浙江理工大学学报,第56卷,第3期,2026年6月
Journal of Zhejiang Sci-Tech University
DOI:10.3969/j.issn.1673-3851(s).2026.03.010

我国数据出境安全评估事项的立法不足与完善

王永杰,潘娅丽
(浙江理工大学法学与人文学院,杭州 311199)

摘　要:我国数据出境安全评估的主要事项包括:出境数据的目的、范围、方式等是否具有合法性、正当性与必要性,数据的规模、范围、种类及敏感程度,数据处理者与接收方对数据的安全保障能力,数据出境后的风险,以及数据跨境传输法律文件的有效性等。然而,当下评估实践面临目的、范围、方式等关键术语内涵不明、数据出境后存在被非法利用的风险、法律文件中的数据安全保护责任难以落实、境外接收方的数据安全保护水平和政策评估难度大等问题。因此,有必要推动安全评估向场景化转型,构建全生命周期的数据安全协同治理机制,建立数据出境案例库,并引入第三方评估机构,以完善我国数据出境安全评估体系。

关键词:数据出境;评估事项;安全评估;自评估;评估标准
中图分类号:D992　　**文献标志码**:A　　**文章编号**:1673-3851 (2026) 06-0348-10

Legislative deficiencies and improvement of security assessment matters for data cross-border transfer in China

WANG Yongjie, *PAN Yali*
(School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou 311199, China)

Abstract: The main matters of the security assessment for China's data cross-border transfers include the legality, legitimacy, and necessity of the purpose, scope and method of the outbound data transfer, the size, scope, type and sensitivity of the data, the security capabilities of data processors and overseas recipients, the risk after data outbound transfers, and the validity of legal documents for data cross-border transfer. Currently, however, there are issues with the assessment matters, such as unclear definitions of key terms like purpose, scope and method, the risk of illegal use of data after outbound transfers, the difficulty in implementing the responsibility for data security protection in legal documents, and the difficulty in evaluating the data security protection policies of overseas recipients. In response to these problems, it is necessary to promote the transformation of security assessment towards scenario-based approaches, establish a full-lifecycle collaborative governance mechanism for data security, create a case database for outbound data transfers, and introduce third-party assessment institutions.

Key words: data cross-border transfer; assessment matters; security assessment; self-assessment; assessment standards

在数字社会快速发展的背景下,数据具有重要的价值,已成为关键生产要素与国家基础性战略资源。与此同时,全球化浪潮推动世界经济联系日益密切,数据出境需求也持续增长。然而,数据频繁出境加剧了数据安全风险。我国数据在境外一旦发生泄露、丢失或被恶意利用,将可能引发连锁反应:轻

收稿日期:2025-12-18　　网络出版日期:2026-05-07
基金项目:国家社会科学基金一般项目(25BFX152)
作者简介:王永杰(1972—),男,安徽寿县人,副教授,博士,主要从事国际经济法方面的研究。

则导致个人信息被盗用、财产受损,重则威胁国家与社会稳定,甚至对国家安全构成直接挑战。

为应对国内外复杂的数据安全形势,《数据出境安全评估办法》(以下简称《评估办法》)明确要求数据出境前必须开展风险评估。现有研究主要围绕数据出境评估制度在适用层面存在的困境展开。有学者指出,评估制度体系存在交叉重复,且与其他制度关联性不足[1-2];也有学者对评估制度规则的适用原则、适用情形和自评估要点进行解读,探讨评估的风险和注意事项[3];还有学者从关键基础设施和重要数据的概念切入,指出制度初期配套细则不完善的问题[4]。然而,现有研究多偏向宏观的制度运用,缺少对评估事项①的关注,导致实务中评估效果不佳。本文以评估事项为切入点,首先分析评估事项所体现的数据主权和国家安全观,进而梳理评估事项的立法缺陷,最后提出完善建议,旨在为数据出境评估实践提供理论支撑与实践指引。

一、《评估办法》设立评估事项的理论依据

当前数字技术已嵌入社会各领域,数据成为社会经济发展的核心资源,数据出境更是释放数据价值的必然选择。《评估办法》所规定的评估事项,看似是对数据处理者与境外接收方的约束,实则彰显了国家数据治理的立场。因此,探究其理论依据,不仅有助于理解制度设计的内在逻辑,更能为数据出境评估提供理论指引。下文将从数据主权与国家安全观视角,阐述评估事项的理论基础。

(一)基于数据主权视角:国家主权在数据领域的体现

数据主权是国家主权在数据领域的延伸,也是构建数据出境安全评估制度的重要理论基础。数据主权是网络主权在数字时代的新发展[5],其核心是国家对数据的支配权,且国家有权决定本国数据参与国际流动的规则。这正是《评估办法》能够对我国数据出境活动进行审查、设立相关评估事项的理论依据。在对内主权方面,数据主权体现为一国对境内数据的支配性权力,强调主权国家对本国数据的绝对主导权[6],是集数据管理权、控制权、立法权于一体的权利,即主权国家有权对本国数据的流入与流出进行规制。然而,数据本质是人类发展过程中发明的二进制编码[7],其无形性、可复制性与可移动性等特征增加了主权国家对数据的管辖难度,因此,必须将数据主权转化为数据处理者的法定义务。例如,《评估办法》第五条对数据出境目的、境外接收方的责任义务及数据保护水平等作出规定,体现了国家对数据出境目的的严格审查。一方面,通过企业自评估机制,确保我国数据流动符合国家立法意图;另一方面,以国内法定标准作为数据出境的基本门槛,间接约束境外接收方的行为。这一系列制度设计,不仅实现了主权国家对跨境数据流动的监督与管控,集中彰显数据主权,也确立了主权国家对本国数据活动所享有的排他性管理权力。

数据之所以在各国备受重视,主要是因为数据在流动中蕴含着经济价值[8]。这就要求数据主权国家正确对待并鼓励数据跨境流动,根据全球格局变化,构建具有弹性的数据主权规则。数据出境安全评估制度的立法目的是在数据主权的基础上,规范数据出境活动的同时促进数据的自由流动。《评估办法》规定安全评估应当审查数据从出境前到出境后整个过程可能存在的风险,以此规范数据处理者和接收方的义务[9]。这一规定既强调对数据出境前后的风险审查,又要避免自我封闭,充分发挥数据要素潜能,积极主动参与国际事务,实现新的经济价值。至此,在对外主权方面,数据主权可以理解为主权国家根据本国需求自主制定数据政策,自主决定参与国际数据治理活动而不受任何其他国家的干预,而这一系列规定都以数据主权为基础。

(二)基于总体国家安全观:数据出境对国家安全的挑战

党的二十大报告以专章的形式系统阐述了国家安全问题,指出必须把国家安全贯穿党和国家工作的各方面、全过程[10]。此处的"总体"二字,既包括政治安全、军事安全等传统安全领域,也包括网络安全、科技安全等非传统安全领域。数据作为国家战略资源,其安全状况与国家安全深度绑定,已经成为总体国家安全观不可或缺的一部分。数据出境安全作为数据安全的重要领域,其制度设计必然以总体国家安全观为前提。数据出境虽有利于我国数字经济发展,但数据流动缺乏规范易引发一系列安全问题。例如境外接收方处理数据的合规性不足、数据泄露后追责与救济机制缺失等,这些问题直接关系到国家安全。同时,数据出境也增加了国家维护数据安全的难度,导致国家安全风险上升。因此,需将

① 本文所称的评估事项,是指数据处理者向境外提供数据前,依法对出境活动的安全性进行系统性审查,包括合法性审查、风险等级判定、境外接收方履约能力、全流程风险防控、合同条款充分性及其他可能影响数据出境安全的因素。

总体国家安全观从理论转化为具体的制度与要求。

从总体国家安全观的视角审视,数据出境对国家安全造成的风险主要体现在内部性风险和外部性风险两个方面。内部性风险表现为数据出境活动本身对国家安全造成的风险。数据一旦出境,国家便丧失了对数据的物理管理权和控制权,且出境数据可能遇到不同的技术与网络环境,如可能被篡改、破坏、泄露、丢失甚至滥用,进而引发严重的国家安全风险,对国家和社会稳定造成威胁。数据出境的外部风险是指数据出境给他人和社会造成非数据层面的影响并借助数据的可复制性和可预测性特征,间接危害国家安全[11]。正是基于对总体国家安全观的把握,《评估办法》第五条明确要求,数据处理者在正式提交评估申请前,须先行开展数据出境自评估。该条规定的评估事项,均蕴含着深远的国家安全考量[12]。《评估办法》第八条则规定,国家评估事项时应审查数据出境活动对我国法律的遵守情况[13],并最终根据安全评估结果决定是否准许数据处理者开展数据出境活动。由此可见,上述具体评估事项均以总体国家安全观为理论前提,具有鲜明的国家安全导向。

二、我国数据出境安全评估事项的立法现状与不足

《评估办法》第五条和第八条分别规定了企业自评估事项和国家安全评估事项①,二者在内容上虽高度重合[14],但国家评估更注重对境外接收方数据安全保护政策法规和网络安全环境的审查。然而,无论是企业自评估还是国家评估,在实践中均面临评估事项界定过于宽泛、数据出境后存在被非法利用的风险,以及法律文件中明确的数据安全保护责任难以落实等挑战。此外,针对境外接收方的数据安全保护水平及其相关政策,国家层面的评估仍面临较高的难度。

(一)数据出境安全评估事项界定过于宽泛

《评估办法》第五条第一项与第八条第一项均对出境活动目的、范围和方式作出规定,且核心需求基本一致,区别在于第五条增加了对境外接收方的评估。对出境目的进行评估,旨在核验数据流向境外的意图是否正当、合法。数据出境的范围应以业务目的所必需为限②,包括但不限于与数据出境目的相关业务功能有直接关联的内容。在数据出境方式上,我国已构建起数据出境安全评估、个人信息出境标准合同、个人信息保护认证等多元路径,出境主体可以结合自身情况和数据类型自主选择,但涉及重要数据或处理100万人以上个人信息等情形的,则依法采用安全评估方式[15]。尽管《评估办法》规定了安全评估的具体事项,罗列了审查要点,虽覆盖范围广泛,但内容以原则性表述为主,条文内容笼统,缺乏具体、可操作的实施细则。

首先,对数据出境目的缺乏体现行业差异化的规则。数据主权要求国家对数据出境享有排他性的支配权,这意味着数据出境的目的始终要契合国家立法意图和安全需求。然而,《评估办法》仅笼统要求评估数据出境目的的合法性、正当性与必要性,未结合行业属性进行细化,忽略了营利性与公益性数据出境的安全风险差异。以金融领域为例,出境的多为商业活动中的数据,以追求经济利益为目的,此类数据风险主要集中在金融信息泄露对国家经济安全的冲击[16]。而在医疗领域,基于跨境医疗会诊、国际医学临床试验等数据出境则具有公益性[17],与追求经济利益为目的的数据出境截然不同。但目前针对不同目的的数据出境的审查标准并未有明确规定。其次,数据出境目的不得违反我国法律或国际义务。在刑事领域,若数据出境目的是对特定种族被告人进行歧视性追诉,因其违背禁止歧视和压迫的法律精神,此类数据出境行为是不被许可的[18]。

其次,对出境数据范围的审查,也存在宽泛、笼统的问题。一般认为,数据出境范围应遵循“最小必要原则”。然而,不同类型、行业的数据出境,它们的最小必要范围差异显著。如何确定数据出境的最小范围,以及通过何种标准判定出境造成的损害最小,目前尚无明确规定,导致法定的评估事项沦为模糊的指引。以智能互联网车辆数据出境为例,不同企业在数据采集、存储以及数据出境数量、范围等方面存在较大差距,此类非必要数据出境的问题频发[19]。司法实践中,左某诉某琴商务咨询公司、某高股份有限公司一案印证了该问题,某高公司基于营销传播目的,将左某的个人信息向位于美国和爱尔兰的某公司传输。广州互联网法院审理后认为,商业营销目的不属于履行合同所必要③。由此可

① 为了兼顾表述的严谨性与区分的便利性,本文将《评估办法》第五条规定的评估事项称为“数据处理者自评估事项”,将第八条规定的评估事项称为“国家评估事项”;若无需对二者作出区分,则统一表述为“安全评估事项”。

② “业务目的”是出于业务开展或合作的需要,境内组织将数据传输给境外组织(可以是本组织的境外分支,也可以是其他组织)。

③ 广州互联网法院(2022)粤0192民初6486号民事判决书。

见,实践中存在“最小必要范围”不明确的问题不仅给企业带来合规困境,也给个人信息安全埋下隐患。

再者,数据安全评估并非针对所有数据,而是仅针对涉及国家安全、公共利益且风险较高的数据。然而,从规模角度看,《评估办法》以个人信息达到一定规模作为触发安全评估的门槛,虽然便于操作,却忽视了我国数字市场规模庞大的现状。这意味着数据纳入安全评估范围,未必是因为该数据涉及国家安全或者公共利益而具有较高风险,也可能是因为数据市场规模过于庞大而被动落入评估范围之中[20]。这分散了本应集中在真正高风险领域的监管资源与注意力,加重监管负担,也不利于提升数据流动效率,难以实现总体国家安全观要求的“安全与发展并重”的目标。此外,数据出境的“目的”“范围”“规模”“种类”“敏感程度”等核心术语内涵模糊,而数据出境与国家安全的关联本就依托数据出境的种类、规模、敏感程度这些要素来衡量[21],这进一步给实践操作带来困难。

(二)数据出境后存在被非法利用的风险

《评估办法》第五条第二项①和第八条第三项②均对出境数据的规模、范围、种类、敏感程度作出规定,但第八条第三项是对第五条第二项和第四项的整合,第五条第二项规定的评估事项与其他评估事项构成并列关系③。在规模上,可从静态标准和动态标准两个维度衡量:静态标准指向境外提供的个人信息数量达到 100 万人以上;动态标准指自上年 1 月 1 日起,累计向境外提供个人信息达到 10 万人,或敏感个人信息数量达到 1 万人。一般来说,数据规模越大,数据的类型越繁杂,数据出境的风险相应越高。针对个人信息的出境,需特别关注其敏感程度[22]。然而,现行法律规定和实际操作存在诸多缺陷,导致数据出境安全屏障存在漏洞,数据仍面临被非法利用的风险。

《评估办法》第五条罗列了自评估的核心要点,要求数据处理者开展风险自评估。为了保障数据出境安全,我国法律对自评估作出了一系列复杂、繁重的要求,出境主体可获得的收益可能还不能够偿付为评估而支付的费用。实践中,出境主体为追逐利益,要么选择不评估,要么选择虚假评估。2025 年 5 月,中国多名用户收到官方警示信息,声称其姓名、手机号码、邮箱、地址等个人信息可能遭到泄露。经公安网信部门调查,泄露原因是某时尚消费品牌将中国用户数据传输到法国总部时未通过任何法定出境途径,未向用户告知并获得同意,更未采取安全技术措施④。该案例表明,安全评估由于各种原因流于形式甚至完全缺失时,数据在未经过任何评估状态下流向境外,国家通过安全评估对境内数据进行管理,维护国家安全、社会公共权益和个人信息的目的已被架空。当法律赋予国家的审查权因企业有意规避而无法行使时,数据出境活动便脱离了国家意志的约束,给国家安全带来威胁。此外,数据处理者的自评估工作既广泛又深入,需要融合运用多种专业知识和技能才能有效完成。例如在涉及刑事数据出境的问题上,若评估团队里缺少刑事司法领域的专业人员,仅依靠企业内部法务人员,往往无法准确识别潜在风险。综上,自评估存在动力不足、能力欠缺、评估效果不佳等问题,间接加剧数据出境后被非法利用的风险。这不仅导致评估流于形式甚至缺失,更导致针对数据出境可能对国家安全、公共利益、个人或者组织合法权益带来风险的评估沦为一纸空谈。这也反映出企业因能力不足而无法有效评估时,国家数据主权无形中被削弱。

当前,数据跨境流动日益频繁,数据已成为影响国家政治安全和社会稳定的重要因素。政治安全作为国家安全体系的核心,若境外势力通过数据跨境流动的技术漏洞获取大量的个人、企业和政务数据,极可能通过数据的聚合效应与深入挖掘,对我国社会状况进行精准画像,有针对性地开展情报工作[23],窥探我国政治等领域机密,甚至通过舆论对社会价值观进行渗透,影响政治安全和社会稳定,极易对国家安全、商业机密、社会公共利益和个人的合法权益带来威胁,也将冲击我国意识形态安全。不同类型的数据,其重要程度与敏感程度因场景而异,但《评估办法》未对不同类型和不同敏感程度的数据作出不同规定,最后得出的评估结果是否科学存疑,甚至可能导致高敏感数据被当作低敏感数据处理,对真正敏感或者关键数据可能无法充分揭示其出境

---

① 该条款要求评估出境数据的规模、范围、种类、敏感程度,数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险。

② 该条款要求评估出境数据的规模、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。

③ 参见《数据出境“安检”新规——〈数据出境安全评估办法〉深度解读》,载于网络安全应急技术国家工程中心网站,https://www.dehenglaw.com/CN/tansuocontent/0008/023056/7.aspx?MID=0902。

④ 公安部 2025 年 9 月 18 日公布的“护网—2025”专项工作行政执法典型案例,详见网址:https://www.mps.gov.cn/n2254098/n4904352/c10237071/content.html。

后面临的极端威胁。敏感程度不同的数据混杂传输出境,会使高敏感数据受到低敏感数据的影响。例如,低敏感数据遭到泄露,可成为攻击高敏感数据的跳板,可能引发连锁反应,给高敏感数据带来威胁。针对生物医药、金融、军事等高度敏感领域的数据出境,该办法尚未制定出专门的保护性条款,难以充分应对这些领域的特殊需求与挑战。以金融领域为例,我国企业开展境外投资时,其他国家要求我国企业或金融机构披露金融数据,这可能违反我国法律并引发金融数据安全风险。更关键的是,现行规定对风险评估的前瞻性不足。生成式人工智能(GAI)作为新兴技术被广泛应用,而法律具有滞后性,这就导致现行法律规定未能涵盖GAI数据跨境流动情景,容易引发数据主权、国家安全、数据隐私等问题[24],使数据跨境流动的风险加剧。我国作为全球数据生产和消费大国,各领域都源源不断地产生海量数据资源,其中不乏涉及国家机密、敏感信息以及公民个人隐私的数据。一旦此类数据在跨境流动过程中遭遇非法窃取、恶意篡改或意外丢失,将严重危害国家利益与社会稳定。以ChatGPT为例,用户使用该平台进行提问时,所有信息都会传输至OpenAI公司服务器进行处理[25],这些信息可能存在被用于商业开发甚至政治目的的风险。

(三)法律文件中的数据安全保护责任难以落实

《评估办法》第五条第五项①与第八条第五项②均要求评估境内外双方拟订立的法律文件。评估重点在于数据出境相关合同及其他法律文件是否详尽约定了数据安全保护责任和义务,以及境外接收方的数据管理水平和技术措施能否保障数据安全,确保其数据保护水平符合我国现行法律、行政法规和强制性国家标准。《评估办法》第九条进一步细化了法律文件应涵盖的必要事项,包括数据出境后的存储介质、存储时长及使用目的,明确数据接收方留存数据的合法期限、数据转移限制条款,以及发生数据安全事件时的违约责任和争议解决方式[22]。

然而,这些规定多停留在原则性和方向性的指导层面,这种原则性规定过多、实操性指引不足的困境,导致数据处理者和境外接收方开展数据相关工作时,对其数据安全保护责任与义务认识不足。在具体执行过程中,相关主体往往只关注并履行某些表面化、浅显的义务,而没有认识到深层次、核心的数据安全保护责任。这使得评估人员在实践中难以准确把握评估标准,导致法律文件中的数据安全保护责任难以有效落实。《评估办法》第九条规定,数据处理者应当与境外接收方在法律文件中明确约定数据安全保护责任义务。从条文表述可见,落实这一义务主要涉及两类主体,即数据处理者和境外接收方。

首先,从数据处理者的角度来看,由于不同国家和地区的数据安全保护法规、防护能力与监管力度存在显著差异,部分国家和地区的数据保护水平与我国标准、要求差距较大。在此背景下,若数据处理者计划向境外传输数据,经过初步评估发现,数据接收方所在国家或地区的整体数据保护水平未能达到我国法律要求,其数据出境安全评估往往难以通过监管部门的审核。对于以数据跨境传输为业务开展必要前提的企业或机构而言,这可能直接影响其跨国业务的正常推进。部分数据处理者可能放弃通过合规途径,转而通过非法手段规避监管审查。例如绕开法定安全评估程序,私自开展数据跨境传输,或者将原本需要整体申报评估的大批量数据拆解成若干小批量数据片段,以降低单次数据传输规模。一旦数据出境主体采取上述非法手段,原本在法律文件中明确的数据安全保护责任义务将彻底失去法律效力,无法真正落地。尽管目前公开案例中,鲜有数据处理者因数据出境违法、违规出境数据的事件而被追责,但从上述时尚消费品牌公司公然漠视数据出境合法路径、违规出境数据的事件不难看出,即便数据处理者签订了数据保护相关的法律文件,也有可能因企业主观违规而形同虚设。

其次,从境外接收方的角度来看,即便在数据出境流程正式启动前,境外接收方已与数据处理者签订了数据安全保护文件,且在前期表现出积极配合的态度,也不意味着其在实际接收数据后会始终严格恪守约定。数据出境后便由境外接收方实际控制,但受境外数据监管环境、接收方运营成本、内部安全管理体系或短期利益等因素影响,其仍有可能出现“阳奉阴违”的情形,即形式上履行数据安全保护义务,实际上却未落实相应的安全防护措施,最终导致前期签订的法律文件沦为空文,约定的数据安全保护义务难以落地。

同时,目前仅有少数企业拥有对境外接收方数

① 该条款规定,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。

② 该条款规定,数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务。

据安全保护能力的评估能力,对数据处理者和境外接收方数据安全保护水平的评估方式存在明显的局限性。环球律师事务所与南方财经全媒体集团合规科技研究院组成的联合研究团队调研显示,仅有77%的受访企业通过合同条款约束境外接收方履行责任义务,只有极少数企业具备派遣专业人员实地考察的能力(6 家),或要求对方出具合规报告(6 家)①。这种以合同约束为主的被动管理模式,既反映出多数企业在跨境数据安全管理上的资源不足与执行乏力,也凸显了当前评估机制对境外主体实际管控能力的薄弱。

此外,评估事项要求评估个人信息维权渠道是否通畅,但通畅的具体标准缺乏清晰的指标。例如,个人信息主体投诉后的响应时间、问题解决时限、境外联系人及联系方式、争议解决的流程等未得到明确。这使得数据处理者在自评估时只能进行形式化描述。实践中,极易出现对个人信息主体的投诉长期不响应或公布的联系方式失效、境内数据处理者与境外接收方互相推诿的情况。更关键的是,《评估办法》只关注有无维权渠道,却未构建完整的救济路径。《个人信息出境标准合同》虽要求境外数据接收方承担相应义务,但当境外接收方不履行义务时,个人信息主体应通过何种途径主张权利,并未作出明确规定。

(四)对境外接收方数据安全保护水平及政策的评估难度大

数据安全关乎国家安全,在保障数据跨境安全时,尊重国家主权是一项重要的国际法原则。这意味着每个国家都有权自主制定数据保护法律,因此在数据出境安全上,各国可以要求数据接收方提供与其同等水平的保护。《评估办法》第八条第二项将境外接收方所在国家或者地区的数据安全保护政策法规、网络安全环境对出境数据安全的影响,以及境外接收方的数据保护水平是否达到我国法律法规的规定和强制性国家标准的要求,纳入国家评估事项的范畴。这意味着数据出境前必须对境外接收方的数据安全保护水平进行评估。这种评估模式类似于欧盟的“充分性认定”模式,即只有数据进口国的数据安全保护水平达到数据出口国所认定的充分性保护标准时,数据才能够跨境传输。但实践中因缺乏具体的细则指引,面临一系列困难。首先,由于缺乏具体细则,不同评估人员对同一事项基于不同的理解做出不同的判断,造成评估结果不一致。其次,我国尚未建立数据跨境白名单制度,每次数据出境都需要重新评估境外接收方的数据安全保护水平,大幅增加了劳动成本和时间成本。

实践中,上述两方面的评估挑战主要源于各国法律环境的差异性以及政策法规的动态变化。首先,不同国家和地区的历史传统、文化背景和社会制度存在差异,其法律框架和监管体系也截然不同,在数据保护、隐私保护、网络安全等方面的法律法规差异明显。不同国家和地区的文化差异不仅影响法律政策,也给评估工作增加难度。评估人员不仅要深入了解境外接收方所在国家或地区的数据安全保护政策与网络安全环境,还需将其与我国法律要求进行对比。据斑马数据研究中心调研,深圳数交所认为在实际业务开展过程中,域外法律政策识别和数据安全环境评价等事项因涉及域外法律解读与监管实践调研等,实际执行难度极高。

除法律环境差异外,境外接收方所在国家或地区的数据安全保护政策并非一成不变的。近年来全球数据主权意识增强,各国都加快数据立法进程,频繁出台或修订数据保护法律法规。这要求评估人员持续学习和更新知识,否则可能导致评估结论不准确。即便部分境外接收方的法律政治环境相对稳定,但由于我国数据出境频繁、数据出境主体数量较多,每个数据出境主体独立评估,可能对同一个国家或地区重复评估[26]。目前,我国缺乏由国家或第三方机构提供的数据安全保护政策和法律环境评估,导致企业各自为政、合规成本高。上述因素叠加,使得对境外接收方的安全保护环境政策评估难度较大②。此外,需要评估的国家和地区要根据境外接收方所在地确定,即数据流向哪里,就需关注当地的数据安全保护政策。通常,境外接收方一般指第一手境外接收方,但在跨境数据传输的实践中,存在数据再传输的情况,即第一手境外接收方在接收数据后,可能会将数据进一步传输给其他境外主体。这种情况在跨国企业的内部数据共享、供应链数据流转以及国际合作项目中较为常见。由于第三方境外接收方的数据安全保护政策千差万别,国家在评估时是否需要覆盖所有主体成为难题;若不对其评估,则会加剧数据出境风险;若逐一评估,将显著增加评估的工作量和难度。

---

① 斑马数据合规研究中心 2023 年发布的《数据跨境现状调查与分析报告》,第 41 页。

② 斑马数据合规研究中心 2023 年发布的《数据跨境现状调查与分析报告》,第 43 页。

三、完善我国数据出境安全评估事项的路径

数据出境安全评估事项的设立,旨在规范数据跨境流动秩序,兼顾数据出境安全与数据资源利用的关系。然而,维护国家安全仍然是数据出境监管的底线。根据上文分析,我国数据出境安全评估仍存在评估事项界定过于宽泛、数据出境后存在非法利用的风险等问题,将对国家安全、社会公共利益、个人或组织的合法权益构成威胁。因此,应从推动安全评估转型、构建全链条风险监测体系、建立案例库与监管救济体系,以及引进第三方评估并与国际接轨等四方面入手,为我国数据出境安全评估提供优化路径。

(一)推动安全评估向场景化转型

当前,《评估办法》规定的评估事项界定过于宽泛,核心问题是原则化过高,无法应对不同行业数据的敏感性差异,也忽视了同一行业内不同场景的风险区别,导致数据出境监管资源可能被低风险的数据活动占有,而真正的高风险数据未能得到充分关注。为了保障数据出境活动在总体国家安全观的框架下进行,也为了解决上述困境,2024年3月国家网信办出台实施的《促进和规范数据跨境流动规定》(简称"《跨境规定》"),正式确立了数据出境负面清单管理模式。在《跨境规定》的指引下,全国各自由贸易试验区纷纷制定各具特色的数据出境负面清单,对数据按行业、场景进行划分,为应对评估事项界定过于宽泛带来的困境提供解决路径。

负面清单不再是孤立地强调数据出境目的、范围、规模、敏感程度等评估维度,而是将评估维度与具体的场景关联,以实施差异化监管和动态调整阈值,解决因规模僵化而触发评估的问题。上海2024版数据出境负面清单将数据出境规模、敏感程度与风险紧密关联。针对低风险场景,扩大敏感个人信息出境规模。例如,在商贸领域会员管理场景下,将敏感个人信息出境阈值从1万人大幅提升至100万人,且将场景名称前置单列,并增加解释性说明,便于企业直接对照。天津数据出境负面清单也将跨境电商领域商家入驻场景的敏感个人信息阈值设定为200万人。而北京数据出境负面清单首创行业、应用场景、数据字段特征三维识别表,按应用场景设置差异化门槛。例如对于汽车行业,不再笼统评估,而是细分至军工车辆数据、车外图像数据、车联网信息服务数据等具体场景,并列举每个场景下受关注的数据字段。这意味着,对出境数据范围的审查,由原来的主观判断很大程度上转为依据客观场景来判断是否落入清单范围,将宽泛的评估事项聚焦到具有明确业务目的的场景,以便数据出境活动最大限度地维护国家核心利益。

(二)多元共治,构建全链条风险监测体系

针对数据出境主体自评估能力不足、评估意识不强、人才短缺等问题导致数据出境后被非法利用的情况,可以充分动员社会力量监督企业数据出境行为,引导民间力量参与数据出境安全评估活动。当前,我国数据出境安全评估依赖以国家网信部门为主的国家机关和政府部门,缺乏民间力量的参与。对此,我国可以借鉴日本"政府主导、民间参与"的治理经验,构建具有中国特色的"政府统筹+行业协会+市场主体"的治理格局。在具体的实施路径上,可由国家网信部门发挥主导作用,牵头成立全国性的数据出境安全协会,积极吸纳具备专业知识的法律服务机构、科研院所等社会力量,制定数据出境安全评估的行业标准和操作指南,建立专业人才培训体系,搭建企业自评估技术支撑平台,辅助企业完成数据出境安全评估工作,以提高数据出境安全保障水平。

此外,在数据出境安全评估过程中可融入风险监测思维。针对生物医药、金融、军事等高度敏感领域的数据出境,需联合该领域专业机构与人士,协同制定专门的评估细则和保护条款。以汽车领域数据为例,《汽车数据安全管理若干规定(试行)》第12—14条明确规定,国家网信部门可联合国务院有关部门,采用抽查方式检查已经出境的重要数据与其在出境前评估所声称的目的、范围、方式、种类和规模是否一致,境内的汽车数据处理者应该给予配合。在每年的固定日期(12月15日)前,境内的汽车数据处理者向有关部门报告汽车数据在境外的保存情况,包括地点、期限、接收者情况[①]。

科技发展一日千里,滞后性是法律的内生问题。随着GAI的迅猛发展,GAI数据跨境流动日益频繁。为应对GAI数据跨境流动带来的风险,需建立政企协同、多方参与的数据跨境治理机制。一方面要明晰各主体的数据安全责任,构建以政府为主导、各私营机构积极参与、行业组织协同发力的治理机制。另一方面由政府统筹风险评估框架,企业落实风险核查与整改责任,行业组织则通过制定行业自

① 参见《汽车数据安全管理若干规定(试行)》第12-14条。

律规范与技术标准,形成硬法与软法互补、政策与市场同步的治理机制。在完善制度保障的基础上,还需从技术层面强化监管。我国政府应推动技术创新,通过税收优惠、基金扶持等措施,鼓励企业研发更安全、更高效的数据传输技术,提升企业数据保护能力,降低数据出境后的安全风险。此外,要建立争端解决机制,在数据遭到非法利用后能够及时通过有效渠道解决。

(三)建立数据出境案例库,构建动态监管机制与救济体系

针对《评估办法》关于境外接收方数据安全保护责任义务的规定偏原则化、实操性不足的问题,应根据数据出境不同场景,出台具体的、可操作性的指南,使数据处理者和境外接收方在评估时能够准确把握,也更能深入理解各自应承担的责任和义务。法律条款具有原则性和抽象性,企业在实际执行中通常不知如何操作,可以模仿法律案例库的方式,在数据出境方面也建立相应的案例库,将抽象的责任要求转化为具体的行动指南。案例库可收集不同行业的典型案例,按出境场景和问题类型进行划分,并保持持续更新,不断加入新的案例以供各主体参考。案例库中成功的案例可以给企业提供经验,失败的案例能够给企业提供参考,避免其重蹈覆辙,也能够增强企业的危机意识和保护出境数据安全的责任感。

针对不同国家或地区的数据保护水平不同的问题,可鼓励国际合作,开展国际专家交流活动,对数据出境安全保护水平欠发达的国家或地区给予帮扶,从技术和管理两个方面提高其数据安全保护水平。一是在技术方面,帮助欠发达国家或地区提高数据加密技术,同时完善其数据安全应急保护机制。二是在管理方面,通过与欠发达国家或地区开展人才跨境交流,对相关法律法规和政策进行讲解,助力其培养具有数据跨境安全管理能力的高级管理人员。针对数据处理者通过非法手段规避监管的问题,可采取技术识别、法律规制相结合的方法。在技术方面,建立数据跨境监测平台,利用人工智能分析企业的异常数据出境行为,例如自动识别同一主体频繁向同一目的地发送小规模数据包的可疑操作。在法律规制方面,加大对违规数据出境行为的处罚力度,增加违法成本。

面对境外接收方表面配合、实则阳奉阴违的行为,必须打破当前“过度依赖其自主整改”的被动局面,构建动态化实时监管机制,对数据的流向、流动轨迹实施全程追踪,重点监控数据在境外接收方所在国家及地区的存储、加工、使用等一切与数据安全相关的活动。一旦捕捉到异常数据信号,第一时间触发警报机制。若仅为轻微异常,可及时通知相关监管部门开展核查,并推动整改修正;若发现境外接收方存在数据滥用、违规泄露等严重违规行为,应立即通过远程技术手段废除访问密钥,或启动数据自毁程序,从源头遏制风险蔓延。此外,可借助区块链技术不可篡改的特性,对已出境数据的全生命周期进行追溯与校验。当数据出境的实际路径、传输时间、操作方式等关键信息与预先报备的信息出现偏差时,区块链技术能快速完成溯源定位,及时锁定问题根源[27]。

而针对个人信息维权渠道的问题,也应建立相应的监管机制。首先应制定响应时效,如明确个人信息主体投诉后的响应与处理时限,要求境外联系人在收到投诉指定工作日内完成首轮响应并告知处理进度与处理的具体时限,可根据不同类型投诉设置差异化的处理时限。其次,为防止个人信息主体的投诉长期不响应导致维权渠道形式化的问题,评估时应要求境外接收方出具佐证材料,例如提供近一年的投诉处理记录。最后,应确立个人信息救济的具体流程,同时可由官方设立跨境数据争议调解中心,为个人信息主体提供便捷的救济渠道。

(四)引入第三方评估机构并与国际接轨,降低评估难度

由于境外接收方的数据安全保护政策法规涉及范围较广,国家在进行评估时开展实地考察不仅难度大,还会增加成本。尽管各国的数据安全保护政策、网络安全环境处于动态调整之中,但亦具有一定的稳定性。在数据出境时,若由每个数据出境主体独立评估境外接收方数据安全保护政策,会面临成本高昂、难度大,且评估工作效率低下、造成大量重复性劳动费时费力等问题。针对这一情况,可引入第三方评估机构,由其负责对境外接收方所在国家和地区的数据安全保护政策法规进行评估并划分风险分级[19]。在引入第三方评估机构时,监管部门应对其评估资质和评估能力进行监督。第三方评估机构不仅须具备安全评估能力,还应依法取得相关评估资质,定期向监管部门汇报工作、反馈结果,确保评估的客观性和可追溯性。通过出境处理者自评估与第三方评估相互配合,构建更科学的评估框架,避免因利益驱动引发评估偏差或违规行为。

对境外接收方所在国家或地区的法律政策环境

进行评估时,可借鉴国际经验。例如,欧盟发布了两项与此相关的建议文件,分别是《关于补充传输机制以确保遵守欧盟个人数据保护水平的建议》和《关于监控措施的欧盟重要保障建议》。这两份文件规定在审查境外接收方所在国家的法律环境时,要求评估境外接收方是否有数据安全保护法律,第三国的立法或执法机构对个人权利和自由进行限制是必要的且具有适当性。此外,第三国应当拥有独立的监督机构,保障数据安全保护措施有效执行,以及在个人数据权益受损时,数据主体能够通过合法渠道获得司法或其他形式救济。结合国际经验和本国实际情况,我国可以从法律体系、国际承诺、落实机制、机构权力四个方面来评估境外接收方所在地的法律和政策环境。在法律体系层面,评估境外接收方所在国个人信息保护、网络安全和数据安全方面的法律法规及其完善程度,并与我国法律进行对比。在国际承诺层面,主要考察境外接收方所在地是否加入区域性或全球性数据保护组织,以及是否作出具有法律约束力的国际承诺。在落实机制层面,关注境外接收方所在国是否有监管机构,能否有效监督数据安全事件。在机构权力层面,分析境外接收方所在国执法机关和司法机关在数据获取方面的权力,是否存在有效的执法和司法机制,是否有相关负面案例。国家网信部门可根据上述维度及第三方机构的评估结果,通过官网及时发布存在高风险的数据出境国家或地区的警示信息。

四、结 语

当前数字经济蓬勃发展,数据出境日益频繁,由此引发的国家安全、社会公共利益和个人信息保护等风险逐渐增加。为维护国家安全和社会公共利益,我国颁布《评估办法》为数据出境安全评估提供法律依据,其中,评估事项是数据出境安全评估制度的重要组成部分,其科学性与执行效果影响评估公信力,也与国家贸易和数字经济发展密切相关。本文在数据主权和总体国家安全观的基础上,梳理我国数据出境安全评估事项的立法现状,结合实践案例,指出现行评估事项界定宽泛、风险管控以及责任保障等方面存在的问题,并据此提出针对性优化路径。本文旨在提高自评估和安全评估的科学性,为数据处理者和国家网信部门开展数据出境安全评估工作提供参考,保障数据出境安全。

中国数据出境安全评估事项的完善需要循序渐进,未来评估事项完善应着眼于动态风险预防。特别是生成式人工智能的发展极大地丰富了数据出境场景,同时也带来更多风险,这要求数据出境安全评估具备前瞻性,能敏锐识别和应对新型数据安全风险。应当构建出境信息安全动态防护系统等新兴技术对可能危害国家安全、社会公共利益和个人信息的数据出境行为进行规范。唯有在保证国家安全的前提下,最大程度地降低企业合规成本,提升跨境企业数据出境效率,激发数据潜能与价值,才能增强我国在全球数字经济中的综合实力。

参考文献:

[1] 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(2):62-72.

[2] 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.

[3] 王春晖.数据安全出境评估规则与适用:《数据出境安全评估办法》解读[J].南京邮电大学学报(社会科学版),2022,24(4):1-10.

[4] 马光.论我国数据出境安全评估制度构建[J].上海政法学院学报(法治论丛),2023,38(3):126-137.

[5] 文铭,谭榕.数据主权视阈下数据跨境流动监管合作及中国因应[J].国际贸易,2024(6):5-14.

[6] 冉从敬,刘妍.数据主权主体论[J].武汉大学学报(哲学社会科学版),2024,77(2):41-50.

[7] 王玫黎,陈雨.中国数据主权的法律意涵与体系构建[J].情报杂志,2022,41(6):92-98.

[8] 胡东兰,夏杰长.数据作为核心要素的理论逻辑和政策框架[J].西安交通大学学报(社会科学版),2023,43(2):107-118.

[9] 尉明洋.中国数据跨境流动安全的类型化法律规制研究[C]//外交学院国际法系.《新兴权利》集刊2025年第1卷:部门法的数字化进路研究文集,2025:65-78.

[10] 徐拥军,王兴广.总体国家安全观下的跨境数据流动安全治理研究[J].图书情报知识,2023,40(6):20-30.

[11] 熊光清,张素敏.总体国家安全观视角下我国数据出境安全管理制度的完善[J].哈尔滨工业大学学报(社会科学版),2023,25(5):32-40.

[12] 梅傲,陈子文.总体国家安全观视域下我国数据安全监管的制度构建[J].电子政务,2023(11):104-115.

[13] 李爱君,王艺.数据出境法学原理与实务[M].北京:法律出版社,2023:181.

[14] 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.

[15] 马其家,李晓楠.论我国数据跨境流动监管规则的构建[J].法治研究,2021(1):91-101.

[16] 陈统.数据出境风险自评估机制的理解与适用[J].企业经济,2023,42(4):143-152.

[17] 马兰.金融数据跨境流动规制的核心问题和中国因应[J].国际法研究,2020(3):82-101.

[18] 何晶晶,张心宇.中国健康医疗数据跨境流动规制探析[J].国际法研究,2022(6):62-74.

[19] 郑曦.刑事数据出境安全评估制度研究[J].法学论坛,2023,38

(4):128-138.
[20]邱诗韵,林梓瀚.智能网联汽车产业数据出境安全机制构建探析[J].信息通信技术与政策,2024,50(8):73-79.
[21]刘辉,吴俊雄.总体国家安全观下数据跨境流动法律治理优化研究[J].电子科技大学学报(社科版),2025,27(6):91-102.
[22]李晓楠,宋阳.国家安全视域下数据出境审查规则研究[J].情报杂志,2021,40(10):74-82.
[23]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(5):14-24.
[24]姚迁,刘晋名,盛小宝.生成式人工智能数据跨境流动的安全风险及治理范式[J].网络安全与数据治理,2024,43(12):80-87.
[25]王大志,张挺.风险、困境与对策:生成式人工智能带来的个人信息安全挑战与法律规制[J].昆明理工大学学报(社会科学版),2023,23(5):8-17.
[26]杨洁.合法预期保护原则下的数据出境安全评估制度完善[J].北方法学,2024,19(6):18-33.
[27]谢波,李玉菁.我国数据出境安全管理的数字生态审视及其制度机制优化[J].科技智囊,2025(3):54-64.

(责任编辑:陈丽琼)