. European data protection law and restrictions on international data flows [J]. Iowa Law Review, 1995, 80: 471—496.

[31] MASING J. Herausforderungen des datenschutzes [J]. Neue Juristische Wochenschrift, 2012(3): 2305—2310.

[32] 肖永平. "长臂管辖权"的法理分析与对策研究[J]. 中国法学, 2019, 212(6): 39—65.

[33] 李庆明. 论美国域外管辖：概念、实践及中国因应[J]. 国际法研究, 2019, 31(3): 3—23.

[34] 沈伟. 中美贸易摩擦中的法律战——从不可靠实体清单制度到阻断办法[J]. 比较法研究, 2021(1): 180—200.

[35] 闫文光. 坚持守正创新 助力人权发展——"《人权》杂志创刊20 周年学术研讨会"综述[J]. 人权, 2022(4): 178—186.

[36] 周鲠生. 国际法大纲[M]. 北京: 商务印书馆, 2013: 57—89.

[37] 新华网. 习近平在网络安全和信息化工作座谈会上的讲话[EB/OL]. (2016-04-26)[2024-01-05]. http://www.xinhuanet.com/zgjx/2016-04/26/c_135312437_4.htm.

[38] 陈磊, 彭理云, 单博深, 等. 重要数据安全国家标准的设计思路[J]. 网络安全与数据治理, 2023, 42(11): 53—57.

[39] 祝高峰. 认识与识别：重要数据的界定及其规制路径选择[J]. 社会科学家, 2023(6): 105—111.

[40] 张志洲. 人民日报人民要论：增强中国在国际规则制定中的话语权[EB/OL]. (2017-02-17)[2023-10-21]. http://opinion.people.com.cn/n1/2017/0217/c1003-29086917.html.