区域贸易协定数据本地化与例外问题研究

郑玲丽

（南京师范大学法学院，江苏 南京 210046）

摘　要：跨境电子商务的数据本地化及隐私保护是当前国际贸易法领域新兴而未决的问题。欧盟法院和美国联邦最高法院裁决的两起数据隐私诉讼案，虽然没有直接创立数据本地化法律制度，但突出了美国和欧盟在数据隐私方面不可调和的不同做法，并排除了有效的跨境数据传输路径，使得数据本地化成为仅存的弹性解决方案。WTO 电子商务谈判前景不明，而以 CPTPP 电子商务规则和 USMCA 数字贸易规则为代表的新生代区域贸易协定禁止数据本地化，禁止强制公开源代码，大有合围建构全球跨境电子商务规则的样板之势。未来示范性区域电子商务规范应基于数据类型，有效规范跨境数据流动及数据本地化措施，同时界定合法的公共政策例外，这是弥合跨境电子商务规则碎片化的举足轻重的区域法治现代化变革。

关键词：CPTPP；USMCA；跨境电子商务；数据本地化；公共政策

中图分类号：D996　　**文献标识码：**A　　**文章编号：**1006-1894（2020）04-0085-12

由于 WTO 电子商务谈判前景不明，区域贸易协定（Regional Trade Agreements，以下简称 RTAs）已然成为试图解决“与贸易相关电子商务法律问题”（Trade Related E-commerce Legal Issues）的试验田。《跨太平洋伙伴关系协定》（Trans-Pacific Partnership Agreement，以下简称 TPP）作为第一个将电子商务纳入谈判议题的新型 RTA，其生效和实施对亚太区域乃至多边跨境电子商务的发展有着至关重要的影响。美国 2017 年退出 TPP 后，其余 11 个缔约方在 2018 年 3 月 8 日签署了《跨太平洋伙伴关系全面渐进协定》（CPTPP）。[①] CPTPP 是一个“21 世纪”的贸易协定，将比重商主义和实用主义的 WTO 协定更符合当代国际贸易现实。[②] 此外，2018 年 9 月 30 日，美国、墨西哥和加拿大达成《美墨加贸易协定》（The

作者简介：郑玲丽，南京师范大学法学院副教授，法学博士，中国法治现代化研究院研究员，南京师范大学“一带一路”智库研究员，南京师范大学区域法治发展协同创新中心研究员，研究方向：国际经济法。

基金项目：国家社会科学基金 2016 年一般项目“TPP 环境章节文本分析及我国法律对策研究”（项目编号：16BFX04）；江苏高校优势学科建设项目（PPAD）阶段性研究成果。

① Comprehensive and Progressive Agreement on Trans Pacific Partnership[EB/OL]. 2017, https://www.mfat.govt.nz/assets/CPTPP/Comprehensive-and-Progressive-Agreement-for-Trans-Pacific-Partnership-CPTPP-English.pdf. [2018-08-10](2019-04-20).

② Mira, Burri. The Regulatory Framework for Digital Trade in the Trans-Pacific Partnership Agreement[C]. in Pedro, Roffe and Xavier, Current Alliances in International Intellectual Property Lawmaking: The Emergence and Impact of Mega-Regionals, Seuba, Geneva/Strasbourg: ICTSD and CEIPI, 2017.

United States–Mexico–Canada Agreement，以下简称 USMCA），修改和替代《北美自由贸易协定》（NAFTA）。新协议数字贸易章节颇具特色。以美式 FTA 电子商务条款为基础的电子商务规则在某种程度上将成为国际电子商务立法领域的标杆和范本。CPTPP 电子商务规则和 USMCA 数字贸易规则中禁止数据本地化的立法模式将对未来 RTAs 电子商务谈判和规则制定产生深远影响。

一、数据本地化的缘起与现状

随着越来越多的电子商务模式和实践转移到数字平台，数据在国际范围内越来越多地共享和交换，其与跨境电子商务的关系也越来越密切。由于数据是在全球基础上由众多缔约方收集、数字化、存储和移动，因此有关数据的域内限制措施和法律规定直接影响跨境电子商务的发展。面对数据安全和隐私的担忧，世界各国许多立法机构都在转向实施数据本地化措施。

数据本地化（Data Localization）有两层含义。第一，是指各国政府强制互联网主机将本国互联网用户的数据存储在该国政府管辖范围内的服务器上（本地化数据托管）。存储在本地管辖区内的数据可以是数据的唯一副本，也可以是发送到另一个管辖区内存储或处理的数据本地副本。第二，即各国政府强制互联网服务提供商通过仅位于其管辖范围内的网络在其管辖范围内的互联网用户之间发送数据包（本地化数据路由器）（陈寰琦等，2019）。本文只讨论第一类数据本地化。

世界各国针对数据本地化采取了一系列不同政策措施，主要分为两大类：

（1）反对数据本地化政策。发达国家认为，数据本地化是数字贸易的大敌，跨境信息传输中的数据存储设施本地化要求是阻碍发达国家电子商务发展的重要因素（陈咏梅等，2017）。以美国为首的国家强烈反对数据本地化，认为数据本地化政策是一种“有害的非关税壁垒形式，它损害了数字贸易的增长”（洪延青等，2018），可能构成数字贸易壁垒，会导致互联网的“巴尔干化”（Balkanization of the Internet）。[①]美国政府大力推动新一代 RTAs 跨境电子商务规则，全面禁止计算设施本地化，禁止强制公开源代码，从而在区域法治层面限制其他国家实施数据本地化的努力。鉴于在全球层面就跨境电子商务问题达成协议困难重重，新一代 RTAs 中禁止数据本地化条款将产生规则溢出效应，受影响国家的数量和范围都有所增加。

（2）支持数据本地化政策。中国等为数不少的国家则坚持数据本地化，理由如下：首先，数据本地化提供了更好的针对外国情报机构的信息安全；其次，数据本地化保护公民数据的隐私和国家安全；再次，数据本地化支持地方执法。

① Albright Stonebridge Group. Data Localization: A Challenge to Global Commerce and the Free Flow of Information[EB/OL]. http://www.albrightstonebridge.com/files/ASG Data Localization Report September 2015.pdf, [2015–09–20](2020–03–18).

2018年美国《国家贸易评估报告》详细列举了主要国家的数字贸易壁垒措施：中国、印度尼西亚、尼日利亚、俄罗斯、土耳其、越南等对跨境数据流动的限制和数据本地化要求，中国和泰国的网络过滤和屏蔽，韩国对基于位置的数据跨境传输限制等。[①]

二、数据本地化与隐私保护案例述评

最近在欧盟法院和美国联邦最高法院裁决的两起数据隐私诉讼案，虽然没有直接创立数据本地化法律制度，但突出了美国和欧盟在数据隐私方面不可调和的不同做法，并排除了有效的跨境数据传输路径，使得数据本地化成为仅存的弹性解决方案。

（一）数据保护署专员诉施雷姆斯案

跨境数据传输分为两类：商业传输和执法传输。商业数据传输首先在数据保护署专员诉施雷姆斯案（Data Protection Commissioner v. Schrems I，以下简称Schrems I）[②]中受到质疑。

2014年，奥地利律师马克西米利安·施雷姆斯(Maximillian Schrems)向爱尔兰数据保护署(DPA)提交了一份针对Facebook爱尔兰子公司的指控，称根据欧盟法，美国法律未能对美国的大规模监控提供足够的数据保护。[③]施雷姆斯的指控是直接响应斯诺登事件，他认为Facebook与美国国家安全局棱镜项目合作，涉嫌违反1988年和2003年《欧盟数据保护指令》（EU Data Protection Directive）及2000年《安全港决议》（EU-U.S. Safe Harbor Agreement）。[④]在初级法院失利后，施雷姆斯上诉至爱尔兰高等法院。该院经司法审查发现，一旦个人数据被转移到美国，美国国家安全局和联邦调查局能够通过大量不加选择的监测和搜集数据访问个人信息。虽然该院承认这种行为违反了爱尔兰的宪法和数据保护法，但这个问题最终涉及欧盟法的解释和适用，因此将案件提交给欧盟法院。

在分析施雷姆斯的诉讼请求时，欧盟法院全面审查了《安全港协议》与《欧盟数据保护指令》。欧盟法院认为，美国法律没有提供基本上相当于欧盟法的足够程度的保护，因为美国政府允许普遍获取电子信息，而没有提供救济机制。[⑤]2015年10月6日，欧盟法院推翻了《安全港协议》作为从欧盟向美国转移数据的有效法律

① 2018 Fact Sheet: Key Barriers to Digital Trade[EB/OL], https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital. [2018-03-15] (2020-03-22).
② S[2016] IEHC 414 (Hi. Ct.) (Ir.).
③ See Written Observations of Applicant 21-23, Case C-362/14, Schrems I, 2014 E.C.R. 6[EB/OL], http://www.europe-v-facebook.org/CJEU_subs.pdf. [2014-08-26] (2020-03-24).
④ Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215), p.7~47.
⑤ Schrems I, 2014 E.C.R. 81~82, 93, 95; Charter of Rights, Article. 7.

依据的规定。[①]本案裁决的直接后果是，安全港制度下所有从美国转移到欧盟的数据将违反《欧盟数据保护指令》。[②]安全港制度的失效造成了法律上的不确定性和新制度安排的必要性。然而，该指令仍然允许公司使用标准合同条款（Standard Contract Clauses, 以下简称 SCCs）或其他减损（例如同意）作为可替代数据转移机制，直至欧美《隐私盾协议》（EU-U.S. Privacy Shield）[③]出台。该协议旨在纠正 Schrems I 所述的问题，并允许公司自行证明其遵守了《隐私盾协议》中隐私保护原则的承诺。2016 年 7 月 12 日，欧盟委员会 (European Commission) 发布了关于《隐私盾协议》的决定，认为新的框架确保了对跨境数据传输的足够保护。[④]虽然该决定受到了美国和欧盟企业的欢迎，但《隐私盾协议》却遭到了广泛批评。虽然《隐私盾协议》为公司提供了一种证明采取了足够安全防护措施的机制，但仅适用于美国联邦贸易委员会管辖范围内的公司。不在此管辖范围内的公司一般依据《欧盟数据保护指令》第 26(2) 条所规定的提供充分数据转移基础的 SCCs。然而，在下文讨论的 Schrems II 中，施雷姆斯对这些条款是否适当提出了质疑。

继 Schrems I 之后，施雷姆斯向 DPA 提交了第二份投诉，质疑 SCCs 的有效性，该案被称为“Schrems II”。DPA 根据《欧盟数据保护指令》对美国法律的充分性进行调查。最后结论是，虽然它对《欧盟宪章》所载条款的有效性提出质疑，但在爱尔兰高等法院或欧洲高等法院就这些条款的有效性作出裁决之前，它无法作出最后决定。[⑤]爱尔兰高等法院审理了该案件，并审查了 DPA 的决定。最后，爱尔兰高等法院同意 DPA 就 SCCs 的有效性所作的裁决。然而，爱尔兰高等法院也发现自己受到司法管辖的约束，因为撤销案件将等于默认 SCCs 的存在。2017 年 10 月 3 日，爱尔兰高等法院正式将 Schrems II 提交给欧盟法院，对 SCCs 的有效性进行初步裁定。[⑥]鉴于 88% 的公司使用 SCCs 将个人数据从欧盟转移到美国，此案审理结果将受到密切关注。[⑦]

---

① McCann, Fitzgerald. Commercial Court Affirms Legal Principles on Admission of an Amicus Curiae, Lexology[EB/OL] https://www.lexology.com/library/detail.aspx?g=8be84b34-c0b7-4a66-9542-fdde0db0e269. [2016-08-03] (2020-03-26).

② See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), at 4 COM (2015) 566 final.

③ EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce[EB/OL]. https://www.privacyshield.gov/servlet/ servlet.FileDownload?file=015t00000004qAg. (2020-03-26).

④ See Commission Implementing Decision of July 12, 2016. Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of Protection Provided by the EU-U.S. Privacy Shield, art. 1, 13, C (2016) 4176 final[EB/OL]. http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacydecision_en.pdf. [2016-07-12] (2020-03-29).

⑤ Draft Decision of the Data Protection Commissioner 62, Schrems II, [2016] IEHC 414 (Hi. Ct.) (Ir.) (No. 4809P)

⑥ See Commission Decision 2011/497/EC of June 2001, 2001 O.J. (L 181) 19; Commission Decision 2004/915/EC of 27 December 2004, 2004 O.J. (L 385) 74; Commission Decision 2010/87/EU of 5 February 2010, 2010 O.J. (L39) 5.

⑦ Lee, Matheson. Understanding “Schrems 2.0” IAPP[EB/OL]. https://iapp.org/news/a/understanding-schrems-2-0. [2017-10-03] (2020-04-01).

（二）美国诉微软公司案

影响用户数据跨境传输的另一典型案例是美国诉微软公司案（United States v. Microsoft Corp.）。[①]此案关键争议点在于：根据1986年美国《存储通信法案》（the Stored Communications Act，SCA），美国政府的搜查令是否能要求通信服务商提交存储在美国境外的数据？

2013年12月，美国联邦调查局（FBI）向纽约南区联邦地方法院申请搜查令，要求微软公司披露所有客户账户相关的电子邮件和其他信息。联邦执法人员已经证明有足够的理由相信该账户被用于进一步的非法毒品交易，但该用户的数据仅存储在位于爱尔兰都柏林的微软数据中心。微软公司披露了搜查令中要求的所有其他信息，但请求地方法官撤销有关都柏林存储的用户数据的搜查令，理由是1986年《存储通信法案》没有授权联邦法院强制执行已存储在美国境外的数据，即坚持“数据存储地标准”。纽约南部巡回法院驳回了这个论点，认为《存储通信法案》授权地方法院对“存储在国外服务器上的信息”发出搜查令。地方法官认为，相关的执行地是政府审查内容所在地美国，而不是内容存储所在地爱尔兰，即坚持“数据控制者标准”。微软公司立即上诉。

纽约第二巡回上诉法院推翻了初审裁决，并裁定《存储通信法案》不能授权强制执行美国服务供应商已存储在外国的数据。[②]第二巡回法院确定《存储通信法案》的主要焦点是存储通信的隐私，因此，法院应适用侵犯隐私发生地法。由于对用户隐私的实际侵犯发生在爱尔兰数据中心（Irish Data Center），法院裁定将适用爱尔兰法律，而不是美国法律。2017年10月16日，最高法院批准调审此案。[③]那么，根据《美国联邦法典》（U.S.C）第18卷第2703节的规定，即使电子邮件记录仅存储在美国境外，被送达的电子邮件供应商是否也必须向联邦政府提供电子邮件？

2018年3月23日，美国国会制定并签署了《明确合法海外使用数据法案》（the Clarifying Lawful Overseas Use of Data Act，CLOUD Act；以下简称《云法案》）。《云法案》[④]修正了《存储通信法案》，明确采纳了“数据控制者标准”，只要数据在美国的数据控制者手中，默认的情况是美国政府能够直接从全球各地调取，仅在少数情况下是例外，而且例外的大小宽窄均由美国法院单独裁量决定（王亮，2016）。

---

① Andrew, Keane Woods. A Primer on Microsoft Ireland, the Supreme Court's Extraterritorial Warrant Case[EB/OL]. https://www.lawfareblog.com/primer-microsoft-ireland-supreme-courtsextraterritorial-warrant-case. [2017-10-16](2020-04-02).

② Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d at 222.

③ United States v. Microsoft Corp., 138 S. Ct. 356 (2017).

④ 《云法案》第103条(a)款(1)款加入以下条文：“无论通信、记录或其他信息是否存储在美国境内，服务提供者均应当按照本章所规定的义务要求，保存、备份、披露通信内容、记录或其他信息。”

根据最新法案，美国政府新颁布了一个搜查令。鉴于本案双方同意搜查令以新代旧，且双方对获准调查的问题没有任何实际争议，最高法院认为此案已变得毫无意义。2018 年 4 月 17 日，最高法院判决发回美国第二巡回上诉法院重审。虽然评论人士倾向于认为美国法院会站在美国政府一边，但是这对双方都有不利的影响。[①]另外，美国法院的判决可能会减损美国在 Schrems II 上的首战告捷效果，因为美国政府将对欧盟居民适用美国法，而不是欧盟法，从而增加美国执法部门可以不受限制地访问欧盟用户数据的印象。

（三）综合点评

上文第一起案件限制了出于商业目的的用户数据跨境移动，而第二起案件可能会限制执法部门访问美国公司在外国持有的用户数据。然而这两起案例有两个关键联系点。首先，对于公司遵守国内法院的命令持有的数据，公司必须将数据从外国转移到美国，以便向美国执法部门披露信息。如果数据存储在欧盟，则此传输将自动涉及适用《隐私盾协议》、SCCs 或其他传输工具。其次，由于微软公司案也影响了美国执法部门获取用户数据的范围，因此该判决将被纳入欧盟法院在 Schrems II 中的判决，对《隐私盾协议》也构成挑战，最终都将要求企业数据本地化，以确保遵守事实上的数据本地化制度。

概括而言，这两个案例将以两种方式推进数据本地化：（1）取消用于商业数据传输的合法跨境数据传输机制；（2）为执法目的分配数据的领域。Schrems I 和 Schrems II 本身就强调了欧盟和美国在隐私保护方面的根本差异，并明确指出美国的做法不当，从而促进了数据本地化。此外，由于 SCCs 和《隐私盾协议》均以相同的充分性标准为基础，因此，SCCs 的失效亦会增加《隐私盾协议》面临的挑战，并使欧盟法院难以支持后者的体系。因此，尽管美国在《安全港协议》失效后做出了一些改变，但如果 SCCs 和《隐私盾协议》进一步失效，将表明美国和欧盟之间的隐私保护差异是不可调和的。微软公司案进一步推动了数据本地化的趋势，因为它确保了数据所在地法律限制执法部门访问这些数据。综上所述，两起案例有效地在无国界的网络中设立了领土边界，限制了企业跨境传输和接收数据的能力，也限制了执法机构访问数据。

如果欧盟法院认定 SCCs 和《隐私盾协议》无效，美国可以有两个选择：（1）通过立法加强隐私保护以满足欧盟标准；（2）对数据进行本地化。在欧美《隐私盾协议》谈判中，美国修改了许多法律，并实施了各种保护措施，以加强对欧盟公民数据的隐私保护。考虑到美国政府已做出改变的程度，国会似乎不太可能立法加强

① Jennifer, Daskal. There's No Good Decision in the Next Big Data Privacy Case[EB/OL]. N.Y. TIMES. https://www.nytimes.com/2017/10/18/opinion/data-abroad-privacycourt.html. [2017-10-18] (2020-04-04).

隐私保护。此外，正如 DPA 委员在 Schrems II 中的决定草案所反映的那样，几个有争议的问题涉及关键的宪法分歧，如第三条的立场。[①]针对美国判例这些长期存在的原则，欧盟向美国发出了最后通牒，要求美国要么调整美国法律的基本原则，要么不要转移数据。因此，美国能否在不推翻数十年法律先例的情况下，在谈判桌上做出更多让步，的确让人疑窦丛生。

此外，从国家安全角度来看，美国的让步都将使美国受到比欧盟更大的限制。例如，在 Schrems I 之后，美国修订了《外国情报监听法》（Foreign Intelligence Surveillance Act，FISA）。这些保护措施与欧盟指令和 GDPR 所提供的保护措施相当，甚至超过后者。

三、CPTPP 和 USMCA 对数据本地化的限制及例外

在电子商务时代，数据为王。但与此同时，在数据本地化、隐私保护、法律适用与管辖权等法律问题上，欧美和其他国家各持己见。根据 UNCTAD 调查显示，截至 2016 年 4 月，全球已有 108 个国家制定了数据保护法规，但仍有 30% 的国家尚未出台相关法律。透过国际贸易法中围绕各国在数据本地化问题上的纷争，折射出不同国家在数据流动监管乃至数据主权上的分歧和博弈。

在 TPP 谈判中，美国为维护本国企业在全球数字贸易中的竞争优势，主张不受限制的跨境数据传输；而澳大利亚、新西兰、马来西亚和越南等国则强调必要的数据审查和个人信息保护，主张在跨境数据流动监管方面赋予政府更多的自由裁量权。由于美国极力倡导贸易数据的跨境自由流动，推动 TPP 成为第一个在“电子商务”章节中纳入具有约束力的规制跨境数据流动的自由贸易协定（王利明，2012）。

（一）禁止计算设施本地化和禁止强制公开源代码

CPTPP 第 14.13 条禁止强制计算设施本地化，使用了与跨境数据传输相同的例外条款，都是基于“合法公共政策目标”（legitimate public policy objective）的例外，即隐私和基本安全。但无论是依条约上下文还是语义解释，均无法对隐私和基本安全的含义做出恰如其分的解释，因此这些例外情形使得 CPTPP 禁止数据本地化条款的范围和可操作性变得不确定、不可预测。CPTPP 第 14.17 条禁止强制公开源代码，但只适用于“大众市场软件或包含这种软件的产品”（mass-market software or products）。[②]因为关键定义没有界定，该条同样产生了很大的不确定性。

① McCann, Fitzgerald. Commercial Court Affirms Legal Principles on Admission of an Amicus Curiae, Lexology[EB/OL], https://www.lexology.com/ library/detail.aspx?g=8be84b34-c0b7-4a66-9542-fdde0db0e269 [2016-08-03] (2020-04-05).

② CPTPP协定第14.17条第2款。

USMCA 第 19.12 条[①]则更进一步将 CPTPP 第 14.11（2）条[②]发展为一项措辞强硬的禁止性声明。除此之外，根据 USMCA 第 17.20 条，任何一方不得要求涵盖的人使用或定位计算设施作为开展业务的条件，只要该缔约方进入监管当局的监管或监督的目的在于直接完成或正在进行的信息获取位于处理或存储在计算设施外的人使用或定位的领域。一刀切地禁止强制计算设施本地化将对缔约方互联网行业的发展造成不公平竞争的局面。尽管市场力量帮助塑造了不平等的程度，但国家政策塑造了那些市场力量（王蕊，2016）。

CPTPP 电子商务章节乃至 USMCA 数字贸易章节均明令禁止计算设施本地化和禁止强制公开源代码，对金融服务和机构的本地化措施禁令有所放宽，政府采购也被排除在外，从而反映了美式 FTA 电子商务章节少有的“硬法”特色。美国势必会在日后的区域及多边规则的谈判中引入这一规则，对发展中国家的数据主权构成严峻的挑战。这些“硬核”条款在一定程度上是针对那些对美国现有企业构成重大竞争威胁的发展中国家，特别是中国（张子源译，2013）。这是中国在最近的 FTA 谈判中开始重视电子商务议题的原因之一（Avril，2002）。

（二）保护个人信息与隐私

虽然关于个人信息权的定义存在不同观点，但不能否认个人信息属于个人隐私的范畴。在 FTA 中最具政治敏感性和技术挑战性的问题之一就是个人隐私，包括通过电子手段跨境传输信息、计算设施的使用和位置以及个人信息保护。[③]

CPTPP 过度降低隐私和数据保护标准，[④]已经在国外学术界备受诟病。在个人信息保护的不同体制间，CPTPP 鼓励“缔约方增强不同体制的兼容性，包括对监管结果的认可，无论该认可是自主给予还是通过共同安排，或是通过更广泛的国际框架。”[⑤]

USMCA 第 19.8 条共有 6 款对“个人信息保护”做出了具体规定，且参照了《APEC 隐私框架》和 2013 年《OECD 隐私保护和个人数据跨境流动指南》。美国并没有象以往所签订的 RTAs（如 TPP 第 14.13 条）那样在 USMCA 中对“数据存储非强制本地化”设置例外条款。相对于 CPTPP 而言，USMCA 对个人信息保护设置了“武装到牙齿”的法律条款，并提高了国内保护标准。

① USMCA第19.12条规定：“任何一方均不得禁止或限制通过电子手段跨境传输信息，包括个人信息，如果该活动是为所涵盖人员的业务行为而进行。”

② CPTPP第14.11（2）条规定：“当通过电子方式跨境传输信息是为涵盖的人执行其业务时，缔约方应允许此跨境传输，包括个人信息。”

③ Robert, Wolfe. Learning about Digital Trade: Privacy and E-commerce in CETA and TPP[EB/OL], EUI Working Paper RSCAS 2018/27. https://ssrn.com/abstract=3188158. [2018-05-01] (2020-04-06).

④ CPTPP第14.8（2）条规定：“每一缔约方应采取或维持保护电子商务用户个人信息的法律框架。在建立对个人信息保护的法律框架过程中，每一缔约方应考虑相关国际机构的原则和指导方针。”该条注释规定：“为进一步明确，一缔约方可通过采取或维持措施，如保护隐私、个人信息或个人数据的综合性法律，涉及隐私的部门法律，或规定企业对隐私做出自愿承诺实施的法律，以符合本款规定的义务。”

⑤ CPTPP第14.8（5）条。

（三）合法的公共政策目标例外

CPTPP 电子商务章节和 USMCA 数字贸易章节旨在促进国际贸易自由化的措施与缔约国为实现合法公共政策目标（如保护人权、环境、公共健康、公共道德和文化等）而进行监管的主权之间试图达成平衡。

CPTPP 在其电子商务章节中纳入了合法公共政策目标例外条款，包括第 14.11（3）条通过电子方式跨境传输信息例外条款[①]和第 14.13（3）条计算设施的位置例外条款。[②]虽然这两个例外规定在很大程度上反映了 GATS 第 14 条的规定，但将其扩大到所有“合法的公共政策目标”，反映了 CPTPP 缔约方对 GATS 例外规定中可能适用的公共政策措施的潜在范围有限的担忧。[③]

而 USMCA 取消了这些豁免，导致对签署国的要求更加严格。根据 USMCA 附件 19-A，USMCA 第 19.17 条受第 32.1 条“一般例外”和 GATS 第 14（a）条“公共道德例外”约束。正如 Jacqueline 所指出：“在这方面，USMCA 在计算设施上的立场更加严格，其简化的语言允许的例外空间更小。”[④]

从 CPTPP 乃至 USMCA 合法的公共政策目标例外条款可以看出，新一代巨型 FTA 立法导向仍然是贸易至上，极力推动贸易自由化，而对缔约国公共政策目标予以“合法的”弹性条款进行平衡。这种“合法的”公共政策目标例外条款为今后贸易与公共政策例外争端埋下伏笔。维持区域贸易协定中数字贸易自由化和合法的公共政策目标间的平衡面临着独特的挑战，因为数字产业内在的某些特性和数字市场上的商务规则会引发严重的反竞争问题。

四、区域贸易协定的数据本地化规则与例外发展态势

美国原则上容忍了欧盟基于数据本地化的保护立法，并积极与欧盟执法机关之间开展必要的合作，以保障本国企业在欧盟数据市场的地位。但与此同时，美国非常重视加强 RTAs 层面对数据的掌控，美国诉微软公司案直接推动了美国国内法的修订。

跨境数据流动与货物流动同等重要，贸易政策制定者必须找到促进这些流动的方法。[⑤]如何在国家数据主权、公司利益与用户隐私安全的冲突之间达成平衡与协调？

---

① CPTPP第14.11（3）条规定：“本条不得阻止缔约方为实现合法公共政策目标而采取或维持与第2款不符的措施，条件是该措施：（a）不得以构成任意或不合理歧视的方式适用，或对贸易构成变相限制；及（b）不对信息传输施加超出实现目标所需要的限制。”

② CPTPP第14.13（3）条规定：“本条不得阻止缔约方为实现合法公共政策目标而采取或维持与第2款不符的措施，条件是该措施：（a）不得以构成任意或不合理歧视的方式适用，或对贸易构成变相限制；及（b）不对计算设施的使用或位置施加超出实现目标所需要的限制。”

③ Aaditya, Mattoo, Joshua, P. Meltzer, International Data Flows and Privacy: The Conflict and Its Resolution[R], World Bank Policy Research Working Paper 8431, 2018.

④ Jacqueline, Yin. Cross-Border Data Continues to Flow under the USMCA[EB/OL], http://www.project-disco.org/21st-century-trade/100518-cross-border-data-under-the-usmca/. [2018-10-05] (2020-04-06).

⑤ WTO Public Forum. USTR Froman Warns Poor Countries Would Be the Biggest Losers If Bali Fails[EB/OL]. http://www.wto.org/english/news_e/news13_e/pfor_01oct13_e.htm. [2013-10-01] (2020-04-06).

又有多少主权国家愿意在多高的透明度水平上放弃多少数据流动自由以换取何种水平的隐私安全？到目前为止，CPTPP 和 USMCA 并未澄源正本，厘清数据本地化与贸易壁垒的关系问题。从 CPTPP 到 USMCA，其中关于跨境电子商务最重要的条款——禁止数据本地化条款，也是最有可能成为未来贸易争端焦点的条款。展望未来 RTAs 数据本地化规则及其例外条款，应从以下几个层面规范数据本地化，防范数字贸易壁垒：

（1）数据本地化规则适用范围因数据类型不同而异。鉴于网络空间的无国界性质，在互联网上创建、获取和处理跨境数据不可避免产生公共政策影响，“一刀切”的决策是最不可行的。RTAs 成员可通过数据分类从而将数据与处理数据的贸易政策（包括防止数据跨边界移动的决策）耦合起来，在技术上可以对数据进行差异处理。[①] 根据数据类型，包括通过确保某些类型数据的市场准入来进一步开放数字经济，同时为其他类型的数据保留更大的监管自主权。例如，可以对数据的自由流动作出更多的横向承诺，即对不与个人或社会数据重叠的公司数据，在选择退出的情况下，对市场准入和国民待遇义务作出更多的横向承诺。这将导致一种允许某些数据自由流动的制度。但是，对于国家希望加强国内管制的数据，例如个人和社会数据，可以保留正面清单办法。

（2）RTAs 成员需证明数据本地化措施符合“公共政策目标”例外。RTAs 电子商务条款规范了参与跨境电子商务的国家、公司和个人的行为，而贸易协定由各国政府主导谈判，公司特别是个人的隐私保护和利益诉求容易被忽视。本文上述 Schrems I 和 Schrems II、美国诉微软公司案均从司法实践层面揭示了这一点。由于政府秉承的公共政策目标与公司、个人的利益和立场有差异，防止滥用“公共政策目标”例外条款的最佳方案是参考具有习惯国际法属性的具有普遍约束力的基本人权标准，如《世界人权宣言》。成员可考虑采用类似于《实施卫生与植物检疫措施协定》（SPS）的机制，由另一个在公共政策、公共道德问题上有管辖权的国际组织如联合国人权委员会制定标准，并在贸易与公共政策例外争端产生时将其授权给 WTO 争端解决机制予以裁决。在跨境电子商务司法实践中，援引公共政策例外的主要是隐私和安全问题。联合国及其机构可接受并倡导 2018 年生效的欧盟 GDPR 隐私保护标准，并在符合 1976 年生效的《公民权利和政治权利国际公约》（International Covenant on Civil and Political Rights，ICCPR）第 17 条[②]基础上，更新数字时代隐私权的

① Jatinder, Singh. Seeing through the Clouds: Managing Data Flow and Compliance in Cloud Computing[EB/OL]. https://www.cl.cam.ac.uk/research/srg/opera/publications/papers/ 2015ccmagSI.pdf. [2015-01-12] (2020-04-06).

② 《公民权利和政治权利国际公约》第17条规定：“1.对任何人的隐私、家庭、住宅或通信，不得无理或非法侵扰其名誉及信用，亦不得非法破坏；2.对于此种侵扰或破坏，人人有受法律保护之权利。”

文件。2016 年 3 月 8 日，联合国人权理事会根据第 28/16 号决议（“数字时代的隐私权”），已设立隐私权特别报告制度，调查各国隐私保护状况。虽然当代政府都把保护人权（特别是公民的安全）作为头等大事，认为“保护人权本身是不可谈判的”，但哪怕是 ICCPR 在全球也欠缺法律约束力或强制执行力。然而，区域贸易协定具有强制约束力和可具体执行的承诺，使得它们成为监管跨境数据流动、保护个人隐私和安全的一个有吸引力的工具。

（3）RTAs 成员需证明数据本地化措施不构成“数字保护主义”（Digital Protectionism）或“数字贸易壁垒”（Digital Trade Barrier），即不会导致任意的或无理的歧视，也不会对跨境数据流动构成变相限制或者扭曲。数据本地化措施主要分为 3 种：强制本地数据存储（Forced Local Data Storage），如中国、俄罗斯和越南；特定部门的数据存储要求（Sector-Specific Data Storage Requirements），如加拿大和澳大利亚；限制数据传输（Restrictions on Data Transfers），如欧盟。无论成员采取哪种数据本地化措施，与其他贸易保护措施一样，都要通过“必要性”测试（necessity test）。RTAs 可借助 WTO“必要性测试”的判例。WTO 专家组和上诉机构在最近的案件[①]中认定，根据 GATT 第 20 条，评价一项措施“必要性”的路径取决于风险的性质、所追求的目标和所寻求的保护水平。问题的关键在于数据本地化措施与其所依据的公共政策目标之间的联系。[②]在必要性分析下，数据本地化措施的权衡还要考虑是否存在与 WTO 一致的可替代措施？或者是否有与 WTO 宗旨目标更符合的合理可行的措施？可替代措施必须前后一致，同时对受质疑的数据本地化措施所追求的目标的实现做出同等贡献。

参考文献：

[1] 陈寰琦，周念利 . 从 USMCA 看美国数字贸易规则核心诉求及与中国的分歧 [J]. 国际经贸探索，2019,(6).
[2] 陈咏梅，张姣 . 跨境数据流动国际规制新发展：困境与前路 [J]. 上海对外经贸大学学报，2017,(6).
[3] 洪延青 . 美国快速通过 CLOUD 法案 明确数据主权战略 [J]. 中国信息安全，2018,(4).
[4] 王利明 . 论个人信息权在人格法中的地位 [J]. 苏州大学学报，2012,(6).
[5] 王亮 . 中国自由贸易协定电子商务条款研究 [J]. 河南财政税务高等专科学校学报，2016,(4).
[6] 王蕊 . TPP 电子商务规则对中国的影响及启示 [J]. 国际经济合作，2016, (2).
[7] [美] 约瑟夫·E·斯蒂格利茨 . 不平等的代价 [M]. 张子源译 . 北京：机械工业出版社，2013.
[8] Avril, D. Haines. Why Is It So Difficult to Construct an International Legal Framework for E-commerce? The Draft Hague Convention on Jurisdiction and the Recognition and Enforcement of Foreign Judgments in Civil

① Appellate Body Report, European Communities-Measures Prohibiting the Importation and Marketing of Seal Products (hereinafter EC-Seal Products), WT/DS400/AB/R, WT/DS401/AB/R, 18 June 2014, para. 5.210.

② Panel Report, Colombia-Measures Relating to the Importation of Textiles, Apparel and Footwear (hereinafter Colombia-Textiles), WT/DS461/AB/R, 27 Nov. 2015, para. 7.304. Panel Report, Argentina-Measures Relating to Trade in Goods and Services (hereinafter Argentina-Financial Services), WT/DS453/AB/R9, May 2016, para. 7.684.

and Commercial Matters: A Case Study[J]. European Business Organization Law Review, 2002, 3(1).

[9] Jane, Kelsey. How a TPP-Style E-commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)[J]. Journal of International Economic Law, 2018, 21(2).

[10] John, Selby. Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?[J]. International Journal of Law and Information Technology, 2017, 25(3).

[11] Mira, Burri. New Legal Design for Digital Commerce in Free Trade Agreements[J]. Digiworld Economic Journal, 2017, 107(3).

[12] Mishra, N. Data Localization Laws in a Digital World: Data Protection or Data Protectionism? [J]. Journal of Public Policy, 2016, 19(5).

[13] Peng, Shin-yi, Liu, Han-wei. The Legality of Data Residency Requirements: How Can the Trans Pacific Partnership Help? [J]. Journal of World Trade, 2017, 51(2).

On Legal Issues of Data Localization and Exceptions in RTAs

ZHENG Lingli

Abstract: Data Localization and privacy protection of cross-border e-commerce are emerging and unresolved issues nowadays in the field of international trade law. Although the two cases, Schrems I and Schrems II as well as United States v. Microsoft Corp., did not directly create data localization regulations, they highlighted the irreconcilably different approaches of US and EU to data privacy, and eliminated effective solutions for cross-border data transfer, thus made data localization the only remaining elastic one. While the future of WTO e-commerce negotiation is unclear, the new RTAs represented by CPTPP e-commerce rules and USMCA Digital Trade rules prohibit Data Localization and forced disclosure of source code, which has potential to form a model of global cross-border E-commerce rules. Cross-border data flows and data localization measures should be effectively regulated based on data types effectively, while legal public policy exceptions being defined in the future model regional E-commerce norms. This is significant regional modernization of rule of law to bridge the fragmentation of cross-border E-commerce rules.

Keywords: CPTPP; USMCA; cross-border e-commerce; data localization; public policy

（责任编辑：金孝柏）