

《电子商务协议》文本下我国数据跨境流动规则的检视与完善^{*}

何云富, 赵庆超

(西南民族大学 法学院, 四川 成都 610041)

摘要: WTO 电子商务谈判的目标是在现有的协定与框架基础上, 建立高标准的国际电子商务规则。2024 年 7 月 6 日, 电子商务谈判达到了新的里程碑, 达成了一个稳定的《电子商务协议》文本。《电子商务协议》文本中的数据跨境流动规则围绕着个人数据保护和例外条款构建, 以协同治理为理念, 流动性优化为准则, 限制流动为例外。我国的数据跨境流动规则平衡发展与安全的理念能够与《电子商务协议》文本的建构理念相契合; 我国数据存储本地化和数据出境制度能够满足《电子商务协议》文本个人数据保护条款和相关例外条款的规定, 数据跨境流动规则能够与《电子商务协议》文本相协调。但是, 需要对国家重要数据目录进行改进和完善。

关键词: 《电子商务协议》; 数据跨境流动; 个人数据保护

中图分类号: D922.294

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2025.08.007

引用格式: 何云富, 赵庆超.《电子商务协议》文本下我国数据跨境流动规则的检视与完善 [J]. 网络安全与数据治理, 2025, 44(8): 46-52.

Review and refinement of China's cross-border data flow rules under the E-Commerce Agreement framework

He Yunfu, Zhao Qingchao

(Law School, Southwest Minzu University, Chengdu 610041, China)

Abstract: The goal of the World Trade Organization (WTO) e-commerce negotiations is to establish high-standard international e-commerce rules on the basis of existing agreements and frameworks. On July 6, 2024, the e-commerce negotiations reached a new milestone, and a stable text of the "E-Commerce Agreement" was reached. The rules on cross-border data flow in the text of the "E-Commerce Agreement" are constructed around the protection of personal data and exception clauses, taking collaborative governance as the concept and liquidity optimization as the principle, with restricted data flow being the exception. The concept of balancing development and security in China's rules on cross-border data flow can be in line with the construction concept of the text of the "E-Commerce Agreement"; China's data storage localization and data outbound system can meet the provisions of the personal data protection clauses and relevant exception clauses in the text of the "E-Commerce Agreement", and the rules on cross-border data flow can be coordinated with the text of the "E-commerce Agreement". However, it is necessary to improve and perfect the catalog of important national data.

Key words: E-Commerce Agreement; cross-border data flows; personal data protection

0 引言

在全球化时代, 数据增长迅猛, 国际数据公司

(IDC) 预测, 到 2028 年全球数据量将增长至 393.8 ZB, 相比于 2018 年增长 9.8 倍。数据作为新的生产要素在流动中产生价值也必然具有外部性, 数据治理因此成为促进数字贸易健康发展的题中应有之义。然而, 全球数据治理问题突出, 难以达成共识, 这与全球经济依赖数据驱动的现状不相匹配, 致使难以完全发挥数据的生产要

^{*} 基金项目: 西南民族大学 2025 年研究生创新型科研项目; 四川省哲学社会科学重点研究基地社会治理创新研究中心青年项目 (SHZLQN2401)

素驱动作用。2019 年, 76 个世界贸易组织 (World Trade Organization, WTO) 成员正式启动与贸易相关的电子商务谈判, 目标是在现有的协定与框架基础上, 建立高标准的国际电子商务规则。但因成员众多, 利益不同, 谈判进展缓慢。在数据跨境流动、数据本地化、电子传输免关税、源代码披露和算法公开等问题上, 各国立场仍然存在显著分歧。截至 2024 年 7 月, 共有 91 个 WTO 成员参与了电子商务谈判, 并达成了一个稳定的《电子商务协议》文本 (以下简称《协议》文本)。数据跨境流动议题作为各方面关注的核心问题, 被认为是谈判面临最大挑战^[1]。本文基于 WTO 电子商务谈判取得的最新成果, 依据《协议》文本数据跨境流动相关规定, 对我国的数据跨境流动规则展开审视, 探寻限制数据跨境流动举措在《协议》文本框架下的合法依据, 进而推动相关规则的完善。

1 《协议》文本数据跨境流动框架与我国规则

1.1 《协议》文本数据跨境流动框架

1.1.1 协同治理理念

《协议》文本框架下, 数据跨境流动规则的协同治理呈现出多方主体参与、利益关系协调、制度协同并行的显著特征。

首先, 多方主体参与表现为《协议》文本由全球性的经济、多边贸易规则管理组织, 即 WTO 的 76 个成员共同发起, 历时五年, 最终由 91 个 WTO 成员 (涵盖全球贸易的 90% 以上, 包括 38 个发达成员、47 个发展中成员和 6 个最不发达成员) 参与电子商务谈判并达成的里程碑式成果^[2]。其成功构建起多元主体广泛参与、深度协商、联合治理、共建共享的有效机制。

其次, 利益关系协调主要体现为《协议》文本数据跨境流动规则充分兼顾了以美欧、中国、缅甸等为代表的各发展阶段国家的利益。欧盟在个人隐私与数据安全方面保持高标准, 重视隐私保护^[3]。美国倡导跨境数据自由流动和低监管^[4]。而中国的数据跨境流动立场可以根据《全球数据安全倡议》《全球数据跨境流动合作倡议》《促进和规范数据跨境流动规定》等相关法律法规、国际倡议总结为: 秉持开放、包容、安全、合作、非歧视的原则, 注重主权与差异、平衡发展与安全, 反对泛化安全, 鼓励跨境传输, 构建合作框架, 弥合数字鸿沟。《协议》文本中, 各国的利益诉求均予以体现。在《协议》文本前言中, 便提到了“各缔约方权利”“开放、透明、非歧视、可预测”“安全”“数字鸿沟”“援助”“代表性不足群体”“中小企业”等主题, 对透明度、合作与发展问题进行了专节论述 (见《协议》文本

第 E 节)。充分体现了《协议》文本在重视并鼓励数据跨境流动的前提下, 强调保障个人数据安全、保护个人隐私, 尊重各国主权和法律实践的差异, 倡议国际合作, 平衡发展与安全, 弥合数字鸿沟。另外, 《协议》文本也为部分数字产业落后的缔约国设置了适用宽限期特别条款, 第 20.6 条规定, “每个发展中国家和最不发达国家缔约方可在本协定对其生效之日, 通过向委员会提交此类条款清单, 自行指定本协定中其需要不超过五年实施期限的任何条款。”宽限期旨在为产业落后的缔约方发展国内数字产业、完善数据跨境流动治理规则提供时间, 通过技术援助和能力建设帮助发展中国家和最不发达国家缔约方实施本协议的规定。

最后, 制度协同并行主要体现为《协议》文本充分尊重各国法律实践的差异, 允许不同模式的法律框架构建或维持以达到促进数据跨境流动和保障个人数据安全的平衡。《协议》文本第 16.3 条构建或维持法律框架条款的注释规定, “为更明确起见, 一缔约方可通过采取或维持相关措施, 或这些措施的组合遵守本款规定, 例如制定全面的隐私法、个人数据保护法、涵盖隐私内容的特定行业法, 或其他针对侵犯隐私行为的法律。”该注释旨在说明, 为确保缔约方切实履行保护电子商务用户个人数据的义务, 在法律实践上给予一定的灵活性。即缔约方在构建保护个人数据的法律框架时, 方式并非单一固定。既可以通过专门制定一部全面的隐私法, 从宏观层面规范各类隐私相关问题; 也能依靠个人数据保护法, 聚焦于个人数据这一核心范畴进行保护; 还可以针对不同行业的特性, 制定特定行业的隐私法规; 甚至可以将这些法律手段相结合, 再辅助其他针对侵犯隐私的法律, 以此满足《协定》文本对个人数据保护的要求, 确保电子商务用户的个人数据得到有效保护。

当然, 《协议》文本数据跨境流动规则的协同治理理念也意味着其对数据跨界流动的治理只能达成较为框架的内容。WTO 电子商务谈判协议受诸多因素影响, 这从《协议》文本达成所耗时间就可以看出。具体来看, 这既有前述立场分歧, 即各国在数字经济中的不同优先级考虑 (我国强调数据主权和安全, 美国倡导跨境数据自由流动低监管, 欧盟则更加重视隐私保护^[5]), 又有现实因素即各国不同的法律实践和全球经济发展的南北差异所致。正基于此, 《协议》文本多次提及缔约国之间的援助, 允许在《协议》文本框架内不同的法律制度并行。

1.1.2 流动性优化准则

在全球性的电子商务谈判尚未达成《协议》文本时, 地区性的数据跨境流动规则框架的主要内容多以电子商务专章的形式出现。如《全面与进步跨太平洋伙伴关系

协定》(CPTPP)数据跨境流动规则集中于第14章电子商务。《协议》文本作为WTO批准的第一套全面的电子商务规则,多个章节论述了“电子商务”,包括“促进电子商务”“开放与电子商务”“信任与电子商务”。《协议》文本数据跨境流动性优化准则主要体现为以电子方式便捷交易,免征关税降低成本,保障安全稳定交易。

其一,电子方式便捷交易。《协议》文本中涉及的电子交易框架、电子认证和电子签名、电子合同、电子发票、无纸化交易、电子支付等内容无一不是为数据跨境流动提供全球性的便捷。

其二,免征关税降低成本。电子传输是否征收关税作为前期谈判的核心议题分歧,在《协议》文本中作出了定论。各缔约方认识到不对电子传输征收关税的做法在数字经济中发挥着重要作用,因此《协议》文本第11.3条规定,“各缔约方不得对缔约方个人相互间的电子传输实施关税征收行为”。这一规定降低了跨境电子交易的成本,促进了数字产品和服务的跨境流动,便利了数据跨境流动,激发了数字经济活力。如在跨境电商交易中,商品信息、交易记录、消费者数据等实现跨境流动,免征电子传输关税降低了电商企业的运营成本,企业无须为数据传输支付额外关税,这使得企业能够投入更多资金用于技术研发、市场开拓和服务优化。

其三,保障安全稳定交易。其实,促进数据跨境流动和保障数据安全是一体两面的关系。正如同人们对自由和确定性的追寻,没有自由的确定性与奴役无异;而没有确定性的自由也与被抛弃和被丢失无异^[6]。只有保障数据安全,电子商务用户才能对数据跨境流动无后顾之忧,进而促进全球经贸发展。《协议》文本第16条是个人数据保护专条。《协议》文本规定须以法律框架保障个人数据安全,保证对自然人的个人数据给予非歧视性保护。缔约方为用户提供的个人数据保护信息应当包含自然人如何寻求救济,企业如何遵守法律要求。虽然各缔约国保护方式有别,但应推动保护机制兼容,以便数据跨境流动。一系列的个人信息保护要求即为重视数据这一新型生产要素的表现,而重视本身必然有着更深层次追求,最根本的目标就是促进缔约各国数字经济贸易的发展。而这必然得发挥数据跨境流动的积极作用,通过构建、完善个人数据保护规则,规范数据跨境传输,方能促进全球数字经济的健康发展。

1.1.3 限制流动例外

《协议》文本在倡导提供便利条件促进数据跨境流动的同时,也规定了例外条款对数据跨境流动进行了限制。《协议》文本第G节第22条至第26条共约定了5项例外,包括一般例外、安全例外、审慎措施例外、个人数

据保护例外等。一般例外条款的适用,需参照《1994年关税与贸易总协定》第20条及其阐释,以及《服务贸易总协定》第14条,通常涉及公共道德、人类和动植物生命健康、自然资源等方面。安全例外涵盖了国家安全相关的例外情形,允许缔约方在特定情形下为保护自身安全利益采取限制贸易的措施,但缔约方必须证明其目的真实且手段具有必要性。审慎措施例外则针对电子商务活动中的金融服务信息数据。个人数据保护例外平衡了数据保护与贸易便利化的关系。《协议》文本中关于数据跨境流动的例外条款,对推动缔约国间数据跨境流动的便利性起到补充作用,有助于保障缔约国的数据安全。

1.2 我国数据跨境流动规则

我国是WTO《协议》文本的主要缔约国,在电子商务谈判中提出了中国方案,显示了中国力量,贡献了中国智慧。我国的数据跨境流动规则以数据分类分级保护、平衡发展与安全为理念,在数字经济和贸易持续发展壮大的过程中,形成了以《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)、《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》)为核心,以《数据出境安全评估办法》《个人信息出境标准合同办法》《关于实施个人信息保护认证的公告》及其附件、《促进和规范数据跨境流动》《网络数据安全条例》等为补充的规则组合框架。

1.2.1 立法理念:平衡发展与安全

我国的数据跨境流动规则的构建理念经历了安全至上到平衡发展与安全的转变。2016年公布的《网络安全法》的立法目的强调保障网络安全,作为首部全面规范网络安全的基础性法律,《网络安全法》要求关键信息基础设施的运营者进行数据本地化存储和跨境安全评估。2021年公布实施的《个人信息保护法》对个人信息跨境流动设定了安全评估、保护认证、标准合同等义务。《数据安全法》虽然以数据安全为首要立法目的,但还包含促进数据开发利用,也即充分利用数据的价值。在数据跨境流动方面,不仅强调传统的“促进数据跨境安全”,而且开始强调数据“自由流动”。《数据安全法》以专章的形式规定了数据发展与安全,强调“国家统筹发展与安全”。

在我国,有不少学者强调我国的数据出境制度以安全至上理念构建^[7-10]。随着我国数字贸易的发展和立法技术的演进,我国的数据跨境流动规则理念已经由安全至上逐渐转变为平衡发展与安全^[11]。发展与安全是一对辩证关系。发展和安全的关系也是我国总体国家安全观的五对关系之一。“发展是安全的基础,安全是发展的条件”。党的二十届三中全会审议通过的《中共中央关于进

一步全面深化改革 推进中国式现代化的决定》将系统观念、处理好发展和安全等重大关系，作为进一步全面深化改革的原则。《网络安全法》要求相关主体进行“数据本地化存储和跨境安全评估”，正是为了保障数据安全。数据安全为数据跨境传输创造条件。《数据安全法》则强调“统筹发展与安全”“促进数据跨境安全、自由流动”。这正是我国数据跨境流动立法以平衡发展与安全为理念的体现。

1.2.2 出境制度：分类分级治理

数据分类分级保护治理最早见于《网络安全法》中对“重要数据”和“个人信息”的分类保护规定，这为后续数据分类分级制度发展奠定了基础。《数据安全法》中正式确立了“数据分类分级保护制度”。该法第21条规定，国家建立数据分类分级保护制度，对数据实行分类分级保护。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等不同的数据出境制度，正是我国数据跨境流动分类分级治理、保护的体现。

《关于实施个人信息保护认证公告》这一部门公告所附文件《个人信息保护认证实施规则》对个人信息处理者开展个人信息收集、传输、跨境等处理活动进行认证的基本原则和要求进行了规定。该规则规定了个人信息保护的认证依据，即个人信息处理应当符合《信息安全技术个人信息安全规范的要求》（GB/T 35273）的规定。对跨境个人信息流动，还应当符合《个人信息跨境处理活动安全认证规范》（TC260-PG-20222A），该规范为个人信息处理提供了操作指南，降低了合规成本，提高了个人信息跨境处理的效率，规范了数据跨境处理行为。《关于实施个人信息保护认证公告》及其附件衔接《个人信息保护法》，为个人信息跨境流动提供了另一种合规途径。

2024年公布实施的《促进和规范数据跨境流动规定》对安全评估、标准合同、保护认证等数据出境制度作出了最新的总结规定。该规定从正反两方面对数据跨境流动进行了规制。简言之，数据跨境流动是否受到严格的数据出境制度规范，其标准为跨境传输的数据中是否包含重要数据或者个人信息。申言之，跨境传输的数据没有重要数据或个人信息的，免于严格的数据出境制度规范。该规定同时明确数据出境制度的适用情形，对于关键信息基础设施运营者、非关键信息基础设施运营者提供重要数据，或者累计提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息的应当通过所在省级网信部门向国家进行出境安全评估；对于非关键信息基础设施运营者提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，应当适用出境标准合同或者通过保护

认证；对于以上分类之外的个人信息的跨境传输则履行告知、取得个人同意、进行个人信息保护影响评估义务；对于以上分类之外的数据，即一般数据的出境则履行数据安全保护义务和安全事件报告义务。另外，对于相关规定同本规定不一致的部分，《促进和规范数据跨境流动规定》明确适用本规定。

总之，我国数据跨境流动规则在数据分类分级保护、平衡发展与安全理念下，以跨境传输的数据中是否包含重要数据或者个人信息为标准，建立起松紧有度的数据出境制度。

2 《协议》下我国数据跨境流动规则的检视

我国作为《协议》文本缔约国，应当如《电子商务联合声明》倡议，推进国内程序，以期将谈判成果纳入世贸组织法律框架。我国应当以《协议》文本数据跨境流动框架为蓝本，对我国数据跨境流动规则开展审视。这涵盖对立法理念的探究，以及研判数据出境制度是否契合《协议》文本例外条款的相关要求，即检视数据跨境流动的限制能否与《协议》文本适恰。

2.1 理念的考察：协同治理与平衡发展与安全

孟德斯鸠在《论法的精神》中提到法律的精神是指法律所体现的理性、公正、平等、自由和人道主义的价值观念，强调法规不是孤立存在，其背后蕴含着这些重要的价值理念，并且这些价值理念要贯穿于法律的制定和执行过程中^[12]。因此，在检视规则之前，应对《协议》文本和我国数据跨境流动规则的理念进行考察。《协议》文本数据跨境流动规则以协同治理为其理念基础，具体体现为多方主体参与、利益关系协调、制度协同并行；以流动性优化为准则，具体体现为电子方式便捷交易、免征关税降低成本、保障安全稳定交易。我国的数据跨境流动规则秉持平衡发展与安全理念。因《协议》文本是各缔约方利益调适的结果，并非单独强调“美式自由”或“欧式权利”，而是倡导数据便利流动、保障安全稳定交易，所以《协议》文本和我国的数据跨境流动规则的理念能够契合。

2.2 数据储存本土化和出境安全评估：一般例外和安全例外条款的援引

《网络安全法》要求关键信息基础设施的运营者进行“数据本地化存储和跨境安全评估”。按照《促进和规范数据跨境流动规定》，若关键信息基础设施运营者向境外提供个人信息或重要数据，非关键信息基础设施运营者提供重要数据、100万以上（不包括敏感个人信息）个人信息或者1万人以上敏感个人信息，那么就需要进行出境安全评估。这正是我国平衡发展与安全的数据跨境流动规则为

了保障数据安全,为数据跨境传输创造条件的体现,也是数据主权的具体实践。作为《协议》缔约国,我国行使数据主权利要求数据存储本地化和跨境安全评估应当兼顾《协议》的要求,数据本地化存储和跨境安全评估对外效力的实现需要以《协议》例外条款作为支撑。

数据本地化存储和跨境安全评估措施在《协议》文本之下的合规性考察,需要证明该措施符合《协议》“一般例外”和“安全例外”的情形。基于此,《协议》一般例外和安全例外条款的解读成为了问题的关键。第22条一般例外规定《协议》文本比照适用《1994年关税与贸易总协定》第20条及其解释说明和《服务贸易总协定》第14条。《1994年关税与贸易总协定》第20条及其解释说明包含了一系列允许缔约方在特定情况下采取偏离总协定一般规则措施的规定,即允许缔约方在特定条件下采取可能与总协定其他规则相冲突的措施,这些情况通常涉及公共道德、人类和动植物生命健康、自然资源等方面。《服务贸易总协定》第14条也约定了公共道德和生命健康例外情形,相比《1994年关税与贸易总协定》第20条的特殊之处在于C款的例外,即个人信息处理和传播过程中的个人隐私保护。综上,一般例外的情形主要包含公共道德、人类和动植物生命健康、自然资源、个人隐私保护等方面。

《协议》文本第23条是安全例外条款,该条规定,就《协议》而言,《1994年关税与贸易总协定》第21条和《服务贸易总协定》第14条之2应比照适用。以上协定中均涉及安全例外规定,主要涵盖了国家安全相关的例外情形,允许缔约方在特定情形下为保护自身安全利益采取限制贸易的措施。在电子商务中,如果传输的内容涉及国家安全,缔约方就可以参考此条款采取限制措施。在服务贸易领域的跨境数据流动中,若某些服务(如云计算涉及大量敏感信息)可能威胁国家安全,缔约方可依据以上条款行动,如限制特定国家的云服务提供商进入本国市场,防止数据被恶意获取,保障信息安全。当然,缔约方必须证明其目的真实且手段具有必要性,即援引该条款应当承担的证明责任包括:其一目的真实,以“善意原则”阐明数据本地化存储和跨境安全评估措施保护何种安全利益;其二手段必要,证明数据本地化存储和跨境安全评估措施与安全利益之间具有“最小合理”的关联性^[13]。

首先,针对《网络安全法》要求关键信息基础设施的运营者进行“数据本地化存储和跨境安全评估”。基础设施这一概念常见于反垄断法领域,一般指电力、交通等领域因承担公共性和基础性社会功能的设施,应当保持开放性和中立性。《网络安全法》语境下的关键信息基础设施与此具有相似性,该法第31条和《关键信息基础

设施安全保护条例》规定,关键信息基础设施是指具有“一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益”的重要行业和领域,如金融、公共服务等。在关键信息基础设施运行时,数据不可或缺,如果该数据遭到破坏、泄露或丧失功能,必然会导致国家利益受损。如“滴滴出行案”,滴滴作为中国最大的出行和交通平台,拥有中国所有城市的详细地理数据、城乡道路信息等,这些数据经过分析和加工,可用于多种用途,关系到国家地理信息安全和战略安全。因此,滴滴应是关键信息基础设施的运营者,如果上述数据不在本地存储,而是在境外存储,势必会影响国家对相关数据的掌控。因此关键信息基础设施的数据本地化存储与“安全利益”之间存在“最小合理”的关联度。而关乎国家安全的数据需要本地化存储,当相关数据出境时遵循严格的数据出境制度对其进行出境安全评估自然具有合理性,放任关乎国家利益的数据自由出境,同在境外存储该类数据一样皆不能有效保障相关领域的数据安全,进而难以维护国家安全、保障国计民生。

其次,针对《促进和规范数据跨境流动规定》要求非关键信息基础设施运营者提供重要数据时进行出境安全评估。《数据出境安全评估办法》规定重要数据是指“可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”。目前在全国范围内并无统一的重要数据目录。《网络安全管理条例》通过专章的形式规定了重要数据安全,对重要数据处理者设定了诸如风险评估、方案报告等安全保护义务。《数据安全技术数据分类分级规则》(GB/T43697—2024)为重要数据目录的制定提供了技术标准和参考依据,明确了数据分类分级的原则、框架、方法和流程。数据分类根据业务特点和数据属性可以划分为个人信息、商业秘密、国家秘密等;数据分级则根据数据敏感性、重要性和潜在风险可以划分为一般数据、重要数据、核心数据等。该标准同样强调重要数据的损毁可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅涉及组织或个人的数据则一般不是重要数据。该标准还将“重要数据识别指南”作为规范性附录G纳入体系。在前述定义的基础上,重要数据识别还应考虑以下因素:可被其他国家或组织利用发起对我国的军事打击,或反映我国战略储备、应急动员、作战等能力,如满足一定精度指标的地理数据或战略物资产能、储备量有关的数据等。通过对重要数据的解读发现,重要数据一般牵涉到国家、经济、社会安全等。对于这一类关乎国家安全的重要数据应纳入《协议》安全例外条款的规范,对重要数据出境执行安全评估、限制其跨境流动具有合法性和合理性。

最后,针对《促进和规范数据跨境流动规定》要求非关键信息基础设施运营者提供 100 万以上个人信息(不含敏感个人信息)或者 1 万人以上敏感个人信息的安全评估。个人信息的关键在于可识别到具体的自然人,不包括脱敏无法识别后的信息^[11]。敏感个人信息是指一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。《协议》文本一般例外条款参照适用的《服务贸易总协定》第 14 条 C 款强调了对个人信息中个人隐私的保护。该款规定,“个人隐私保护”可以得到一般例外条款的援引。隐私是指“自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”。敏感个人信息属于个人信息,个人隐私一定属于个人信息,但是个人信息不一定属于个人隐私,个人隐私和敏感个人信息有可能交叉存在。若上述个人信息和敏感个人信息中包含个人隐私,则对于该类数据的出境采取安全评估可以通过《协议》一般条款的援引获得依据;若不包含个人隐私则只能通过下文个人数据保护例外条款的援引获得支撑。

2.3 保护认证和标准合同:个人数据保护专条和个人数据保护例外条款的援引

《促进和规范数据跨境流动规定》对订立个人信息出境标准合同或者通过个人信息保护认证的情形作出了规定。标准合同和保护认证在一定程度上是对数据跨境自由流动的限制,但其目的在于有序促进数据安全、自由流动,更是为了降低出境的合规成本。标准合同和保护认证均针对个人信息,《协议》文本中设定了个人数据保护专条和个人数据保护的例外规定。《协议》文本中的“个人数据”指“已识别或可识别的自然人相关的任何信息”,而个人信息不包括匿名化处理后的信息,因此,个人数据的范畴大于个人信息。针对包含个人信息的个人数据,《协议》文本通过专条规定要求构建或维持相关法律框架以保障电子商务用户的个人数据安全,保证对自然人的个人数据给予非歧视性保护。推动保护机制兼容,以便数据跨境流动,鼓励各方就实施机制交流信息,促进跨境数据流动中个人数据保护。因此,我国数据出境制度对非关键信息基础设施运营者提供 10 万人以上、不满 100 万人个人信息(不含敏感个人信息)或者不满 1 万人敏感个人信息应当依法订立标准合同或者通过保护认证的规定能够获得《协议》个人数据保护专条的支持。

同时,《协议》文本中规定了个人数据保护例外,“协议中的任何规定,均不妨碍一缔约方通过或维持有关个人数据和隐私的保护措施,包括与跨境数据传输的相关的措施,前提是该缔约方的法律规定了在普遍适用的条件下,允许数据传输的机制,以保护传输的法律。”我

国在统筹发展与安全理念下,通过数据分类分级保护制度,对数据跨境传输适用不同的出境制度。我国作为《协议》文本缔约方,通过《促进和规范数据跨境流动规定》等法律制度,在普遍条件下规定了允许并保护数据跨境传输的机制。保护认证和标准合同作为有关个人数据和隐私出境的规范、保护措施,能够适用《协议》文本个人数据保护例外条款的规定。因此《协议》文本中的任何规定,都不影响个人信息保护认证和个人信息出境标准合同的实施。此外,如前文所述,非关键信息基础设施运营者提供 100 万以上个人信息(不含敏感个人信息)或者 1 万人以上敏感个人信息时,若不包含个人隐私,则可以通过个人数据保护例外条款的援引获得对其适用出境安全评估的支撑。

综上所述,我国的数据跨境流动规则平衡发展与安全的理念能够与《协议》文本协同治理的理念相契合。我国数据存储本地化和数据出境安全评估、个人信息出境标准合同、个人信息保护认证制度等数据出境制度能够满足《协议》文本个人数据保护条款、一般例外、安全例外和个人数据保护例外条款的要求,可以获得支持并援引其作为合规性依据。但是,在检视我国的数据跨境流动时,笔者也发现须对国家重要数据目录进行改进和完善。

3 《电子商务协议》文本下我国数据跨境流动规则的完善

通过前文的分析可以得出:我国的数据跨境传输制度以数据分类分级保护制度为基础,以个人信息、个人数据等为分类,一般数据、重要数据、核心数据为分级,对数据跨境传输适用不同的出境制度。国内对数据跨境传输的制度限制,能够在《协议》文本中得到援引。然而,国家重要数据目录作为数据分类分级制度保护的基础,其完善与否直接关乎着我国数据出境制度的正确适用。但是,由前文的分析可知,我国尚未建立起全国范围内的重要数据目录。《数据安全法》《促进和规范数据跨境流动规定》等相关法律法规仅提出要建立重要数据目录。虽然《数据安全技术数据分类分级规则》(GB/T43697—2024)为重要数据目录的制定提供了技术标准和参考依据,以“定义+列举”的形式推进了重要数据目录的识别与建立工作,但是该规定仅为国家推荐性标准,并不具有强制力,也未被相关法律法规、监管要求等提及,并无约束性。

虽然我国尚未建立全国性重要数据目录,但是一些地区、行业正积极开展试验试点工作。上海市于 2022 年便在市委网信办和市政府办公厅的组织下开展数据分类分级、制定重要数据目录试点,圆满完成了 16 家单位的

试点工作;随后,上海市通信管理局启动“浦江护航”2023年电信和互联网行业数据安全专项行动,组织首批重点企业开展重要数据识别认定及目录备案工作;《临港新片区数据跨境流动分类分级管理办法(试行)》提出,2024年临港新片区将率先围绕智能网联汽车、金融理财、高端航运等重点领域的具体场景,陆续发布一批重要数据目录。当然,除了北京、上海等地,西部地区也有提出要尽快推动建立重要数据目录的城市,如《大理州数据治理工程数据存储管理规定》明确提出建立核心数据和重要数据目录,鼓励市场主体将本单位核心数据和重要数据目录向州数据管理行政主管部门备案。

当前,我国已在多个地区对建立重要数据目录工作进行了充分试点,积累了经验。在建立全国范围内的重要数据目录时,可以考虑:一是贯彻分类分级制定理念。数据分类不仅可以分为个人数据、企业数据、公共数据,还可以按照行业类型分为工业数据、金融数据、医疗数据等;数据分级不仅可以基于风险等级区分为一般数据、重要数据、核心数据,还可以基于管理级别划分为州(市)级数据、省级数据、国家级数据。这也是当前我国数据治理的思路。自2023年10月成立国家数据局以来,各省、州(市)积极推进数据治理工作,相继建立地方数据局,并在工业和信息化、电信等领域分行业推进重要数据识别和目录建立工作。二是落实目录制定主体责任。重要数据目录的制定是一个多方主体协同参与的工作,全国性的重要数据目录需要国家部门统筹,行业主管部门分工,各管理级别联动,各行各业人才参与。《工业和信息化领域数据安全管理办法(试行)》即要求工业和信息化领域的数据处理和安全保护监管须在国家数据安全协调机制统筹下,工业和信息化部负责督促指导各省级和计划单列单位工业和信息化主管部门。同时明确了工业和信息化部负责组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定标准规范,指导开展数据分类分级管理工作,制定行业重要数据和核心数据具体目录。三是建立动态管理机制。数据的价值基于流动而释放,其风险程度也并非一成不变,应当建立“定时评估+动态调整”机制,由行业主管部门联合技术人才、法律人士、行业专家、数据处理主体组成评估小组,定时评估数据的重要性变化。如因技术迭代,相关数据的重要性上升,或因脱敏技术成熟,相关数据的风险下降时,须做好数据处理安全评估工作,同步更新目录,实施动态管理。此外,动态管理机制还有利于应对新型网络攻击、重大安全事件等突发情况。

健全重要数据目录不仅有助于正确适用数据出境制度,而且有助于我国的数据出境制度能够顺利得到《协

议》文本个人数据保护条款和例外条款的援引。对此,应当优先在数据贸易、跨境金融等数据跨境需求旺盛的行业试点目录应用。做好国际合作与规则互认工作,将我国的数据分类分级治理经验推广至国际数据治理规则,提升我国重要数据目录的国际认可度,推动主要贸易伙伴的重要数据目录互认。例如通过重要数据类型互认清单,促进双方对目录中同等风险等级数据管理标准的认可,减少重复评估,为企业“走出去”提供规则保障,促进我国数据经济和国际贸易的繁荣发展。

参考文献

- [1] 李墨丝. WTO 电子商务规则谈判: 进展、分歧与进路 [J]. 武大国际法评论, 2020, 4 (6): 55 - 77.
- [2] 中国世界贸易组织研究院. 国际经贸规则量化分析报告: WTO 电子商务谈判达成“稳定协议” [R]. 中国世界贸易组织研究院, 2024.
- [3] 夏菡. 欧盟数据跨境流动监管立法的市场规制转向及对中国的启示 [J]. 河北法学, 2023, 41 (8): 169 - 182.
- [4] 洪延青. 推进“一带一路”数据跨境流动的中国方案——以美欧范式为背景的展开 [J]. 中国法律评论, 2021 (2): 30 - 42.
- [5] 杜玉琼, 裘韵. WTO 数据跨境流动规则建构的困境与中国方案研究 [J]. 四川大学法律评论, 2022, 20 (1): 3 - 20.
- [6] [英] 齐格蒙特·鲍曼. 共同体: 在一个不确定世界中寻找安全 (第1版) [M]. 欧阳景根, 译. 苏州: 江苏人民出版社, 2003.
- [7] 张晓君, 屈晓濛. RCEP 数据跨境流动例外条款与中国因应 [J]. 政法论丛, 2022 (3): 109 - 119.
- [8] 黄秋红, 李雅颖. 对接 CPTPP 数据跨境流动规则研究 [J]. 南海法学, 2022, 6 (1): 115 - 124.
- [9] 李烨. RCEP 协定下我国数据跨境流动规则的检视与完善 [J]. 科技与法律 (中英文), 2023 (1): 119 - 128.
- [10] 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.
- [11] 梅傲, 侯之帅. 总体国家安全观视域下企业跨境数据的合规治理 [J]. 江苏社会科学, 2022 (6): 169 - 176.
- [12] 孟德斯鸠. 论法的精神 [M]. 许明龙, 译. 北京: 商务印书馆, 2012.
- [13] Panel Report. Russia-measures concerning traffic in transit [R]. WT/DS512/R, 2019.

(收稿日期: 2025 - 03 - 18)

作者简介:

何云富 (1999 -), 男, 硕士研究生, 主要研究方向: 数据法学、刑法学。

赵庆超 (1999 -), 男, 硕士研究生, 主要研究方向: 行政法学、数据法学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com