武汉大学学报(哲学社会科学版)
WUHAN UNIVERSITY JOURNAL (Philosophy & Social Science)
第75卷第6期 2022年11月
Vol. 75 No. 6 Nov. 2022 030~040
DOI:10.14086/j.cnki.wujss.2022.06.003

国际体育赛事数据跨境传输的规则适用问题研究
——以北京冬奥会数据跨境传输为视角

肖冬梅 苏 莹

摘 要 由于各国(地区)数据治理规则不一致,当前国际体育赛事承办者面临数据跨境传输的规则适用难题。根据欧盟数据跨境传输规则,冬奥会承办者收集境外欧盟参赛者个人数据的可行路径有:一是获得充分性保护水平认定,二是通过BCRs及SCCs及行为准则提供适当保护措施,三是适用公共利益例外规定。在欧盟"软数据本地化存储"的规则体系下,以上三条路径都还面临挑战。国际奥委会通过合同要求北京奥组委在冬奥会结束之后,将所有赛事相关数据转移至瑞士的国际奥委会总部,这有违我国数据本地化存储的原则规定。在目前尚未形成通行国际数据处理规则的情况下,解决国际体育赛事数据跨境传输规则适用难题的可选路径有:一是在协议中设置合规性保护义务条款,二是适用标准合同条款及约束性企业规则工具,三是推动建立双边或者多边合作机制,四是推动制定我国体育产业数据保护规范。前三条路径都有其局限,第四条路径是目前解决国际体育赛事数据跨境传输合规问题的优选方案。

关键词 国际体育赛事;个人信息保护;数据主权;数据跨境传输
中图分类号 G80-05;DF92 **文献标识码** A **文章编号** 1672-7320(2022)06-0030-11
基金项目 国家社会科学基金重大项目(21&ZD169)

当前,各主权国家(地区)争相制定数据治理规则,对数据的产生、收集、存储、流动等活动进行规范,其目的在于更好地保护其国民权益和数据主权,并取得数字经济发展的竞争优势。但数据跨境自由流动和安全流动一直是数据治理规则构建中不可回避的一对矛盾。虽然从1980年起,经济合作与发展组织《隐私保护和个人数据跨境流动指南》就将"数据跨境流动"纳入法律议题,但进展缓慢,从20世纪80年代到2013年,能满足各国破除贸易壁垒需求的"数据自由流动"主张一直占据主流,直至2013年"斯诺登事件"引发全球范围内的"数据本地化"立法运动,60个国家实施了数据本地化法律①。近年来,随着数据跨境流动日益频繁,单纯的数据"本地化存储"局限凸显,扩张国家管辖权、对跨境数据进行"域外管辖"成为不少发达经济体的选择。在国际法上,域外管辖并不是一类独立的管辖权,可以理解为一国在其境外行使主权权力或权威[1](P169)。典型的有2016年欧盟颁布《一般数据保护条例》(General Data Protection Regulation,简称GDPR),其"影响主义原则"将数据保护监管扩展到欧盟境外②;2018年美国《云法案》(The Clarifying Lawful Overseas Use of Data Act,简称The CLOUD Act)通过长臂管辖原则扩张了管辖范围。为确保对本国数据的控制、管理与利用,我国自2016年以来相继颁布《网络安全法》《数据

① "数据本地化(data localization)"是主权国家进行数据管控的一种方式,要求数据控制者将在一国收集的数据(个人信息和非个人信息)存储在境内,经审查方可跨境传输。

② GDPR第3条基于传统属人管辖和属地管辖的连接点,从数据处理行为的效果入手,将欧盟境内机构境外处理个人数据的行为和欧盟境外机构处理欧盟境内个人数据的行为纳入管辖。

安全法》《个人信息保护法》等法律，构建了较为严密的数据限制性流动规则体系。基于以上国际数据跨境传输的现状，本文将结合北京冬奥会数据跨境传输的案例，探讨国际数据跨境传输规则适用难题的可选路径。

一、问题的提出

举办国际体育赛事涉及境外参赛者数据的流入和赛事期间在境内产生大量数据的流出问题。大型国际体育赛事尤其是冬奥会这样的赛事因其规模大、项目广、参与人数众多，且涉及市场化运作[2]（P26-28），须收集境外众多参赛者的个人数据；境外参赛者亦会在我国境内产生大量数据。大量数据的跨境传输，不管是流入或流出，都受相关主权国家（地区）有关数据跨境传输规则的规制。由于欧盟通过GDPR确立了域外管辖规则，我国构建了数据限制性流动规则，使得北京冬奥会组委会不管是赛前从境外收集数据，还是赛后按要求将数据转移至国际奥委会，都存在难以回避的规则适用难题与合规风险。

（一）收集境外参赛者个人数据的合规风险

我国作为赛事承办方，一方面，为组织、协调、参与赛事筹备和举办活动，北京冬奥会和冬残奥会组织委员会（以下简称北京奥组委）等相关主体必须收集境外参赛者个人数据。根据《奥林匹克宪章》第41条①的规定："运动员、教练员、训练员或随行官员等参加冬奥会的资格必须由所在国国家奥委会报名。"而依据该宪章第44条，冬奥会举办的邀请和报名具体程序为"在冬奥会开幕前，国际奥委会将参加冬奥会的邀请发给所有国家奥委会，所有的国家奥委会根据国家单项体育协会推荐的名单为运动员报名②，并按国际奥委会的规定向北京奥组委提交。"③可见，通过冬奥会运动员注册与报名程序，参加冬奥会的运动员、教练、随行官员的个人数据，还有境外观众购票所提交的个人数据以及境外媒体记者入境采访报道所提交事先审核的个人信息等，不得不从其所在国传输至我国境内。另一方面，以欧盟为代表的国家与地区严格限制个人数据跨境传输，从境外收集举办国际体育赛事相关的必要数据遭遇制度壁垒。因为根据GDPR的规定，如果欧盟委员会没有认定数据传输的目的地第三国具有与欧盟相当的数据保护水平（即未达到"充分性保护水平"），欧盟个人数据的跨境传输应当以GDPR第46条中的数据传输工具（包括标准合同、约束性企业规则、行业准则）为基础。由于中国不是欧盟认定的充分性保护水平国家，那么作为赛事举办者收集来自欧盟的运动员、裁判、观赛人员等主体的个人数据，不能直接适用GDPR有关"充分性保护水平"的规定。若不采用合适的数据传输工具就直接收集境外欧盟参赛者个人数据，面临合规风险，但若采用数据传输工具则有削足适履之嫌。

（二）赛后将赛事数据向境外转移的合规风险

依据北京奥组委与国际奥委会订立的《2022年第24届冬奥会主办城市合同》（以下简称《主办城市合同》），北京2022年冬奥会举办所产生的相关数据独属于国际奥委会所有，国际奥委会要求冬奥会结束之后北京奥组委将所有相关数据转移至瑞士的国际奥委会总部。可见，北京奥组委作为受委托方仅在合同的权限范围内为举办冬奥会收集、处理相关数据，须在冬奥会结束之后将所有北京2022冬奥会相关数据转移至瑞士的国际奥委会总部。另一方面，北京奥组委若依约进行数据跨境传输，将面临合规风险。北京奥组委将冬奥会相关数据转移至国家奥委会需满足我国的数据出境传输规则。我国《网络安全法》确定了我国关键信息基础设施收集和产生的个人信息以及重要数据的本地化存储原则；《数据安

① 《奥林匹克宪章》第41条"参赛资格条例"规定：运动员、教练员、训练员或其他随队官员要想具备参加奥林匹克运动会的资格，必须遵守《奥林匹克宪章》以及经国际奥委会批准的相关国际单项体育联合会的规则，并且由其国家奥委会报名。

② 《奥林匹克宪章》第44条"邀请及报名"第1款规定：参加奥林匹克运动会的邀请应由国际奥委会于开幕式前一年发送给所有国家奥委会；第3款规定：国家奥委会只能根据国家单项体育协会推荐的名单为运动员报名。如果国家奥委会予以批准，应将该报名名单报送奥运会组委会。奥运会组委会收到后必须予以确认。国家奥委会必须审查各国家单项体育协会推荐的报名名单的有效性。

③ 《奥林匹克宪章》第44条"邀请及报名"规则的细则第3款规定：所有报名必须按国际奥委会的规定提交。

全法》进一步明确重要数据的出境安全管理、主管机关批准、法律责任承担等多方面的规定,严格限制重要数据出境;《个人信息保护法》规定了个人信息出境的合规要求,列明允许及禁止个人信息出境的情形,明确安全评估等个人信息出境程序,在本地化存储一般性原则的基础上提供个人信息保护认证与境外签订合同等跨境传输办法。据此,北京奥组委为履行《主办城市合同》,需要通过国家网信部门的安全评估或者经由其他合法正当途径才可以向境外传输数据。否则,向境外转移赛事数据将面临合规风险。

可见,我国作为冬奥会的承办方,从欧盟境内收集参赛者或消费者的个人数据,需要遵守GDPR对个人数据跨境传输至第三国的规定,虽然可以选择签订符合GDPR有关个人数据跨境传输规则的标准化合同,但此举不仅是削足以适履,且承办方的合规成本不菲;赛后北京奥组委悉数将冬奥会举办所产生的相关数据从中国境内转移至国际奥委会,履行《主办城市合同》义务,势必与我国数据本地化存储的一般性原则相冲突,这种妥协事实上是对我国数据主权的让渡。本文将以北京冬奥会数据跨境传输这一具体场景为视角,剖析国际体育赛事数据跨境传输的规则适用难题及其解决路径。

二、收集境外欧盟个人数据的有关规则及其适用问题

我国作为冬奥会等国际体育赛事的承办方,从欧盟境内收集参赛者或观众的个人数据,合规依据主要是欧盟通过GDPR明确的个人数据跨境传输至第三国的有关规定。

(一)欧盟个人数据跨境传输至第三国的有关规定

依据GDPR的规定,欧盟的个人数据跨境传输至第三国的可选路径[①]包含:"获得充分保护水平认定"或"提供适当保护措施"或"适用可行例外"。跨境传输个人数据时应依次适用这三条路径,即首先考量个人数据接收国是否达到充分保护水平,其次考量其是否提供适当保障措施,最后考量传输是否属于例外情形。

1. 获得充分保护水平认定

依据GDPR第45条,当欧盟委员会认定第三国或者特定部分或国际组织等的数据保护水平与欧盟实质性等同时,向相关国家或组织的传输被视同为在欧盟内部进行。由此,来自欧盟的个人数据可自由跨境流动[②]。欧盟委员会进行充分保护水平评估时的考量因素[③]包括相关国家是否尊重法治与保护人权,相关立法是否涉及公共安全、国防和国家安全等。目前,包含新西兰、澳大利亚、韩国在内的13个国家获得了充分性保护水平认定[④]。此外,欧盟委员会的充分保护水平认定也可针对部分或特定部门作出,如金融服务或者IT部门等。目前,加拿大的商业组织获得了充分性保护水平认定[⑤]。

然而,我国并不在上述白名单之中,因此北京奥组委无法通过充分性保护认定这一路径来收集境外欧盟公民的个人数据。加之欧盟委员会自由裁量权过大且充分性保护认定呈"动态化",尤其是认定标准往往与政治因素关联甚密[3],故欧盟委员会很难在评判第三国或者国际组织保持中立及客观,通过充

① 《95指令》(Directive 95/46/EC)构建了欧盟数据跨境传输整体框架,且一直延续至今。《95指令》第25条第1款设立了个人数据跨境传输的"充分保护水平"(adequacy level of protection)一般性原则,禁止将个人数据传输到第三国(欧洲经济区以外的国家或地区),除非该第三国为处理个人数据的数据主体的权利和自由提供了充分的保护。若第三国采取了适当的保障措施(Appropriate Safeguards),也可进行个人数据跨境传输。除此之外,还可能适用特定例外情形。2015年10月6号,欧盟法院针对Schrems案(C-362/14)作出判决,将充分性保护决定考量的"充分保护水平"(adequacy level of protection)确切为"实质性等同"(essentially equivalent)水平。2016年4月14日,欧盟议会通过GDPR,延续了《95指令》中关于数据跨境传输的相关规定。

② GDPR第44条规定,个人数据转移不仅包括从欧盟境内向境外转移个人数据的情形,还包括个人数据从第三国或者国际组织转移至另外的第三国或者国际组织。

③ 依据GDPR第45条,委员会在评估时必须考虑:特定的第三国或国际组织是否尊重法治,保护人权及基本自由,以及相关立法是否涉及公共安全、国防和国家安全以及公共秩序与刑法;第三国或者国际组织是否确保对个人权利的行政和司法补救以及具备有效运行的独立监管机构;除所作的国际承诺外,第三国或者国际组织是否参与诸如"108号公约"的多边或区域协定,而担负个人数据保护相关义务。

④ 迄今为止,欧盟委员会已经认定安道尔、阿根廷、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、韩国、瑞士、英国和乌拉圭为充分性保护国家(欧盟委员会充分性保护决定)。

⑤ 其中涉及加拿大的决定是"部分"充分的,仅适用于加拿大《个人信息保护和电子文件法》(Personal Information Protection and Electronic Documents Act,PIPEDA)所覆盖的企业。

分性保护认定这一路径收集境外欧盟公民的个人数据，在短期内难以实现。此外，即便获得充分性保护水平认定，也并非一劳永逸，依据GDPR第46条第3款的规定①，欧盟委员会作出的充分性保护认定决定之后，仍将依据至少每四年一次的定期审核机制继续监督充分性保护实践。如有必要，欧盟委员会可以选择废除、修订、暂停相关的充分性保护决定。欧盟在充分性认定上拥有过大的自由裁量权，加之以常态化的监管机制，即便是符合充分性认定要件的第三国或国际组织，仍不得不承受不菲的合规成本。

2. 提供适当的保护措施

依据GDPR第46条，在缺乏充分性保护认定时，数据控制者或数据处理者仍可通过采取适当的保护措施跨境传输个人数据②。其中，基于合同义务的标准合同条款、基于行为标准的约束性企业规则为非充分性保护水平国家或国际组织跨境传输欧盟个人数据的主要途径。行业适用的行为准则虽暂未实施，基于其鲜明的行业特色，值得关注。

第一，基于合同义务的标准合同条款。欧盟委员会提供覆盖欧盟个人数据保护规定的《标准合同条款》（Standard Contractual Clauses，简称SCCs），认可签订该标准合同条款能够确保个人数据得到充分保护。旧版SCCs依据《95指令》第26条第4款而设定，包含数据控制者之间及数据控制者与数据处理者之间③的两种类型。为涵盖GDPR对个人数据保护的新要求，适用数字经济的发展，欧盟委员在2021年6月4日通过新版本的SCCs，旧版本SCCs留有18个月适用宽限期④。新版本SCCs包含C2C、C2P、P2P、P2C四种类型（前者位于欧盟经济区内）。不同类型的SCCs在保密性、数据处理安全性、第三方限制性转移方面类似，在数据处理权限以及处理后数据的删除或者返还等方面存在差别。无疑，SCCs是确保个人数据合法、安全跨境传输的适当保护措施的实用途径。随着欧美之间“隐私盾”失效，新版本的SCCs将愈发成为个人数据跨境传输的重要路径。

当前，欧盟要求在签订SCCs的基础上，还应提供补充措施。SCCs作为数据跨境流动方式的有效性，在2020年7月的Schrems II案（C-311/18）中得到欧盟法院确认。但欧盟法院提出，第46条第2款中转移工具为合同性质，当事人之间的承诺不能约束第三国当局，签订SCCs之外还需要采取额外的补充措施[4]。同年11月，欧盟数据保护委员会（European Data Protection Board，简称EDPB）发布《关于数据跨境传输工具的补充措施建议以确保个人数据保护遵循欧盟水平01/2020》，附件2部分列明了补充措施的非详尽清单，涉及签定补充合同、采取技术措施，完善组织措施等。可见，对于举办国际体育赛事所面临的欧盟个人数据收集障碍，可通过由举办方签署SCCs的方式化解。北京冬奥组签订SCCs之后，基于合同法上的义务充分保护欧盟公民的个人数据。但根据Schrems II案，仅签订SCCs是不够的，举办方还应该签订补充合同、采用技术措施等。

第二，基于行为标准的约束性企业规则。对于在欧盟境内有关联公司的企业集团或者从事联合经济活动的企业团体⑤，可通过实施约束性企业规则（Binding Corporate Rules，简称BCRs）将个人数据从欧

① GDPR文本包含99个条文以及173个独奏会（Recitals）条款，独奏会条款本身并不具有严格的法律约束力，但对于GDPR的理解与适用至关重要。第107条独奏会阐述了充分性决定可适当修改、撤销和暂停。依据第106条独奏会，欧盟委员会应监测和定期审查充分性决定国家或组织的数据保护水平。

② GDPR第46条第2款、第3款规定了的八种适当保护措施类型：欧盟委员会采用的“标准合同条款”（Standard Contractual Clauses，以下简称SCCs），相关监管机构批准的“约束性企业规则”（Binding Corporate Rules，以下简称BCRs），经欧盟数据保护委员会认定或者经欧盟委员会确认效力的“行为准则”（Code of Conduct），监管机构单独授权的“合同条款”（ad hoc Contractual Clauses），认证机制（certification mechanisms）等。当前，多数适当保护措施方案仍未有效实施。

③ 欧盟委员会通过2001/497/EC决定首次引入数据控制者之间的SCCs，随后在2004年12月27日通过2004/915/EC决定进行细节性的修订。欧盟委员会通过2010/87/EU决定，增加数据控制者与数据处理者之间的SCCs类型。

④ 欧盟委员会于2021年6月4日在最终实施决定中公布新SCCs。新SCCs将废除和取代现有的SCCs，并规定了从生效日期起的18个月过渡期。新旧版本交替期间，旧版本SCCs有效期间最多持续到2022年12月27日。

⑤ 依据第106条独奏会，参与共同经济活动的企业应涵盖一个控制性企业及其受控企业，其中控制性企业应是能够对其他企业施加支配性影响的企业，例如所有权、财务参与或管理它的规则或实施个人数据保护规则的权力。控制性企业及其受控企业一起视为一个企业集团。

盟境内跨境传输至境外的同一企业集团或团体。BCRs最早源于《95指令》中关于数据跨境传输中的“行为准则”标准。依据GDPR第47条,BCRs具有法律约束力,包括个人数据的一般保护原则及权利,在企业集团或团体成员中强制执行,以确保为数据传输提供适当的保护。BCRs由企业集团或团体向数据保护监管机构提交,监管机构在听取欧洲数据保护委员会的相关意见之后,决定是否予以批准①。若企业集团或团体在欧盟境内多个国家营业,其BCRs需要通过多个监管机构的审核。目前,多家知名跨国公司已获得BCRs认可[5]。

我国也可利用BCRs收集国际体育赛事所需欧盟个人数据,但操作空间有限。一是BCRs途径合规成本较高。BCRs在内容上必须包括所有一般数据保护原则和可执行权利,其批准流程相当烦琐,必须先后通过相关监管机构与欧洲数据保护委员会审核。尤其企业集团或者企业团体在欧盟境内多个国家拥有企业时,BCRs的审核还涉及多个监管机构。二是BCRs不能完全解决数据跨境传输的阻碍。因为BCRs严格限制在企业集团内部使用,而国际体育赛事涉及项目广、参与人数众多且通常伴随市场化运作,这意味着无法利用BCRs向供应商、客户、分销商或服务提供商等非内部组织进行数据传输。

第三,基于行业普遍适用的行为准则。具有普遍约束力的行为准则在欧盟境内发生效力,贯彻行为准则的相关企业或者组织享受数据跨境转移的白名单待遇。行为准则最早源于《95指令》第27条的规定,GDPR后续在起草主体、审查批准机构、监督等方面进一步细化。依据GDPR第40条,行为准则由行业协会或他机构起草,经由相关数据监管机构审查批准、欧洲数据保护委员会出具相关意见、欧盟委员会颁布实施性法令等措施,而后具有普遍约束力②。行业准则反映了特定部门或行业的特定数据流的特定特征和需求,是欧盟鼓励行业数据自治的重要举措。

体育领域的行业协会或者相关机构可以考虑针对举办国际体育赛事事宜达成具有普遍约束力的行为准则。但这一途径带有一定的理想主义色彩③。一是欧盟关乎行为准则的实践并不成熟,当前并未确立具有普遍约束力的行为准则。二是体育行业行为准则从起草到最终到欧盟委员会颁布实施性法令,涉及多方主体且程序复杂,使其具有普遍约束力难度大。

3. 适用可行的例外规定

GDPR明确特殊情形下可克减个人数据保护义务,即基于特殊情形下的例外规定(Derogations for Specific Situations)向域外传输个人数据。依据第49条④,例外规定具体包含先合同义务、明确同意、公共利益必要等八种特殊情形。其中,举办国际体育赛事往往涉及公共利益情形。

欧盟鼓励跨境传输保护公共利益所需且必要的个人数据⑤。如在竞争监管机构、税务或海关管理部门、金融监管机构、主管社会保障部门之间,在负责社会安全保障事务或公共健康的服务之间进行国际数据交换。其限制性条件为,上述公共利益为欧盟或数据接收国法律所认可。我国举办2022年冬奥会涉及的体育赛事兴奋剂检测、新冠肺炎疫情等传染性疾病接触者追踪等事宜属于公共利益的范畴。因

① 相关主管监管部门在初步审核之后将决定草案转达给欧盟数据保护委员会,后者将就经过初步审核的BCRs发表意见。最后,相关监管机构依据上述意见最终确定BCRs,再予以批准。依据GDPR第45条第1款到第3款,为了使对企业集团或者企业团体具有法律约束力,BCRs必须:指出数据传输的目的和有关的数据类别,考虑GDPR规定的要求,确认由欧盟主导的数据出口商代表整个集团承担责任,解释投诉程序,提供确保合规性的机制(例如审查)。BCRs依据主体的不同,分为数据控制者BCRs与数据处理者BCRs两种不同类型。

② 具体而言,若符合GDPR的个人数据保护相关规定,行业协会或其他机构起草的文件将经由监管机构批准,变成正式的草案文件。随即,欧洲数据保护委员会将针对行为准则草案是否提供适当的安全保障措施出具意见。对于符合适当的安全保障措施标准的草案,欧洲数据保护委员会有将肯定性意见提交给欧盟委员会的义务。欧盟委员会在收到上述肯定性意见之后,可以通过实施性法令的方式,使该准则具有普遍约束力。

③ 欧洲数据保护委员(European Data Protection Board)已经针对两份草案文件出具了部分肯定的意见,一是关于比利时监管机构提交的“欧盟云服务提供商数据保护行为准则”(EU Data Protection Code of Conduct for Cloud Service Providers),另为法国监管机构提交的“云基础设施服务提供商行为准则”(The Code of Conduct of CISPE)。

④ GDPR第49条规定适用例外规定的七种情形:明确同意转移;基于先合同义务所必须;数据主体利益合同所必要;行使、确立或抗辩法定请求权所必要;特殊情形无法同意但主体及他人利益所必要;依欧盟法规设立的登记簿为提供信息所必须;基于合法利益的限制性传输等。当前,多数适当保护措施方案仍未有效实施。

⑤ 依据第112条独奏会,反兴奋剂运动以及疫情防控等属于出于公共利益的重要原因而进行的数据传输的情形。

而针对上述事宜，存在适用“公共利益”例外规定而收集欧盟个人数据的操作空间。

（二）欧盟个人数据跨境传输规则适用的问题

通过考察欧盟个人数据跨境传输分层级适用的三条路径可以发现，其严密的数据跨境传输机制下数据跨境流动十分受限。可见，欧盟虽未明确数据本地化存储的一般性原则，但却形成了事实上的“软数据本地化存储”规则[6](P25-49)。如图1所示，作为国际体育赛事承办者收集境外欧盟参赛者个人数据的可行路径有：一是获得充分性保护水平认定；二是通过BCRs及SCCs及行为准则提供适当保护措施；三是适用公共利益例外规定。然而，我国举办冬奥会等国际体育赛事，在欧盟“软数据本地化存储”的规则体系下，以上三条路径都还存在问题和挑战。

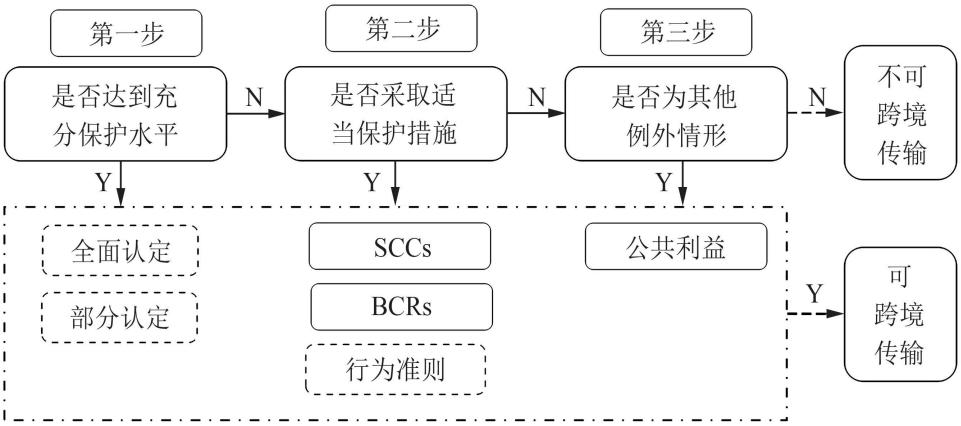

图1 国际体育赛事承办者收集欧盟居民个人数据的路径选择

第一，我国尚未属于欧盟委员会认定的白名单国家。当前存在欧盟委员会自由裁量权过大的问题，且对充分保护水平的认定是动态的，其并非一劳永逸，如欧美之间《隐私盾协议》现已无效。

第二，“提供适当保护措施”途径可操作性不强，合规成本高。SCCs作为一类合同仅用于规范合同约定的数据处理活动，这意味着个人数据处理活动类型发生变化时都必须起草新合同。当个人数据处理活动较为复杂时，存在数据接收方同时为数据控制者或数据处理者的情形，此时须多次签订多份不同类型的SCCs。此外Schrems II案判决提出了在SCCs基础之上提供补充措施的要求。BCRs严格限制在企业集团或团体内部使用，这意味着无法利用BCRs实现向非内部组织进行数据传输。此外，BCRs内容要求高，批准流程烦琐，其须经多个监管机构批准，而带有行业特色的行为准则尚未实践。

第三，“公共利益”例外情形的适用空间小，仅限于小规模数据流动。为开展体育赛事中的反兴奋剂工作，相关数据控制者可基于“公共利益”例外规定收集特定欧盟公民的个人数据，但其所涉及的个人数据范围也仅限定在为实现兴奋剂监管所需的、所必要的个人数据。此外，开展反兴奋剂活动所需的个人数据在奥运赛事相关数据中的占比不高。自然，基于公共利益例外规定进行的个人数据跨境传输必然规模受限，且很难多次或经常性适用。

三、我国数据出境规则及其适用的问题

根据《主办城市合同》，国际奥委会要求冬奥会结束之后北京奥组委须将所有相关数据转移至瑞士的国际奥委会总部。北京奥组委作为此次国际体育赛事数据出境合规的义务主体，需要依据我国数据出境相关规则，向位于瑞士的国际奥委会进行数据转移。

(一)我国数据出境相关规则

数据出境[①]指将在我国境内收集和产生的数据一次或多次提供给境外接受方,或允许境外相关的机构访问或调用。我国并未形成关乎数据出境的统一立法,对其之限制与监管规定散见于各类法律法规、部门规章以及规范性文件当中。依据《网络安全法》《数据安全法》《个人信息保护法》等,我国数据出境整体上以数据本地化存储为原则,以限制出境为例外。其目的在于降低跨境流通对我国国家安全、社会公共利益及个人合法利益带来的风险。当前,我国数据出境的可行途径包括通过数据出境安全风险评估、与境外接收方订立合同以及获取个人信息保护认证。

1. 通过国家网信部门的安全评估

《网络安全法》第37条确立了我国个人信息和重要数据本地化存储的一般性原则,同时明确"安全评估"为本地化存储之例外。自2022年9月1日实施的《数据出境安全评估办法》(以下简称《办法》)搭建起我国数据出境安全评估的基本框架。《办法》历经三次征求意见[②]后发布,针对数据出境安全评估的适用范围、评估形式、评估流程以及常态化监管等进行了完善的规定。一是适用范围。依据《办法》第2条的规定,进行安全评估的主体为数据处理者,其须存在向境外提供数据的情形,提供的数据须在我国境内运营中收集与产生,且这些数据为重要数据与个人信息。二是评估形式。依据《办法》第3条、第5条规定,数据出境安全评估采用自评估与安全评估相结合的方式。在适用层级上,数据处理者应先行开展自评估,自评估属于《办法》第4条[③]规定的四种情形而后进行申报安全评估。三是评估流程。数据处理者应当经自评,自认为符合条件的前提下向省级网信部门提交安全评估申报材料。省级网信部门审核材料完备性,然后上报国家网信部门进行安全评估。国家网信部门根据申报的情况,联合省级网信部门或专门机构进行评估,作出通过评估与否的决定。四是常态化监管。依据《办法》第3条、第14条,安全评估的监管是常态化的,且通过数据出境安全评估的结果有效期为2年。可见,我国数据出境安全评估已基本形成以国家网信部门为主导、自评估与申报风险评估相结合、事前评估与监督相结合的基本框架。

北京冬奥组委可通过国家网信部门的安全评估后向境外转移数据。我国北京冬奥组委担负有将奥运赛事相关数据转移至国际奥委会的义务,北京冬奥组委作为数据处理者,须向位于瑞士的国际奥委会提供数据,所提供数据为冬奥会赛事活动所收集或产生。具体的数据类型必然包含个人信息以及如北京冬奥会网络及终端设备的配置数据等可能涉及国家安全的重要数据。由此,北京冬奥组委作为数据处理者应当进行数据出境安全评估。依据《办法》,若北京冬奥组委提交的数据转移事项通过国家网信部门组织的安全评估,即可向国际奥委会转移相关数据。

2. 获取专业机构的个人信息保护认证

依据《个人信息保护法》第38条第2款,个人信息处理者获取专业机构的个人信息保护认证后即可向境外提供个人信息。2022年6月24日,国家信息安全标准化技术委员会发布《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》(以下简称《认证规范》)。《认证规范》明确个人信息保护认证将从个人信息跨境处理应遵循的基本原则、要求以及个人信息主体权益保障方面展开。然而,其并未明

---

① 国家互联网信息办公室最新发布的《数据出境安全评估办法》中并未明确数据出境的定义,但就《办法》答记者问时明确了数据出境包括:数据处理者将在境内运营中收集和产生的数据传输、存储至境外;数据处理者收集和产生的数据存储在境内,境外的机构、组织或者个人可以访问或者调用。我国关于数据向境外转移的跨境传输、数据出境、跨境提供等不同说法,但都表达相同的含义,其中数据出境使用较为主流,本文中数据出境及数据跨境传输等做同等含义使用。

② 2017年4月11日,国家互联网信息办公室发布《个人信息和重要数据出境安全评估办法(征求意见稿)》,涉及个人信息与重要数据的出境安全评估。2019年6月13日,国家互联网信息办公室发布《个人信息出境安全评估办法(征求意见稿)》,仅涉及个人信息的出境安全评估。随后,2021年10月29日,国家互联网信息办公室发布《数据出境安全评估办法(征求意见稿)》将个人信息与重要数据统一规范。

③ 《数据出境安全评估办法》第4条规定,数据处理者向境外提供数据,有下列情形之一的,应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估:数据处理者向境外提供重要数据;关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息;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;国家网信部门规定的其他需要申报数据出境安全评估的情形。

确开展个人信息保护认证的专门机构。

北京冬奥组委向国际奥组委提供冬奥会相关数据时，涉及个人信息跨境转移。北京冬奥组委可作为个人信息处理者，通过获取专业机构保护认证的途径，向国际奥组委转移冬奥会数据中的个人信息。

3. 依标准合同与境外接收方订立合同

依据《个人信息保护法》第38条第3款，个人信息处理者可依照国家网信部门制度的标准合同与境外接收方签订合同的方式向境外提供个人信息。订立标准合同这一途径合规成本低且可操作性强。按照国家网信部门制定的标准合同与境外接收方订立合同是一种私法主体间的民事行为，操作简便可行。此外，依据标准合同约定与接收方的权利和义务的合规成本低。标准合同由国家网信部门制定，合同内容具备个人信息保护的当然性。2022年6月30日，国家互联网信息办公室发布《个人信息出境标准合同规定（征求意见稿）》（以下简称《标准合同规定》），《标准合同规定》涉及适用范围、合规义务及法律责任等方面，其并非强制性适用，个人信息处理者可以自行拟定不相冲突的合同。

北京冬奥组委可以选择同国际奥组委依据标准合同签订个人信息跨境流动的合同，同国际奥组委约定个人信息保护的权利与义务，如此便可合法合规地向国际奥组委提供冬奥会相关的个人信息。

（二）中国数据出境规则适用的问题

考察我国限制性数据出境规则后不难发现，北京奥组委作为数据处理者，可选择通过安全评估、获取保护认证或订立标准合同的方式向境外的国际奥委会转移数据（见图2），但将冬奥会产生的相关数据向境外提供仍将面临合规挑战。

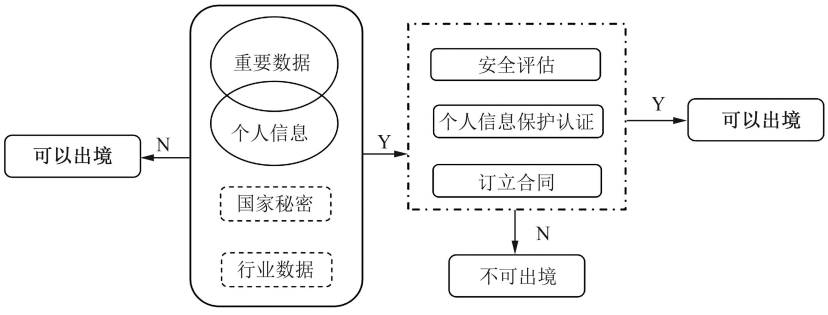

图2　向境外转移国际体育赛事相关数据的可选路径

第一，国际体育赛事举办方面临数据切割难题。我国数据出境监管指向个人信息与重要数据，在《网络安全法》实施前后，受到跨境规制的数据类型还涉及银行金融、医疗健康、自动驾驶、商业服务等多个行业领域的数据，对于国家秘密更是严格限制出境。由此，不属于上述数据范畴的数据可不经监管直接转移。冬奥会相关数据丰富多样，涉及注册、票务、住宿、餐饮、语言、医疗、交通等多领域，其中包含了个人信息，也可能包含重要数据，甚至是人口健康信息等行业领域数据或是国家秘密。目前，个人信息的内涵界定业已形成“识别加关联”的通识，《信息安全技术 个人信息安全规范》附录A部分也列明个人信息的具体类型，提供了相应的判别指引。然而，我国当前并未明晰重要数据的具体范围。2022年1月13日发布的《信息安全技术 重要数据的识别指南》（征求意见稿）表明我国对于重要数据的具体范围仍停留在探索阶段。

由此将导致如下问题：一是无法将不属于个人信息、重要数据、国家秘密以及受监管的行业领域数据切割出来，而这部分数据理应可自由流动。二是无法明确国家秘密以及受监管的行业领域数据与重要数据的关系，这是因为国家秘密以及行业领域数据是否必然属于重要数据的范畴仍不明确。三是个人信息与重要数据存在重叠，个人信息可能属于与国家安全、社会公益密切相关的重要数据，重要数据中包含非个人信息，将二者进行切割的必要性及可行性存疑。

第二,相关配套规则未出台,导致数据出境合规路径尚未畅通。《办法》的适用范围并不清晰,其并未明确安全评估四个要件中的“数据出境”以及“数据处理者”的定义,且我国仍未明确“重要数据”识别标准,这意味着当前进行安全评估尚存规则适用难题。此外,《认证规范》并未明确开展个人信息保护认证的专门机构,《标准合同规定》尚未实施,缺乏相应的实践经验。

四、国际体育赛事数据跨境传输规则适用难题的破解路径

通过考察欧盟个人数据跨境传输路径及我国数据出境限制规则可发现,国际体育赛事数据跨境传输的规则冲突体现在欧盟“软数据本地化”的立场与我国“硬数据本地化”主张相冲突,由此产生的数据跨境流动的矛盾难以有根本的解决方案。结合举办国际体育赛事的特点,本文认为可以考虑的解决路径如表1所示。从我国被动应对的角度,国际体育赛事举办方可在体育赛事相关协议中设置合规性保护义务条款以直接应对,也可适用欧盟SCCs及BCRs跨境传输工具以间接合规。从我国能动应对的角度,我国可以致力于推动建立双边或者多边合作机制,也可以由国家体育总局制定我国体育领域的专门性数据保护规范。

表1　数据跨境传输规则适用难题的解决路径

解决方式	具体路径	优势	挑战
被动	协议中设置合规性保护义务条款	直接、简便	数据治理话语丧失
	适用SCCs及BCRs跨境传输工具	工具较为成熟	合规成本高
能动	推动建立双边或者多边合作机制	多元主体协调治理	谈判挑战
	制定我国体育产业数据保护规范	长效机制	制度成本

(一)在举办协议中设置合规性保护义务条款

就举办北京冬奥会而言,其数据跨境传输的合规义务主要来源于《主办城市合同》中的规定。GDPR生效之后,国际奥委会相继更新了随后将举办大型体育赛事的巴黎、洛杉矶等城市的《主办城市合同》版本,这是国际奥委会作为数据控制者将高标准的欧盟个人数据保护义务内化吸收的结果。未来的国际体育赛事主办方可在国际体育赛事举办协议中设置合规性保护义务条款,以确保外国公民的个人数据权益不受减损。若直接承认GDPR的规则体系,可通过明确如下义务条款保护个人数据:遵循目的限制原则、透明度原则、准确性与数据最小化原则等一般性原则,限期储存个人数据;采取技术措施保保障数据处理安全,限制性向第三方转移,限制对特殊类型个人数据的处理,等等。

在举办协议中设置合规性保护义务条款属于一事一议的方式,这种方式虽较为灵活直接,但在双方长臂管辖原则呈对抗的情形下,一味追求义务合规可能丧失数据治理话语权。北京冬奥组委若悉数将奥运赛事相关数据转移,全然忽略数据本地化存储的一般性原则,实际上不适用本国法律,而适用欧盟的相关法律,这是一种主权的让渡。

(二)适用SCCs及BCRs跨境传输路径

结合欧盟GDPR的相关规则来看,目前可行的数据传输路径有BCRs以及SCCs。两种途径都是对欧盟规则事实上的承认,也仅解决如何对将个人数据的跨境传输到我国境内的问题。

BCRs针对大中型的企业设立,鼓励在欧盟存在经济实体的企业集团或者企业实体使用。理论上,国际体育赛事举办方可与通过BCRs的跨国公司合作,跨境传输国际体育赛事所涉及的欧盟居民个人数据。基于BCRs严格限制在企业集团内部使用,与上述跨国公司合作只能确保将欧盟公民的个人数据从欧盟转移到境外的跨国公司。如果为实现奥运赛事相关活动目的,处于境外的跨国公司实体还需要向其他供应链、酒店或者交通部门等数据控制者或处理者共享数据,该跨国公司需另外同这些主体签订新的SCCs以约束上述共享行为。此外,目前通过BCRs认证的跨国公司仅80余家,从中找到能够提供与

国际体育赛事举办相关跨国服务的合作伙伴较为困难。

此外，国际体育赛事主办方可与欧盟境内的数据处理者或者数据控制者签订SCCs，通过合同条款保障欧盟公民的数据权利。国际体育赛事主办方为数据控制者，为完成赛事相关事宜决定数据的处理目的与方式。其可能签订的标准合同条款（SCCs）有数据控制者至数据控制者（Transfer Controller to Controller，C2C）或者数据处理者至数据控制者（Transfer Processor to Controller ，P2C）两种类型。签订C2C之后，主办方受目的限制原则约束，在为完成奥运会相关事宜范围内进行数据处理活动。举办方可以在权限范围内授权其他数据处理者处理个人数据，但需要保证数据主体的权利。举办方也可以与在欧盟境内的数据处理者签订P2C，要求境内的数据处理者按照举办方的指示进行数据处理活动。SCCs相较于BCRs更为实用，国际体育赛事的举办方可能依据不同的数据处理目的需要签订多份SCCs，由此面临不菲的数据合规成本。

（三）推动建立双边或者多边合作机制

数据跨境传输的规则冲突给全球的行政法体制提出了新难题，有必要进行国际协调，构建双边或者多边的国际协作机制和多元主体协同治理的格局。面对欧盟采取的单边保护主义，我国可以与欧盟委员会进行磋商，就个人信息与重要数据跨境传输探讨双边合作机制。GDPR第50条、我国《数据安全法》第11条及《个人信息保护法》第12条都给未来中国与欧盟的国际合作预留了一定的空间。欧盟委员会以及监管机构有建立国际合作机制以促进GDPR有效实施的义务；我国应积极开展数据领域国际交流与合作，参与数据安全相关国际规则和标准的制定，以促进个人信息保护及数据跨境安全、自由流动。双边协议的达成受协议参与国自身经济、政治力量的制约[7]（P37-48）。面对欧盟强硬的单边主义，我国绝不应作出全面承认GDPR规则的承诺，而应该坚持双方充分磋商之后达成数据跨境传输制度的共识。

即便达成双边合作，也只是解决我国与欧盟之间的数据跨境传输冲突问题。要真正形成多元主体协同治理的局面，在于形成一个刚性的多边条约。如此便可以约束世界范围内的主要国家与地区，确保数据在共识框架基础上的自由流动。但不可避免地，基于不同的文化背景、法律环境及政策考量，其较之双边条约谈判成本更高，难度更大。当下数据跨境传输的迫切现实需求，亟待联合国、WTO等国际组织积极推动构建数据跨境传输的多边条约。

（四）制定我国体育产业数据保护规范

目前我国有制定体育产业数据保护规范的需求。我国在《体育强国纲要》中明确了“体育产业更大、更活、更优，成为国民经济支柱性产业”的战略目标。大型国际体育赛事涉及注册、餐饮、抵离、酒店、医疗、语言、交通、技术等多个方面，其中必然收集与产生大量的个人信息与重要数据。国际体育塞所收集或产生的数据蕴含着巨大的开发与分析价值，是促进体育产业发展的“新石油”。然而，促进体育数据开发利用和产业发展，打造现代产业体系，有着对体育数据更高标准的数据保护需求。国家体育总局有必要出台高于一般保护水平的体育领域数据保护规范，以畅通国际体育赛事数据自由跨境传输渠道，同时为赛事中的个人信息与重要数据提供充分性保护。如此便可在保护体育产业数据安全的前提下，推动以数据为关键要素的人工智能、物联网等技术与体育产业的融合，为创新体育领域的生产方式、服务方式和商业模式提供制度保障。此外，制定体育产业数据保护规范是基于产业格局与国际地位的重要考量[8]（P106-117）。我国体育产业有着自身的比较优势，积极主动地构建体育产业数据保护规范，可构建体育产业数据保护的中国话语。

五、结 语

欧盟严格限制个人数据跨境传输，中国明确数据本地化存储原则，构成数据跨境传输的规则适用难题。规则适用问题的本质在于主权国家以个人数据为抓手展开长臂管辖制度暗战，争夺数据治理规则话语权。当前解决规则适用难题的可选路径中，在协议中设置合规性保护义务条款、适用BCRs及SCCs

跨境传输工具都是一次一议的临时性选择;推动建立双边或者多边合作机制,统筹推动制定我国体育产业数据保护规范是长期、可制度化的解决方案。尤其在我国实施大数据战略、体育强国战略的背景下,制定我国体育产业数据保护规范更是基于产业发展与国际地位的重要选择,有助于构建体育产业数据保护的中国话语,提升我国体育产业在世界范围内的影响力,这也是我国目前解决国际体育赛事数据跨境传输合规问题的优选方案。

参考文献

[1] 廖诗评. 国内法域外适用及其应对——以美国法域外适用措施为例. 环球法律评论,2019,(3).

[2] 唐晓彤. 大型国际体育赛事对社会发展的波及效应. 广州体育学院学报,2007,(1).

[3] European Commission. Exchanging and Protecting Personal Data in a Globalized World. EUR-Lex, 2017-10-01. [2022-09-09] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A201 7%3A7%3AFIN.*

[4] Court of Justice of the European Union. Judgment of the Court (Grand Chamber). InfoCuria, 2020-07-16. [2022-09-09] *https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&p ageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11388612.*

[5] European Data Protection Board. Pre-GDPR BCRs Overview List, EDPB, 2021-01-14. [2022-09-09] *https://edpb.europa.eu/system/files/2021-03/edpb_information_20210126_pre-gdpr_bcrs_over view.pdf.*

[6] 李艳华. 隐私盾案后欧美数据的跨境流动监管及中国对策——软数据本地化机制的走向与标准合同条款路径的革新. 欧洲研究,2021,(6).

[7] 张继红. 个人数据跨境传输限制及其解决方案. 东方法学,2018,(6).

[8] 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. 法学评论,2020,(1).

Research on the Application of Rules for Cross-border Data Transmission of International Sports Events

Taking the Beijing 2022 Winter Olympics as an Example

Xiao Dongmei, *Su Ying* (Xiangtan University)

Abstract　Since the data governance rules of different countries (regions) are inconsistent, the organizers of international sports events face difficulties in the application of data cross-border transmission rules. The first is to set up compliance protection obligations in the international event holding agreement to directly deal with it; the second is to apply Standard Contractual Clauses and Binding Corporate Rules tools; the third is to promote the establishment of bilateral or multilateral cooperation mechanisms; the fourth is to promote the formulation of data protection norms for China's sports industry. The first three paths have their limitations, and the fourth path is currently the preferred solution to solve the compliance problem of cross-border data transmission in hosting international sports events.

Key words　international sports events; personal information protection; data sovereignty; cross-border data transmission

■ **收稿日期** 2022-09-02

■ **作者简介** 肖冬梅,管理学博士,湘潭大学知识产权学院教授、博士生导师;湖南 湘潭 411105;
苏　莹,湘潭大学知识产权学院博士研究生。

■ **责任编辑**　桂　莉