数据竞争的美欧战略立场及中国因应

——基于国内立法与经贸协定谈判双重视角

洪延青*

摘　要：数据的国家间竞争态势日益形成。美国事实上已经将自己的企业打造成了美国在网络空间的国家利益的载体，其数据安全和治理方面的法律和政策工具随着美国企业走向全球，促成美国企业尽可能地掌握和控制全球数据。欧盟则沿着数字单一市场和技术主权两条主线，为欧洲企业消除了在区域内数据获取和控制的壁垒，极大地抬高了外国企业在其境内运营的门槛，并通过域外管辖和数据跨境流动管控实现其数据治理秩序向境外“投射”以促进其企业全球化运作，进而更多地掌握和控制全球数据。在世界贸易组织电子商务规则谈判中，美国和欧盟各自提出了提案以固化其国内形成的数据安全和治理秩序。当下中国通过的立法更多的是设立了数据安全和治理的框架、流程、工具，缺乏对数据竞争的实质性立场，进而导致经贸协定谈判中中国方案的“隐而难发”。中国需要尽快扭转这一局面，为中国企业参与全球竞争提供规则基础。

关键词：数据掌握　数据控制　国家间竞争　经贸协定谈判　内外统筹

一　问题的提出

《外交事务》杂志在2021年第3期发表了一篇广为传播的文章——《数据即权力》（Data is Power）。两位作者直言：

> 与全球经济的其他要素相比，数据与权力更紧密地交织在一起。作为创新的一个日益必要的投入，国际贸易的一个迅速扩大的元素，企业成功的一个重要因素，以及国家安全的一个重要层面，数据为所有拥有它的人提供了难以置信的优势。它也很容易被滥用。寻求反竞争优势（anticompetitive advantages）的国家和公司试图控制数据。那些希望破坏自由和隐私的人也是如此。①

*　北京理工大学法学院教授。本文所用网络文献的最后访问时间均为2021年11月5日。

① Matthew J. Slaughter and David H. McCormick, “Data Is Power”, (2021) 100 (3) *Foreign Affairs* 54, pp. 54 – 62.

这段话清晰、全面地勾勒出数据对于国家间竞争至关重要的意义。显然，数据资源要素的获取将极大促进数字经济发展，这已经成为世界各国的共识。

随后，两位作者从自己的视角概述了欧盟和中国在数字经济领域的政策和措施，特别是中国的各种“数据本地化”要求、5G 网络产业政策、中国标准 2035、数字丝绸之路等，得出了一个结论：“中国对数字时代有一个愿景，美国则没有。”两位作者还指出，对于数据，

> 华盛顿的许多讨论过于狭窄，只涉及隐私、反垄断问题和法律责任。这些都是至关重要的问题。然而，要牢记数据的巨大经济潜力——不仅仅是在美国产生的数据。由于数据是非竞争性的，那些不能获取和使用数据的国家将有重大的潜在损失。①

因此，涉及数据跨境流动的政策和法律的方方面面，很大程度上决定了一个国家获取和使用数据的能力。本文将一个国家在国内法层面对数据跨境流动的管控②与其所参与的国际经贸协定对数据跨境流动的规范联动而形成的一国对数据资源要素的占有，称为国家的数据竞争战略。

在笔者看来，《数据即权力》一文的两位作者实际上极大地低估了，或者是选择性地忽略了美国在涉数据跨境流动方面的法律和政策客观形成的对数据的掌握和控制效果。美国根据自身产业界的技术水平和全球运营的状况，通过推动区域性数据流动框架和《云法》（Cloud Act）打造了数据“宽进严出”的阀门，并在国际经贸协定谈判中极力维护或植入对其产业界有利的规则。至于大西洋彼岸的欧盟，其坚定地沿着“数字单一市场”战略，通过创设各种法律工具打破各成员国之间数据流动的壁垒，筑高数据流出欧盟的门槛，并通过“长臂管辖”实现欧盟外企业自愿或非自愿地将数据带回欧盟境内。同样，欧盟也在国际经贸协定谈判中争取符合自身利益的规则。

反观中国，2017 年生效的《网络安全法》、2021 年 9 月生效的《数据安全法》，以及 2021 年 11 月生效的《个人信息保护法》在增强中国对全球数据掌握和控制的效果方面不甚清晰。与此同时，中国正在参与世界贸易组织（以下简称 WTO）电子商务规则的谈判，③ 中国数据竞争战略的不清晰实际上已经直接导致了中国在国际经贸协定谈判中对于数据跨境流动和本地化的立场“隐而难发”。④ 此外，中国已于 2021 年 9 月正式提出申请加入《全面与进步跨太平洋伙伴关系协定》（以下简称 CPTPP），⑤ 但海外媒体智库普遍认为中国需要通过修法的方式“放松”国内数据跨境流动管控才能符合 CPTPP 的规定。⑥ 因此在未来谈判过程中，如何利用 CPTPP 中的不符

---

① Matthew J. Slaughter and David H. McCormick. “Data Is Power”, pp. 54 – 62.

② 数据本地化或者说数据跨境流动规则，是数据治理国内立法与国际规则最主要的交叉点。相关数据显示，截至 2017 年 10 月，全球 64 个主要经济体中，对数据跨境流动施加限制的国家接近 90%。See Martina F. Ferracane, Restrictions on Cross-Border Data Flows: A Taxonomy, *ECIPE Working Paper*, No. 1, 2017, pp. 1 – 2.

③ 《商务部：中国已提交首轮 WTO 电子商务谈判提案》，新浪网，https://k.sina.cn/article_ 3164957712_ bca56c1002000rr8q.html? from = news&subch = onews。

④ 披露出来的电子商务谈判合并文本与数据跨境流动相关的条款中没有中国提供的条文。详细分析见下文。

⑤ 《中方正式提出申请加入〈全面与进步跨太平洋伙伴关系协定〉（CPTPP）》，商务部网站，http://www.mofcom.gov.cn/article/news/202109/20210903199707.shtml。

⑥ See China's CPTPP push a gambit to break Asia-Pacific solidarity, https://asia.nikkei.com/Spotlight/Comment/China – s – CPTPP – push – a – gambit – to – break – Asia – Pacific – solidarity; A Chinese vision of free trade, https://www.economist.com/china/2021/10/07/a – chinese – vision – of – free – trade.

措施和例外措施、是否需要国内修法、对哪些国内法在多大程度上进行修订等关键问题，都需要从国家数据竞争的角度来考虑。

为此，本文呼吁采取一个关于数据跨境流动乃至国家间数据竞争的综合性视角。这样的视角不仅能够有效指导国内进一步立法的方向和策略，而且对于国际经贸协定谈判应采取的立场和方针的确定，也有重大意义。但不无遗憾的是，我国既有的关于数据跨境流动的研究主要关注单一方面的局面。例如，有些学者关注域外执法司法领域数据跨境调取与我国立场之间的冲突；[①] 有些学者关注各国内部对数据跨境流动的规制要求及相互之间形成的博弈和互动；[②] 还有些学者从国际经贸谈判的角度研究数据跨境流动问题。[③] 从国家间数据竞争角度观察，需要综合地看待国内和国际联动，才能相对完整地勾勒出数据跨境流动背后的政治经济学。有鉴于此，本文沿着上述思路尝试对全球数字经济最重要的三个主体——美国、欧盟和中国做出分析，勾勒其各自的数据竞争战略，并最终落脚到三个国家和地区目前正在开展的 WTO 电子商务谈判中相关条款与其竞争战略的耦合程度。由于 WTO 谈判处于各国提出各自方案的阶段，并没有形成统一案文，而 CPTPP 条文则已经形成且中国已经开始对其进行评估，因此，本文还将以 CPTPP 相关条文作为分析基线，剖析美国和欧盟在 WTO 谈判中最新案文所展现出的立场与 CPTPP 协定中相关条款的“偏离程度”，以及中国目前国内立法和政策与 CPTPP 条款可能存在的差距。这样的分析有利于厘清中国在国际经贸谈判中面临的形势和压力，同时也是呼吁中国尽快确定自己的数据竞争战略以便能像美欧那样“统筹国内国外”。

二　国内法筹划：美欧数据竞争的战略框架

（一）美国的数据竞争战略框架

从业务层面的数据跨境流动来说，美国一直推行亚太经济合作组织（以下简称 APEC）项下的《跨境隐私规则体系》（Cross Border Privacy Rules，以下简称 CBPRs）。从 2011 年以来，美国成功地将其重要盟友（墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、中国台北、菲律宾等 8 个经济体）纳入该体系，并在 2020 年 8 月首次提出将该体系“从 APEC 框架独立出来”，以在更大的范围内吸引更多的国家和地区加入。[④] 这套制度的实质是通过提供较低保护水平的数据跨境流动机制，“削弱”加入其中的国家或地区按照自主意愿管控数据跨境的权力，然后借由美国

① 例如，洪延青：《“法律战”旋涡中的执法跨境调取数据：以美国、欧盟和中国为例》，载《环球法律评论》2021 年第 1 期；唐彬彬：《跨境电子数据取证规则的反思与重构》，载《法学家》2020 年第 4 期；裴炜：《向网络信息业者取证：跨境数据侦查新模式的源起、障碍与建构》，载《河北法学》2021 年第 4 期。

② 例如，吴玄：《数据主权视野下个人信息跨境规则的建构》，载《清华法学》2021 年第 3 期；黄志雄、韦欣妤：《美欧跨境数据流动规则博弈及中国因应——以〈隐私盾协议〉无效判决为视角》，载《同济大学学报（社会科学版）》2021 年第 2 期；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》，载《中国法律评论》2021 年第 2 期。

③ 例如，张倩雯：《数据跨境流动之国际投资协定例外条款的规制》，载《法学》2021 年第 5 期；时业伟：《跨境数据流动中的国际贸易规则：规制、兼容与发展》，载《比较法研究》2020 年第 4 期；张生：《国际投资法制框架下的跨境数据流动：保护、例外和挑战》，载《当代法学》2019 年第 5 期。

④ 《美国提议修改 APEC 数据流通规则》，https：//cn. nikkei. com/politicsaeconomy/politicsasociety/41754 – apec. html。

产业界超强的实力，最终实现数据向美国企业和美国本土的汇聚集中。[①] 一方面，数据一旦为美国公司所掌握，则美国的外国投资委员会（CFIUS）将有权严格审查能够赋予外国组织或个人访问“敏感个人数据”的并购或投资；[②] 另一方面，特朗普当政时期的“清洁网络计划”，拜登政府最新签署的《关于保护美国人的敏感数据不受外国敌对势力侵害的行政命令》[③]，以及美国商务部建立的《确保信息和通信技术及服务（ICTS）供应链安全》暂行最终规则[④]等措施，将“外国敌手”所拥有或控制、或受其管辖或指挥的人所设计、开发、制造或提供的某些联网软件应用程序和设备排除在美国的供应链外，进一步避免了美国数据（包括美国公司所掌握的来自美国境外的数据）的“不当流出”。从为执法和司法目的跨境调取数据来说，美国的法院程序和 2018 年通过的《云法》都在强化对受美国法管辖的实体和个人的数据跨境调取能力。[⑤] 特别是《云法》没有修改原先的《存储通信法》（Stored Communications Act）中禁止受美国法管辖的实体和个人向境外政府提供关于通信内容数据的规定，而是进一步利用该规定，确立了与美国政府签署了协定的“适格国家”才能够直接向美国的公司调取数据。

上述法律和政策方面的“组合拳”客观上达成的效果有三。一是掌握。对数据（低保护水平）自由流动的倡导，使得美国企业能够在业务层面尽可能多和便利地掌握全球数据，并可以将其“带回”美国总部（或者美国公司自主选择的地点）进行分析。二是排除。美国排除了“外国敌手”的信息技术产品通过参与美国企业业务运营而掌握数据的可能性，并严格审查和限制外国的个人或公司通过并购和投资获得美国数据的行为。三是调取和限制。只要是美国公司所控制（control）、拥有（possess）、保管（custody）的数据，无论是否存储在美国境内，都受美国司法和执法程序的管辖，只要有现实需求就应当向美国当局提供；而外国政府如果需要向美国公司调取较为敏感的内容数据，只能通过美国政府的司法协助或者成为《云法》项下的“适格国家”。

通过上述三方面的举动，美国事实上已经将自己的企业打造成了美国在网络空间的国家利益的载体，适用于数据的法律和政策工具随着美国企业走向全球，最终实现了其整体的数据战略——尽可能地掌握和控制全球数据。

（二）欧盟的数据竞争战略框架

欧盟围绕着“数字单一市场”和“技术主权”两条主线打造适用于数据的法律和政策工具。“数字单一市场”的目的是将欧盟各个成员国整合成一个不存在贸易壁垒的统一市场。[⑥] “技术主权”则是“欧洲必须具有的能力，即必须根据自己的价值观并遵守自己的规则来做出自己的选择”。[⑦]

沿着这两条主线，就欧盟内部市场来说，《通用数据保护条例》（以下简称 GDPR）开宗明

---

① 相关分析参见洪延青：《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》。

② 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》。

③ See “Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries”, THE WHITE HOUSE website, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.

④ See “The Interim Final Rule on ‘Securing the Information and Communications Technology and Services Supply Chain’”, https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf.

⑤ 相关分析参见洪延青：《“法律战”旋涡中的执法跨境调取数据：以美国、欧盟和中国为例》。

⑥ See “Shaping Europe's digital future”, European Commission website, https://ec.europa.eu/digital-single-market/en.

⑦ See “Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission”, European Commission website, https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260.

义，在第1条就明确“该条例规定了有关在处理个人数据方面保护自然人的规则和有关个人数据自由流动的规则”，以及“个人数据在联盟内的自由流动不应由于与保护自然人的个人数据处理有关的原因而受到限制或禁止”。[①] 欧盟的《非个人数据自由流动条例》（The Regulation on the Free Flow of Non-personal Data）同样指出，“该条例旨在通过制定与数据本地化要求、向主管部门提供数据以及为专业用户移植数据有关的规则，确保除个人数据外的数据在联盟内自由流动。”[②] 在通过两部条例打通了个人数据和非个人数据在欧盟内的自由流动后，欧盟在2020年2月发布的《欧洲数据战略》[③] 中提出，“本战略所列的措施致力于构建数据经济的综合性方法，旨在提升整个欧盟单一市场对于数据、数据赋能产品和服务的使用和需求。”该战略最核心的举措是建立“单一欧洲数据空间”（a single European data space）。

在2021年，欧盟规划的数据相关立法的草案，例如旨在激励各方数据共享的《数据法案》，以及针对科技巨头收集、使用、共享数据中限制创新和竞争问题的《数字市场法案》等相继问世。综合来看，欧盟在其境内打造了具有欧洲价值观特色的数据自由流动秩序。

除了着力于境内，欧盟还积极将自身的影响力延展至其境外。GDPR宽泛的域外管辖规定即是一例：其不仅扩大了受其管辖的数据控制者范围，[④] 还扩大了数据控制者这个概念本身。[⑤] 这样的思路均被欧盟后续的立法和欧盟境内的司法判例所继承。[⑥]

对于数据从欧盟境内传输至不受GDPR管辖的实体或个人这样的情形来说，欧盟的法律和政策很难用自由来形容。首先，GDPR要求的是确保在数据跨境传输的情形中，其所提供的个人数据保护水平“不会减损”（not undermined）。在美欧《安全港协议》被推翻时，欧盟法院（CJEU）将其解释为数据接收者所在的国家或地区，或者数据接收组织提供的保护水平应当与GDPR的要求“实质等同”（essentially equivalent）。由于欧盟将个人数据保护作为一项基本人权，因此不仅商用场景下的保护非常重要，限制数据接收者所在的国家或地区的公权力部门从接收者调取数据更是至关重要。也正是基于这个原因，无论是美欧之间的《安全港协议》还是《隐私盾协议》，欧盟法院都始终认为美国国内法对公权力调取数据的限制与欧盟类似的法律限制不匹配，上述两个协议对公权力的限制不足，因此无法提供“实质等同”的保护水平。[⑦] 在严苛的判例指引下，欧盟委员会更新了标准格式合同条款（SCCs），强化了数据接收者对抗公权力数据调取行为的义务。[⑧] 欧洲数据

① See “Art. 1 GDPR Subject-matter and objectives”, intersoft consulting website, https://gdpr-info.eu/art-1-gdpr/.

② See “Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.)”, Eur-Lex website, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.

③ See “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data”, Eur-Lex website, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

④ GDPR第3条规定，对在欧盟境内没有设立机构的数据控制者或数据处理者，只要其面向欧盟境内的数据主体提供商品或服务（无论是否发生支付行为），或监控欧盟境内数据主体的行为，就要接受GDPR的管辖。

⑤ GDPR第3条规定，只要数据处理发生在欧盟境内的机构的业务场景之中，无论数据处理是否实际在欧盟境内发生，均受GDPR管辖。

⑥ 见GDPR第3条规定。

⑦ 相关分析参见洪延青：《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》。

⑧ “Standard contractual clauses for international transfers”, European Commission website, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

保护委员会（EDPB）更新了《为确保遵守欧盟个人数据保护水平的数据转移补充工具的建议》，进一步将欧盟法院“实质等同”的逻辑在新版标准格式合同条款的基础上演绎落地。[①] 对于目前最为安全的数据跨境流动工具——“充分性认定”来说，欧盟的战略更为直白。欧盟委员会在 2017 年的通信中明确：应当让全世界的个人数据保护水平向欧盟看齐，最好的工具就是“充分性认定”；但具体和哪些国家和地区开展充分性认定的谈判，除数据保护和经贸水平方面的考虑外，还应当考量“特定国家与欧盟的政治关系，特别是是否秉持共同的价值和目标”。[②] 顺着上述思路，欧盟在亚太地区率先和日本、韩国达成了充分性认定的协议，将这两个国家纳入自己打造的数据跨境流动秩序之中。

欧盟采取了类似 CFIUS 的做法，其制定的《关于建立欧盟外国直接投资审查框架的条例》于 2020 年 10 月生效。该条例第 4 条列举了判断外国直接投资何时可能影响安全或公共秩序的考量因素，其中就包含“获取或控制包括个人数据在内的敏感信息的能力”。[③]

在执法和司法方面的数据跨境调取，欧盟同样效仿美国的《云法》，于 2018 年启动了《关于刑事犯罪电子证据的调取令和保全令的规定》的立法工作，[④] 同样要求所有面向欧盟市场的服务提供者均应当配合执法机构的数据调取命令，无论数据是否存储于欧盟境内。

欧盟很清楚自身面向消费者（以下简称 2C）的产业实力远落后于美国和中国，但其始终对自身面向企业（2B）的产业实力充满信心。总结起来，欧盟在数据方面的法律和政策“组合拳”，为欧洲企业消除了欧盟区域内数据获取和控制的壁垒，极大地抬高了外国 2C 企业在其境内运营的门槛。欧盟通过域外管辖，极力将在境内打造的数据治理秩序投射到欧盟境外；对于投射不到的情况，欧盟设定了极其苛刻的数据跨境流动条件，并事实上形成了将数据留在欧盟境内的局面，且仅仅非常有选择性地向少部分国家和地区开放了数据流动。[⑤] 与此同时，投资审查方面的规定能够很大程度上保障个人数据始终为欧洲企业所控制。类似《云法》的跨境调取数据的法案保障了司法和执法需求。总的来说，欧盟按照自身的产业情况打造了数据治理秩序，并尽可能地将更多的国家或地区纳入该区域之中，试图在最大范围内拉平企业竞争的基线，促进其企业全球化运作。

三　国际法策略：美欧在国际经贸协定谈判中的数据竞争立场

2020 年底，WTO 电子商务谈判的合并文本在网上被公开。[⑥] 文本中详细表明了各个成员所

① “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, European Data Protection Board website, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

② “Exchanging and Protecting Personal Data in a globalised World”, European Economic and Social Committee website, https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/exchanging-and-protecting-personal-data-globalised-world.

③ “Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union”, EUR-Lex Website, https://eur-lex.europa.eu/eli/reg/2019/452/oj.

④ “E-evidence - cross-border access to electronic evidence”, European Commission Website, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

⑤ 笔者认为，充分性认定也是其影响力投射的实现路径之一。

⑥ “WTO Electronic Commerce Negotiations Consolidated Negotiating Text - December 2020”, https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf.

提出的条文方案。数据跨境流动条款被命名为信息流动（flow of information），并放置于第 B 节“开放度和电子商务”（openness and electronic commerce）之中。本部分将首先分析 CPTPP 电子商务章节中关于数据跨境流动的条款，并以此为基线，分析美国和欧盟在 WTO 谈判中的立场演进，以及其立场与前文勾勒的其数据战略的耦合程度。

（一）分析基线：CPTPP 数据跨境条款

CPTPP 中与数据跨境相关的条款主要出现在第 14 章电子商务章节，即第 14.11 条“通过电子方式跨境传输信息”[①] 和第 14.13 条“计算设施的位置”[②]。总的来说，这两条的结构类似，核心关键词为“合法公共政策目标”“任意或不合理歧视的方式”“对贸易构成变相限制”“超出实现目标所必需的限制”。

首先，CPTPP 并未对“合法公共政策目标”做出限定，一般认为信息安全、个人信息保护、确保监管机构方便地访问和调取数据等各国常见的用来正当化数据本地化和跨境流动管制的目的，[③] 都可以认为是“合法公共政策目标”。

其次，即便是为了“合法公共政策目标”而采取的措施，也应符合两个条件。CPTPP 第 14.11 条的（a）项和（b）项中间所用的“及”（and）这一词，表明这两项条件应同时具备，而非“二选一”的关系。具体而言，这里的（a）项规定针对的是措施的适用方式，类似于 GATT 第 20 条和 GATS 第 14 条的前言性规定（chapeau），偏重于对措施在适用程序性方面的要求；（b）项则偏重于对措施的实体性要求，即所采取的措施是必需的，且符合比例性要求。[④]

（二）美国在国际经贸协定谈判中的数据竞争立场

在合并谈判文本中，美国提出的条文基本上和 CPTPP 的第 14.11 条保持了一致，但新增了一个条款：“一项措施不满足第五段[⑤]规定的情形，如果该措施仅仅因为数据是跨境传输，就对

---

① CPTPP 第 14.11 条规定：
1. 各缔约方认识到每一缔约方对于通过电子方式跨境传输信息可能有各自的监管要求。
2. 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. 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 条规定：
1. 各缔约方认识到每一缔约方对于计算设施的使用可能有各自的监管要求，包括寻求保证通信安全和保密的要求。
2. 缔约方不得将要求涵盖的人使用该缔约方领土内的计算设施或将设施置于其领土之内作为在其领土内从事经营的条件。
3. 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 对各国数据跨境流动管理制度的比较分析可参见洪延青：《在发展与安全的平衡中构建数据跨境流动安全评估框架》，载《信息安全与通信保密》2017 年第 2 期。

④ 根据 WTO 关于一般例外的法理，判断一项措施是否必要，在实践中将重在考察措施的设计（design）、措施的目标（the objectives）、措施对于目标实现的贡献（contribution）以及是否有可比的替代措施（alternative measures），或尽管有替代措施，但其并不具有可行性（unavailability）。CPTPP 要求（a）项和（b）规定须同时满足，其实是 GATT/WTO 例外法理中两步测试法（two-tier test）的体现，既注重对措施的实体考察，也关注对措施的适用要求。

⑤ 其中合并谈判文本中的第五段，即是 CPTPP 第 14.11 中的第三段内容。

该传输给予区别对待，从而改变了竞争条件，损害了另一缔约方的服务提供者。”[①] 加上了这样的一个语句，实际上表明美国在 WTO 谈判中的立场与其签订的《美国—墨西哥—加拿大协定》（以下简称 USMCA）第 19.11 条[②]完全相同。以下对该新增语句进行分析。

首先，从字面上理解，假设某类数据传输不出境，某国国内的法律法规没有管制的话，则这类数据传输如果涉及出境，而法律法规做出了区别对待，就满足了该句所谓的“仅仅因为数据是跨境传输”。其次，“给予区别对待，从而改变了竞争条件，损害了另一缔约方的服务提供者”，其强调的是竞争条件的恶化。WTO 法理关注实质效果，并非法律法规对国内外企业形式上“一视同仁”就可以认定国内外企业享受同等待遇。WTO 要求即便是相同的法律法规，如果实际上对外国企业造成竞争上的不利影响，那么该法律法规就是造成了“较低待遇”（less favorable treatment）。因为一旦仅因数据跨境就做出管控，几乎肯定会对外国企业在市场竞争方面造成更加不利的影响。外国企业在成员国运营，肯定会涉及数据跨境传输，因此外国企业在此方面无论是经营空间或者成本花销方面，必然会与纯粹在国内运营的企业相比成本更高。以上的理解基于对“待遇”一词做形式化的理解，即与国内数据传输相比，对数据跨境传输另有规定。

如果对“待遇”一词作实质性理解，以上结论同样成立，即：数据跨境传输所要求的保护水平不应该比国内数据传输所要求的保护水平（包括安全保护措施等）更高。换言之，一国政府不得因为数据跨境，而要求比同类型数据境内传输更高的保护水平或者其他方面更重的义务。[③]

不难看出，美国立场中增加了这一新的段落，目的是将数据跨境流动和数据境内流动“等量齐观”，各国不应当仅仅因为数据是跨境传输就采取“歧视性”措施。无疑这样的条文设计与前文所述的美国数据竞争战略非常符合。另一个突出体现其战略意图的条文设计出现在合并谈判文本的个人信息保护条款。[④] 该条设计的思路与其主导的《跨太平洋伙伴关系协定》（以下简称 TPP）谈判文本[⑤]完全一致。首先，TPP 第 14 章第 11 条“以电子方式跨境传输信息”要求各签署国应当允许个人信息的自由跨境流动，除非是出于“正当的公共政策目标”。保护个人信息显然属于“正当的公共政策目标”。而 TPP 第 14 章第 8 条“个人信息保护”表面上是说，保护个人信息对于电子商务开展十分重要，各签署国有义务对个人信息开展保护。但实际上的效果是说，各签署国保护的方式、方法、水平肯定是不一致的，但是只要满足一定的“较低标准”，那就算做到了对个人信息的保护。为什么说是“较低标准”？原因在于，该章节的注释 6 指出：“为进一步明确，一国可通过以下方式履行该段所规定的义务：采用或保持诸如一部统一的隐

① “A measure does not meet the conditions of paragraph 5 if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of [a covered person/service suppliers] of another [Party/Member].”

② “Chapter 19 Digital Trade”, USMCA, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

③ 如果对“待遇”采形式性理解，则欧盟立场与条文要求相冲突。在欧盟、中国或者有数据跨境管控的国家和地区，恰恰是因为数据跨境传输而增加了部分监管要求。因为数据出境，涉及适用的法律发生变化，例如数据接收方要适用其他国家的法律，而且数据在其他国家落地后，也将受到该国家法律的管辖。如果采取实质性的方式理解“待遇”，目前欧盟（包括其他大部分对个人数据跨境传输做出专章规定的国家和地区）本质上仅要求个人数据跨境时和在国内受到“实质相同”（essential equivalent）的保护，因此其能够接受该条文。

④ 参见合并谈判文本的第 C.2 条：隐私。

⑤ CPTPP 电子商务章节的条款与 TPP 完全一致。

私、个人信息、个人数据保护法律，特定部门或行业的隐私保护法律，或能够监督企业自愿开展与隐私相关举措的法律。”换言之，通过该注释，各签署国获得了采取各自偏好的方式来保护个人信息的空间。例如美国，就不需要像韩国、日本那样需要设立高水平的“统一性的个人信息保护立法”，同时也可以对其他 TPP 签署国声称，其本国法律已经做到了对个人信息的保护了。与此同时，既然美国法律已经做到了对个人信息的保护，那么各签署国就不应该再出于保护个人信息的事由，限制个人信息流向美国，否则就属于第 11 条所说的“非必要措施”。也就是说，正是通过建立在低水平保护的 CBPRs 体系，或者通过 TPP 促使各签署国承认并认同美国法律对个人信息的保护水平。美国努力实现其战略利益——促进个人信息自由地跨境流动，更准确地说，向美国聚拢。

现在，美国把 TPP/CPTPP 的这个关键注释平移到了 WTO 的合并谈判文本之中，实际上意图巩固符合其利益的 CBPRs 制度。同样，USMCA 数字贸易章节的第 8 条也明确承认 CBPRs 体系为签署国认可的有效的数据跨境流动制度。

（三）欧盟在国际经贸协定谈判中的数据竞争立场

从 WTO 合并谈判文本来看，欧盟的条文分两段，本文以条文 A 和条文 B 来指代。其中，条文 A 主要规定了数据（包括各种类型的数据，其中包含个人数据）跨境流动。条文 B 主要是在 A 的基础上，就个人数据做出专门的规定。

首先看条文 A。条文 A 要求：各国政府不应限制数据跨境流动，其中包括 4 个具体方面：（1）不得要求使用一方境内的计算设备或网络元件（network elements）进行数据处理，包括要求使用经在一方境内认证或批准的计算设备或网络元件；（2）不得要求数据在一方境内进行本地化存储或处理；（3）不得禁止在他方境内进行数据存储或处理；（4）不得把使用一方境内的计算设备或网络元件，或者事先满足一方境内的本地化要求，作为数据跨境流动的前提条件。因此，条文 A 主要起到禁止数据本地化的作用。

再来看条文 B。条文 B 主要针对个人数据，因此本质上是在条文 A 的基础上，就个人数据“开辟”出一个例外，以符合 GDPR 的规定。条文 B 规定：（1）各方认可，个人数据和隐私获得保护是一项基本权利，在这一方面设立较高标准有助于数字经济中的互信和贸易的发展；（2）各方均可采取并维持其认为适当的保障措施，包括通过和实施个人数据跨境传输规则，以确保对个人数据和隐私的保护。本协定中的任何内容均不影响各方的保障措施对个人数据和隐私提供的保护。

从条文 B 来看，事实上达到的效果就是欧盟（包括其他接受该条款的签署国）可以为保护个人数据和隐私，采取各自认为恰当的政策、立法、措施等，包括对个人数据的跨境流动进行专门的监管。而这样的监管措施，可以包含数据（和设施）的本地化规定。

与 CPTPP 的条文相比，欧盟两个条文提出了更高的要求。一是因为欧盟条款比 CPTPP 更加彻底地禁止数据本地化要求。CPTPP 允许基于正当公共利益理由提出本地化的要求，但欧盟的条文 A 已经不允许正当公共利益这个事由，仅允许国家安全作为安全例外提出本地化要求。二是因为欧盟条款比 CPTPP 更加支持数据跨境流动。表面上，欧盟条文 B 对个人数据和隐私保护给予了更大空间，主权国家可以采取任何自己认为适当的措施。但是与 CPTPP 条款相比，主权国家只能针对个人数据和隐私保护这个原因对数据跨境流动提出限制，而非 CPTPP 原来允许的

“正当公共政策目标”，相当于更加限缩了主权国家限制数据跨境流动的政策空间。就数据本地化和数据跨境流动来说，欧盟两个条款比 CPTPP 要求更高。而实际上，欧盟方面的条文来自于欧盟官方渠道公开发布的条文范本。欧盟委员会也宣称将以此条文为基础，开展与印尼、日本等国家的贸易协定谈判。①

综合来看，欧盟的两个条文非常契合其数据竞争战略。条文 A 保障数据特别是非个人数据的自由流动。条文 B 则确保其数字单一市场和技术主权，以及相应的配套立法（如 GDPR）的运作空间。

四　双重因应：中国的数据竞争战略与国际联动立场

（一）国内法层面

对于数据跨境流动来说，中国主要的法律框架由《网络安全法》② 《数据安全法》，以及《个人信息保护法》③ 所组成。以 2021 年 9 月 1 日生效的《数据安全法》为例，其在具体制度层面通过重要数据出境安全评估、数据安全国家审查、数据出口管制、跨境执法调取数据的阻断立法等方面，实现对数据跨境流动的全面控制。因此，从制度广度而言，《数据安全法》对数据跨境监管完成了全场景覆盖：一般商业场景中遵循数据出境安全评估制度，特殊商业场景中遵循数据跨境执行出口管制、国家安全审查规则；应境外执法机构要求提供数据须履行境内主管机关批准程序。如此的制度设计看似完备，但细究起来更多的是设立了框架、流程、工具，缺乏对数据跨境流动的方向性的态度或立场。④

首先，从经贸业务场景中数据跨境流动的法律条文来看。国家网信部门是数据跨境流动方面的主要责任部门。《网络安全法》要求其制定关键信息基础设施（以下简称 CIIO）“在中华人民共和国境内运营中收集和产生的个人信息和重要数据的跨境传输”的出境安全评估办法；《数据安全法》要求其制定非 CIIO 的数据处理者“在中华人民共和国境内运营中收集和产生的重要数据”的出境安全管理办法；《个人信息保护法》要求其制定关于个人信息出境的“安全评估办法”“个人信息保护认证规则”“标准合同”，要求其设定必须通过安全评估程序的个人信息处理者的条件（主要是“处理个人信息达到国家网信部门规定数量的个人信息处理者”）。为此，中央网信办曾于 2017 年 4 月就《个人信息和重要数据出境安全评估办法（征求意见稿）》⑤ 公开征求意见，于 2019 年 6 月就《个人信息出境安全评估办法（征求意见稿）》⑥ 公开征求意见。但这两个出境安全评估办法并未最终出台。中央网信办于 2021 年 8 月发布了《汽车

① “EU proposal for provisions on Cross-border data flows and protection of personal data and privacy”, http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf.

② 参见《中华人民共和国网络安全法》第三十七条。

③ 参见《个人信息保护法》第三章：个人信息跨境提供的规则。

④ 类似的观点同样适用于《个人信息保护法》的相关制度设计。

⑤ 《国家互联网信息办公室关于〈个人信息和重要数据出境安全评估办法（征求意见稿）〉公开征求意见的通知》，中国网信网，http://www.cac.gov.cn/2017-04/11/c_1120785691.htm。

⑥ 《国家互联网信息办公室关于〈个人信息出境安全评估办法（征求意见稿）〉公开征求意见的通知》，中国网信网，http://www.cac.gov.cn/2019-06/13/c_1124613618.htm。

数据安全管理若干规定（试行）》。[①] 在这部“若干规定”中，中央网信办对汽车数据中的个人信息和重要数据出境提出了安全评估和备案等要求。其最新举措是于 2021 年 10 月 29 日发布《数据出境安全评估办法（征求意见稿）》[②] 并公开征求意见。该评估办法系统地建立了在中国境内运营所收集和产生的重要数据和个人信息在向境外提供时应当遵循的出境安全评估的触发条件、评估要点和流程等。但总的来说，这些部门规章或规范性文件的主要内容，依旧是建立框架、流程、工具，缺乏实质性的政策立场和态度的表达和阐释。反观美国和欧盟，此方面的战略意图在立法中直接凸显：或者借助于全球运营的企业，或者借助于不容忽视的内部市场，极大地增强了国家对（境内外）数据的掌控和利用能力。

其次，从以执法或司法为目的的数据跨境调取的法律条文来看，无论是 2018 年的《国际刑事司法协助法》，还是《个人信息保护法》和《数据安全法》，中国都鲜明地坚持主权不可侵犯的原则。三部法律的相关条款措辞基本一致，均要求“非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据”。该项要求是对美国《云法》和欧盟《关于刑事犯罪电子证据的调取令和保全令的规定》的明确回应。

从两方面综合来看，中国目前关于数据跨境的法律表达具有浓重的应对性意味：在执法和司法方面明确表达了对绕过司法协助而直接跨境调取数据的反对；在经贸业务层面则“全面铺设”控制数据跨境流动的“闸口”，但其“疏密松严”尚未确定。

（二）国际协定层面

在 WTO 电子商务谈判合并文本与数据跨境流动相关的条款中没有中国提供的条文。中国的立场则可以以其新近签署的《区域全面经济伙伴关系协定》（以下简称 RCEP）为分析样本。RCEP 第 12 章为电子商务，其第 15 条为“通过电子方式跨境传输信息”。与 TPP/CPTPP 相比，RCEP 吸纳了其大多数内容，但有两个显著变化。一是注释 14 中的“就本项而言，缔约方确认实施此类合法公共政策的必要性应当由实施的缔约方决定”。换句话说，新增的这个注释赋予了缔约方自主决定何为“合法公共政策”的权能，因此相比于 CPTPP/TPP，RCEP 更加尊重各个缔约方的规制自由。二是新增了“该缔约方认为对保护其基本安全利益所必需的任何措施。其他缔约方不得对此类措施提出异议”。这一条款相当于在“合法公共政策目标”例外之外，另外开辟了“基本安全利益”（essential security interests）的例外。此外，RCEP 也明确该条款不受第 19 章规定的争端解决机制的管辖。可以看出，RCEP 条款最显著的特点是给各个缔约方留足了规制空间。

RCEP 条文中较为“宽松”的纪律反过来表明，中国国内尚未对国家数据竞争提出整体的战略和立场。对于经贸业务项下的数据跨境流动，单从国内法律框架本身来看“可左可右”，因此中国负责国际经贸协定谈判的部门仅能通过在条文中留足“宽松度”，为将来战略的制定和执行开辟足够的“空间”。

---

① 《国家互联网信息办公室等五部门发布〈汽车数据安全管理若干规定（试行）〉》，中国网信网，http：//www.cac.gov.cn/2021－08/20/c_ 1631049984834616.htm。

② 《国家互联网信息办公室关于〈数据出境安全评估办法（征求意见稿）〉公开征求意见的通知》，中国网信网，http：//www.cac.gov.cn/2021－10/29/c_ 1637102874600858.htm。

（三）中国数据竞争战略的展望

近期，特斯拉 CEO 马斯克关于数据本地化的表态、[①] 中央网信办就将国外上市带来的数据安全风险纳入网络安全审查征求意见、[②] 工信部就工业和信息化领域的重要数据和核心数据严格出境管理征求意见[③]等，引发外界关于中国将严控数据跨境流动的猜测。与此同时，中国正式申请加入 CPTPP。面对 CPTPP 中自由化纪律要求更高的数据跨境流动和本地化条款，中国政府应当如何处理其与国内政策和实践可能存在的不符，显然是谈判过程中的一个核心事项。此外如前文所述，在 WTO 电子商务谈判中，就数据本地化和跨境流动而言，美国和欧盟已经相对于 TPP/CPTPP 再次“往前走了一步”，可以预计中国在 WTO 电子商务谈判中将持续面临巨大压力。

因此，无论是加入 CPTPP 还是 WTO 电子商务谈判，都已经将国家间数据竞争的压力导入中国。除此之外，既然中国的总体方针是“要拆墙而不要筑墙，要开放而不要隔绝，要融合而不要脱钩”，那么在“推动贸易和投资自由化便利化”过程中，中国也将直面国家间数据竞争的压力。[④]

由是观之，在新一轮全球范围内的数据竞争中，国家不再仅仅承担监督组织开展数据安全工作和保护个人合法利益的角色，更是作为在数据安全和使用方面存在独立利益的主体登场。全球数据治理立法均充分考量国家自身的利益诉求，各国的数据竞争战略都服务于大数据时代的综合国力竞争，既包括维护国家安全利益的防御性诉求，也包括促进本国数字经济全球竞争，并通过规则治理抢占全球数据规则话语权。在欧美各自结合自身特点形成数据竞争战略的前提下，以及竞争压力已经通过多个渠道传导输入的情况下，中国如何提出符合自身安全、发展利益的数据竞争战略，是当下关键所在。这个任务已经迫在眉睫。

而在形成数据竞争战略时，笔者认为应当从两个方面同时着手。一方面，坚持数据主权的基本原则，强调一国对其主权管辖范围内的个人、企业和相关组织所产生的数据拥有的最高权力；另一方面，增强国家（包括其管辖的组织和个人）对（境内外）数据的掌握程度和处理利用能力。目前，中国对于数据的监管着重于第一方面：在面对美欧扩张式的数据竞争时，似乎越来越倾向于采取防守态势。

对于第二方面，笔者建议，在通过《数据安全法》及其配套立法维护中国数据主权的同时，应努力思考如何让中国企业能够在全球范围内掌握、利用更多的数据。当前，中国数字经济虽然取得了举世瞩目的成就，规模和实力仅次于美国，但与美国全球化运营的互联网企业相比，中国众多的网信企业更多的是依赖于日渐饱和的国内市场，而国际化进展却不尽人意。中国数字经济

---

① 9 月 26 日，针对数据安全问题，特斯拉 CEO 马斯克在 2021 年世界互联网大会上再次回应称，“特斯拉车主所有个人身份信息都安全地存储在中国国内，不会转移到海外，只有在采购进口零部件等极少数情况下，部分数据才会在获得相关批准后跨境传输”，以及“所有中国业务所产生的所有数据，包括生产数据、销售数据、服务数据和充电数据等，完全存储在中国境内”。参见《马斯克再谈数据安全：特斯拉中国所有数据都安全存储在中国》，澎湃新闻，https://www.thepaper.cn/newsDetail_forward_14672722。

② 参见《国家互联网信息办公室关于〈网络安全审查办法（修订草案征求意见稿）〉公开征求意见的通知》，中国网信网，http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm。

③ 参见《公开征求对〈工业和信息化领域数据安全管理办法（试行）（征求意见稿）〉的意见》，工信部网站，https://wap.miit.gov.cn/gzcy/yjzj/art/2021/art_dcb6cc8d9f5c414eabd70708719965 25.html。

④ 《习近平出席亚太经合组织领导人非正式会议并发表讲话》，新华网，http://www.xinhuanet.com/politics/leaders/2021-07/16/c_1127663533.htm。

产业仍处于上升期，未来网信企业出海存在广阔空间，而过于强调公权力控制及面向美欧的应对式数据跨境流动监管，事实上将会对中国网信企业出海造成阻碍。正常商业合作中数据流不出去，自然会联动地影响数据流进来，并进而导致中国网信企业无法做到“全球一盘棋”式的运营。为打破这个僵局，一个可行的建议是《数据安全法》乃至《个人信息保护法》等相关法律的后续配套立法，应当在国家统一建立的数据分类分级的基础上，明确每类数据出境所面临的主要安全风险，配以相应的出境管控措施，做到精细化的治理，并定期更新数据的分类分级目录，动态性地应对内外部数据安全风险变化。① 对于低安全风险的数据，应鼓励流动，以此扩张中国企业出海业务；对于中安全风险数据，强调通过合适的管理和技术措施，围绕着有限场景、有限目的、有限对象、有限时间等维度，以支撑中国企业出海业务的扎根和深化；对于高安全风险数据，则可以采取一切必要的措施维护国家的主权和安全利益。

U. S. and European Strategic Positions on Data Competition and the Response of China: From the Perspective of Domestic Legislations and Negotiations of Trade and Investment Agreements

Hong Yanqing

Abstract: Interstate competitive dynamics for data are increasingly taking shape. The United States has *de facto* established its enterprises as the carriers of U. S. national interests in cyberspace, and its legal and policy tools for data security and governance have gone global with U. S. enterprises, enabling them to hold and control as much global data as possible. The EU, on the other hand, has removed barriers to data access and control in the region for European companies along the lines of the digital single market and technological sovereignty, significantly raising the threshold for foreign companies to operate within its borders, and “projecting” its data governance order beyond its borders through extraterritorial jurisdiction and control of cross-border data flows to facilitate the globalization of its companies operations and thus gain greater control over global data. In the World Trade Organization negotiations on e-commerce rules, the United States and the European Union have each proposed provisions to solidify their domestic data security and governance order. The legislations passed by China recently are more about setting up the framework, process, and tools for data security and governance, and lack a substantive position on data competition, which leads to the largely absence of Chinese positions in the negotiations of trade and investment agreements. China needs to reverse this situation as soon as possible and provide a rule base for Chinese enterprises to participate in global competition.

Keywords: Data Mastery, Data Control, Inter-state Competition, Negotiations of Trade and Investment Agreements, Internal and External Integration

（责任编辑：谭观福）

① 详见洪延青：《国家安全视角下的数据分类分级保护》，载《中国法律评论》2021 年第 5 期，第 71—78 页。