

全球数据治理：挑战与应对*

□ 蔡翠红 王远志

〔提 要〕 全球数据治理已成为当前全球治理的重要内容，其主要面临两方面挑战：一是主权国家间在数据权属、数据跨境流动等数据治理议题上的主张相异，并竞相提出了各自的数据发展战略；二是个人、企业与主权国家间数据权益存在失衡，亟需有效机制进行协调。为有效应对这些挑战，推动全球数据治理体系走向有序、规范和协调，一方面，全球数据治理应当采取数据主权、数据保护与数字经济发展相统一的数据治理主张，鼓励各主权国家或区域组织参与全球数据治理并构建全球数据治理规则；另一方面，为协调个人、企业和主权国家之间的数据利益，全球数据治理应当构建数据协调治理机制，具体包括“人格权先行”数据协调治理机制、“财产化市场交易”数据协调治理机制和“匿名化战略利用”数据协调治理机制。

〔关键词〕 全球治理、全球数据治理、数据主权、数据协调治理机制

〔作者简介〕 蔡翠红，复旦大学美国研究中心教授、博导

王远志，复旦大学法学院研究助理

〔中图分类号〕 D81

〔文献标识码〕 A

〔文章编号〕 0452 8832 (2020) 6 期 0038-19

当代社会，全球范围内的数据无处不在，正以无法察觉或不显著的方式

* 本文为国家社会科学基金项目“构建全球互联网治理体系研究”（项目批准号：18BGJ022）的阶段性成果。衷心感谢匿名评审专家和编辑部老师对稿件提出的诸多建设性的修改建议。文中若有任何疏漏和不足皆由笔者承担。

嵌入日常生活结构甚至推动社会变革。^[1] 人们渴望利用数据来解决问题，改善福祉，促进经济繁荣。^[2] 数据逐渐成为当代社会重要的潜在资源之一，数据治理正成为全球治理的重要议题。但综观当前的全球数据治理，其不仅面临主权国家间数据治理不同主张的冲突，还面临个人、企业与主权国家间数据权益失衡等多重挑战。如何应对这些挑战并推动全球数据治理进程向前发展，已是学界和实务界亟待研究的重要问题。

一、全球数据治理的内涵与重要性

随着全球化的推进，治理已逐渐从局部的、领域的市场治理、地方治理、城市治理，走向全面的、综合的政府治理、国家治理；从国内治理走向全球治理。^[3] 作为全球治理的细分治理领域之一，全球数据治理具有其独特内涵和意义。

全球数据治理指的是在全球范围内，各治理主体依一定的规则对全球数据的产生、收集、存储、流动等各个环节以及与之相关的各行为体的利益进行规范和协调的过程。例如，在各行为体参与全球数据治理的交往中，对数据权属的明确、对数据安全的保障、对数据交易的监管和对数据跨境流动的法律规制等等，都属于全球数据治理的范畴。

关于全球数据治理的具体内涵，有三点需要进一步厘清。其一，数据是全球数据治理的直接治理对象。广义的数据治理还包括“依靠数据的治理”，即利用数据创新社会治理思路，将数据治理与社会治理总体变革相联系。^[4]

[1] Barbara L. Cohn, “Data Governance: A Quality Imperative in the Era of Big Data, Open Data and Beyond,” *I/S: A Journal of Law and Policy*, Vol.10, No.3, 2015, p.811.

[2] Executive Office of the U.S. President, “Big Data: Seizing Opportunities, Preserving Values,” May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. (上网时间：2019年6月5日)

[3] 蔡拓：“全球治理与国家治理：当代中国两大战略考量”，《中国社会科学》2016年第6期，第6页。

[4] 参见张康之：“数据治理：认识与建构的向度”，《电子政务》2018年第1期，第5页。

随着数据资源在社会生活中重要性的增加，以及其对传统社会治理模式变革的极大推动作用，“依靠数据的治理”也日益成为数据治理的重要内容。但由于要实现“依靠数据的治理”首先需解决“针对数据的治理”，且当前全球数据治理的主要问题仍集中于“针对数据的治理”，因此目前全球数据治理的内涵仍应限缩在狭义范围内，即“针对全球数据的治理”。

其二，全球数据治理是在大数据时代的背景下展开的，但“大数据”的概念与“数据”并不相同，不容混淆。一般而言，“数据”是指伴随人类生产、生活等各种行为产生并以某种方式记录下来的原始记录。而“大数据”指的是大规模数据的集合形成的一种数据形态。根据著名咨询机构麦肯锡（McKinsey）的定义，“大数据”为容量超出传统数据库软件获取、存储、管理和分析能力的数据集。^[1]此外，“大数据时代”则指的是一个时间阶段，其时代特征表现为大数据的产生和应用十分广泛。因此，三者属不同概念，“数据”才是当前全球数据治理的直接治理对象。

其三，全球数据治理是对数据进行全局性、综合性的治理，所要达成的是一种整体善治的目标。早期数据治理被视为一种管理行为，强调对数据资产的决策制定和职责划分。^[2]但这种定义并未能体现“治理”的应有之义，因而其概念逐渐被界定为一个规划了特定组织中数据的角色、功能和程序以实现数据的妥善管理并作为一种战略资产使用的框架，认为其为组织内人员、流程、技术等协作提供了一种模式。^[3]因此，全球数据治理也应当并不局限于对数据的“管理”，而应以全局性的观念看待全球数据的价值，并尝试探索出一套相对全面和完善的全球数据治理规则。

[1] James Manyika, Michael Chui and Brad Brown, “Big Data: The Next Frontier for Innovation, Competition and Productivity,” McKinsey Global Institute, May 2011, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20for%20innovation/mgi_big_data_exec_summary.ashx. (上网时间：2019年12月5日)

[2] Alistair Donaldson, “Information Governance - A View from the NHS,” *International Journal of Medical Informatics*, Vol.73, No.3, 2014, pp.281-284; Vijay Khatri and Carol V. Brown, “Designing Data Governance,” *Communications of the ACM*, Vol.53, No.1, 2010, pp.148-152.

[3] Barbara L. Cohn, “Data Governance: A Quality Imperative in the Era of Big Data, Open Data and Beyond,” pp.813-814.

推行全球数据治理，一方面是回应全球数据发展之关切，另一方面更是因为推行全球数据治理本身具有重要的意义和极大的优越性。主要体现在以下四个方面：

第一，有助于促进数据跨境流动的规范化和有序化，进一步推进全球数据保护，防范全球性数据安全风险。全球经贸交易、技术交流、资源分享、共同打击数据犯罪都会带来跨境数据流动。然而，数据的跨境传输、存储和应用环节存在着各种安全风险，不仅可能被截获、篡改、伪造、泄露，而且不同国家或区域组织制定的不同的数据政策和法律的差异还可能导致数据所有者和使用者权限模糊，从而产生数据被滥用和数据合规等问题。全球数据治理的推进将进一步深化各国在全球数据安全保护方面的共识，增强全球性数据安全风险的应对能力，加快形成全球范围内的跨境数据流动规则，促进全球数据资源的合作利用和开放共享。

第二，有助于促进全球数字经济的发展，为全球数据交往提供指引。《全球数字经济新图景（2019年）》（国际数字经济白皮书）显示，2018年全球47个国家数字经济总规模超过30.2万亿美元，占GDP总量的比重高达40.3%，其中有38个国家数字经济增速显著高于同期GDP增速。^[1]在全球数字经济发展已呈蓬勃之势的背景下，全球数据治理可以通过构建相应的全球数据贸易规则为人们提供较为明确的预期，有助于打通各国间的数据贸易壁垒，从而有利于进一步扫除数字经济发展的障碍，促进信息化产品和服务跨境运营和商业拓展，推动信息网络技术、产品和服务的创新发展。

第三，有助于促进全球治理体系的完善，推动全球善治的形成。数据作为第四次工业革命中最为活跃的技术创新要素，正在全面重构全球生产、流通、分配、消费等领域，对全球竞争、经济发展、产业转型、社会生活等方面产生全面深刻影响。数据治理已成为全球治理的重点领域。全球治理能力的提高有赖于全球各个领域尤其是重点领域的高效治理，全球治理体系的完善有赖于全球各个领域尤其是重点领域治理机制的统筹协调。因此，在全球层面

[1] 中国信息通信研究院：“全球数字经济新图景（2019年）——加速腾飞 重塑增长”，<http://www.caict.ac.cn/kxyj/qwfb/bps/201910/P020191011314794846790.pdf>。（上网时间：2020年6月28日）

对数据这一重点领域进行治理，将切实推动全球治理体系的完善。

第四，有助于促进协同治理，帮助发展中国家推进和完善国内数据治理。全球治理与国家治理互动融合的“整体性治理”正随着人类知识的发展和治理实践能力的提高而成为一种趋势。^[1]推动全球治理与国家治理的双向有效互动正逐渐成为共识，^[2]而全球数据治理能促进这种互动作用。一方面，发展中国家的国内数据治理在全球数据治理背景下展开，全球数据治理的部分规则会内化为国家数据治理。全球数据治理推进过程中所形成的相对成熟的治理机制、治理思路等可为发展中国家提供借鉴，用以完善国内数据治理。^[3]另一方面，当前部分发达国家和地区已经在国家数据治理上先试先行，并积累了一定的实践经验。而其中相对成熟的经验，可以在全球数据治理中予以推广、借鉴和移植。数据的国别式治理经验的形成和推广，将有效推进全球数据治理的进程，实现“国家治理的世界秩序意义”。^[4]

二、全球数据治理面临的挑战

认清当前全球数据治理的现状及所面临的挑战，是推行全球数据治理的第一步。综观当前的全球数据治理，作为治理对象的“数据”体量已十分庞大，与之相伴的消费者隐私和数据安全方面的风险正在进一步加大，^[5]全球范围

[1] 刘贞晔：“全球治理与国家治理的互动：思想渊源与现实反思”，《中国社会科学》2016年第6期，第44页。

[2] 参见刘雪莲、姚璐：“国家治理的全球治理意义”，《中国社会科学》2016年第6期，第29-35页；吴志成：“全球治理对国家治理的影响”，《中国社会科学》2016年第6期，第22-28页。

[3] 需要说明的是，一国的国内数据治理是其参与全球数据治理的重要基础。全球数据治理中，主权国家所提出的全球数据治理主张应与其国内数据治理主张和实践保持一致，而由此形成的全球数据治理主张才更有说服力，也更容易被全球其他国家所接受。因此，从一定意义上来说，全球数据治理与国内数据治理是相互贯通的，全球数据治理的挑战和应对方案将不可避免地涉及到相应的国内数据治理。

[4] 参见陈志敏：“国家治理、全球治理与世界秩序建构”，《中国社会科学》2016年第6期，第14-21页。

[5] Ginger Zhe Jin, “Artificial Intelligence and Consumer Privacy,” Working Paper, No.24253, National Bureau of Economic Research, January 2018, <https://www.nber.org/papers/w24253.pdf>. (上网时间：2020年6月28日)

内的数据泄露愈发普遍，所造成的损失也日益加剧。^[1]同时，现有的全球数据治理机制仍不完善，存在碎片化、滞后化等诸多现实困境，既缺乏专门的全球性数据治理机构，也未能在现有零碎治理机制之间达成协调，并引发了诸多具体的挑战。

具体而言，由于政府、私营部门和市民社会是网络空间全球治理的重要主体，相互间存在着不同的利益主张，导致了在治理机制构建进程中的多层次冲突。^[2]因此，在全球数据治理中，围绕个人、企业和主权国家这三大至关重要的主体，产生了诸多问题，从而使当前全球数据治理面临两方面挑战：一方面是个人与个人、企业与企业、主权国家与主权国家等同一主体之间的数据权益或主张冲突；另一方面则是个人、企业与主权国家等不同主体之间围绕数据权益产生的冲突。

个人与个人、企业与企业的数据权益冲突是现实生活中较为常见的数据治理议题，但其并非全球数据治理的重点问题。因此，本文在探讨同一主体间数据权益或主张冲突问题上，仅着重探讨不同主权国家间的数据治理主张冲突以及由此带来的挑战。

（一）主权国家间数据治理的不同主张及冲突

随着数据的跨区域流动日益频繁，主权国家谋求数据资源管理和控制的主张愈发强烈，“数据主权”（Data Sovereignty）这一概念因而逐渐兴起，也日益成为各主权国家提出数据治理主张的理论基础。本文对数据主权概念采用狭义理解，即数据主权仅指国家数据主权，为以国家为中心的公权力对本国数据进行控制、管理和利用的权力。^[3]在国家数据主权的理论支撑下，各主权

[1] “2018 Data Breach Investigations Report,” Verizon, <https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-2018.pdf>; “2018 Cost of a Data Breach Study: Global Overview,” Ponemon Institute LLC, July 2018, <http://www.justinholman.com/wp-content/uploads/2019/03/The-2018-Cost-of-a-Data-Breach-Study-by-Ponemon.pdf>.（上网时间：2020年6月28日）

[2] 鲁传颖：“网络空间中的数据及其治理机制分析”，《全球传媒学刊》2016年第4期，第9页。

[3] 关于“数据主权”的概念，广义的数据主权包括国家数据主权和个人数据主权。国家数据主权依赖个人数据主权的支撑和表达，是个人数据主权得以实现的前提，参见 Joel Trachtman, “Cyberspace, Sovereignty, Jurisdiction, and Modernism,” *Indiana Journal of Global Legal Studies*, Vol.5, No.2, 1998, p.566; 狭义的数据主权则指的是一国独立自主地对本国数据进行占有、管理、控制、利用和保护的权利，参见齐爱民、盘佳：“数据权、数据主权的确立与大数据保护的基本原则”，《苏州大学学报（哲学社会科学版）》2015年第1期，第67页。

国家纷纷依据各自不同的国情和利益诉求提出了自身的数据治理主张。因而，在全球层面就产生了数据治理主张的碰撞与冲突，进而为全球数据治理的推进带来了一系列挑战。

第一，各国对个人数据的权属认识不统一，导致全球数据治理中对个人数据采用何种保护路径争论不休。用词上，欧洲国家倾向于采用“数据保护”（Data Protection）一词，而欧洲以外国家往往采用“隐私保护”（Protection of Privacy）、“数据隐私”（Data Privacy）或“信息隐私”（Information Privacy）等词，但都是用来指代与个人数据相关的数据处理上的规制。^[1]措词上的差异反映出不同国家在数据保护路径上的差异。即欧盟国家^[2]将个人数据视作公民的基本权利，具有宪法意义，因此在立法上确立了较为严格的个人信息保护模式，并在一体化进程中不断推进个人数据保护立法。而美国等其他国家则倾向于将个人数据信息纳入隐私权保护框架内，试图通过隐私权的宽松解释解决个人数据保护问题，并在司法实践中逐步确立相应规则。^[3]在中国，个人信息权早期被纳入一般人格权保护，^[4]并获司法实践支持。^[5]随后个人信息权又被界定为一种具体人格权，意图通过构建人格权属保护体系以增强个人数据保护。^[6]随着《中华人民共和国民法典》（以下简称“《民法典》”）的颁布，人格权编独立成编，个人信息保护正式被立法纳入人格权保护的范畴，标志着中国对个人数据的保护仍主要采人格权保护路径。^[7]

[1] Lee A. Bygrave, “Privacy and Data Protection in an International Perspective,” *Scandinavian Studies in Law*, Vol.56, 2010, p.166.

[2] 需要说明的是，虽然欧盟并非主权国家，但欧盟成员国实际让渡了部分主权交予欧盟行使，欧盟在一定程度上行使了欧盟成员国赋予的主权权力。欧盟在数据治理议题上的主张，亦代表了欧盟成员国的整体主张。因此，本文在论述全球数据治理中所涉的主权国家治理主张和利益冲突中，将直接引用欧盟的相关主张，而不再对其成员国主张进行具体区分。

[3] 参见龙卫球：“数据新型财产权构建及其体系研究”，《政法论坛》2017年第4期，第65-68页。

[4] 参见谢远扬：“信息论视角下个人信息价值——兼对隐私权保护模式的检讨”，《清华法学》2015年第3期，第94-110页。

[5] 参见（2011）沪一中民一（民）终字第1325号判决书。

[6] 参见王利明：“论个人信息权的法律保护——以个人信息权与隐私权的界分为中心”，《现代法学》2013年第4期，第62-72页。

[7] 参见《中华人民共和国民法典》第1032-1039条（人格权编第六章之“隐私权和个人信息保护”）。同时，由于中国法学界多数学者对“个人信息”和“个人数据”两个概念持不区分态度，本文亦采此观点。

由此可见，不同主权国家对个人数据所采取的不同观点，导致了其保护个人数据路径的差异。

第二，各国所秉持的数据跨境流动规制理念与主张不同，导致全球范围内的数据跨境流动受限，数字经济活力难以充分发挥。2016年欧盟通过了《一般数据保护条例》(General Data Protection Regulation,以下简称“GDPR”)，并于2018年5月正式实施，其中将个人数据权利视作基本人权。GDPR对数据的跨境流动做出了严格的限制，如第五章“向第三国或国际组织传输个人数据”的第四十五条所规定的“充分保护原则”，要求数据接收国/地区确保达到充分水平的保护标准，才允许数据进行跨境流动。这种“人权与隐私优先、自由流动保障居其次”的一般数据跨境流动规制思路，也成为了欧盟规制各类具体数据跨境流动的基础，^[1]更是欧盟在全球数据治理中所秉持的数据跨境治理主张。而与之不同的是，美国政府不希望采取诸如GDPR如此严格的措施，减损或扰乱美国与其他国家之间正常的贸易合作甚至制造贸易壁垒。立足于自身的信息优势地位并受自由经济观念的影响，在数据跨境流动的规制问题上，美国秉持在安全可控前提下最大程度促进数据自由流动的治理主张，并力求通过签订双边或多边协议形成自身的数据跨境流动规制体系，以充分促进数字经济的发展。例如，在美国与韩国达成的《美韩自由贸易协定》(KORUS FTA)以及美国与墨西哥、加拿大最新达成的《美墨加协定》(USMCA)中，美国均在其中主导加入了数据跨境自由流动的相关条款。

为缓和在数据跨境流动问题上的分歧及促进双边经贸发展，在《安全港协定》实质失效后，美欧于2016年7月就数据传输重新达成《隐私盾协议》，从而实现了从《安全港协定》到《隐私盾协议》的转变。^[2]2020年7月，实施近四年的《隐私盾协议》再次被欧盟法院裁决无效，美欧之间的数据跨境

[1] 王远志：“我国银行金融数据跨境流动的法律规制”，《金融监管研究》2020年第1期，第53-54页。

[2] 《安全港协定》由美国商务部与欧盟委员会于2000年11月达成，意在规范美国与欧盟贸易中涉及的隐私保护和数据流动问题，但该协定因2015年10月6日欧洲法院最终裁定2000/520号决议无效而失效。参见张继红：“个人数据跨境传输限制及其解决方案”，《东方法学》2018年第6期，第40-44页。

传输再度出现重大挑战，双方不得不重启谈判。从《安全港协定》和《隐私盾协议》的谈判历程和内容来看，两者都是美欧互相妥协的结果，其在数据跨境流动治理问题上的分歧并未消失。除美欧之外的其他主权国家，在数据跨境流动问题上也各有不同主张，如俄罗斯高度强调数据主权优先并通过要求数据本地存储的方式来限制数据跨境流动，澳大利亚采取分类管理、分级标识、强制性指南与推荐性指南相结合的折中措施来规制数据跨境流动。可见，不同主权国家在数据跨境流动主张上的分歧，为全球数据治理的协调统一带来了极大的困难。

第三，各国为谋求数据的战略价值，争相制定数据发展战略，从而导致全球数据开发竞争加剧，国家间不对称和不平等的权力结构进一步凸显。网络空间的数据已经、正在而且还将持续转变成为一种战略资源。^[1]在奥巴马政府时期，美国就将数据定义为“未来的新石油”，并将大数据发展提升到战略高度。2012年3月，奥巴马政府提出《大数据研究和发展计划》（Big Data Research and Development Initiative），宣布投入超过2亿美元以大幅改进数据访问、收集和汇总所需的工具和技术，旨在加快美国科学和工程领域发展的步伐，并加强国家安全。^[2]特朗普政府亦致力于稳步推进数据挖掘和利用。2018年5月，白宫行政管理和预算局联合开放数据中心共同主办了一场关于将数据用作战略资产的圆桌会议，意在制定改善联邦政府服务、为美国经济创造价值和就业机会的数据战略。^[3]为了提升大数据信息挖掘和获取能力，英国政府2010年上线政府数据网站（Data.gov.uk），并在此基

[1] Brad Brown, Michael Chui and James Manyika, “Are You Ready for the Era of ‘Big Data’?,” *Mckinsey Quarterly*, Vol.4, 2011, pp.24-35. 转引自沈逸：“后斯诺登时代的全球网络空间治理”，《世界经济与政治》2014年第5期，第147页。

[2] Tom Kalil, “Big Data is a Big Deal,” March 29, 2012, <https://obamawhitehouse.archives.gov/blog/2012/03/29/big-data-big-deal>. (上网时间：2020年6月28日)

[3] Suzette Kent, Nancy Potok and Jack Wilmer, “White House Hosts Roundtable Discussion on Leveraging Data as a Strategic Asset,” <https://www.whitehouse.gov/articles/white-house-hosts-roundtable-discussion-leveraging-data-strategic-asset/>; The Center for Open Data Enterprise, “Roundtable on Leveraging Data as a Strategic Asset Key Takeaways,” <http://reports.opendataenterprise.org/OMB-Key-Takeaways-Report.pdf>. (上网时间：2020年6月28日)

础上于 2013 年发布了新的政府数字化战略。2015 年，英国政府承诺将开放部分核心公共数据库，并将投资建立世界上首个“开放数据研究所”。^[1] 澳大利亚政府信息管理办公室（AGIMO）成立了“大数据工作组”，并于 2013 年 8 月发布了《公共服务大数据战略》，在国家层面提出了六条大数据指导原则。^[2] 日本于 2013 年提出新的信息通信技术（ICT）发展战略，以创造新的高附加值企业、解决社会问题、提高和增强 ICT 基础设施，并逐渐形成智慧日本 ICT 战略整体布局。^[3] 在 2019 年 6 月举行的二十国集团（G20）峰会上，日本首相安倍晋三再次表示将致力于推进数据流通，并与世界贸易组织（WTO）合作制定全球数据流通规则。继发布 GDPR 对一般数据保护作出整体规制后，欧盟又于 2020 年 2 月发布《欧洲数据战略》（A European Strategy for Data），指出要创建一个真正的数据单一市场且面向世界开放，并利用数据促进经济增长、创造价值。^[4] 可见，世界范围内的主要科技强国都在谋划布局相应的数据发展战略，并造成了全球范围内数据规制政策的差异，进而加剧了各国家或地区之间有关数据治理政策的冲突，为全球数据治理的统一和有序化带来了一定的挑战。

更深层次的挑战在于，世界已经进入网络政治的新阶段，世界各国陆续作出反应并逐渐形成“武器化的相互依存”状态。经济互动使得国家间处于相互依存的状态，并产生了新的权力结构。这种新的权力结构的表现是国家间的不对称和不平等加剧，占据网络等相关优势的国家能够将企业乃至整个国家从全球网络中剔除，从而产生深远的后果。^[5] 从全球数据治理的角度而言，

[1] 中国计算机学会大数据专家委员会等主编：《中国大数据技术与产业发展报告（2014）》，机械工业出版社，2015 年，第 8 页。

[2] 张勇进、王璟璇：“主要发达国家大数据政策比较研究”，《中国行政管理》2014 年第 12 期，第 114 页。

[3] Ministry of Internal Affairs and Communications, Japan, “Smart Japan ICT Strategy,” June 2014, http://www.soumu.go.jp/main_content/000301884.pdf.（上网时间：2020 年 6 月 28 日）

[4] European Commission, “A European Strategy for Data,” February 19, 2020, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.（上网时间：2020 年 6 月 28 日）

[5] Henry Farrell and Abraham L. Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion,” *International Security*, Vol.44, No.1, 2019, pp.42-79.

全球范围内就数据流通、数据共享所导致的国家间相互依存的状态将越来越紧密，同时随着主要发达国家和技术强国持续推行数据发展战略，如何防范部分主权国家被剔除出全球数据网络、平衡各国的数据发展战略和国家利益，已经成为全球数据治理进程中所面临的巨大挑战，也是未来全球数据治理亟待解决的重点问题。

（二）个人、企业与主权国家间数据权益的失衡

全球数据治理中，个人享有个人数据权利，并寻求多种路径实现权利保护；企业对经过企业再加工的数据享有权利，以最大程度发挥数据的经济价值，谋求企业发展；主权国家获得了享有数据主权的应然状态，已经或者正在制定相应的数据发展战略，以维护国家安全并最大化国家利益。但三者的诉求存在失衡，甚至在实践中存在一定的冲突。

第一，个人数据权利易受不正当企业数据权利侵犯。个人与企业数据权利界限不明，导致企业侵犯个人数据权利的行为层出不穷。某些个人用户虽然意识到企业正在收集自身信息，但他们并不清楚自己的信息是否会被进一步处理，也不清楚这些信息将以何种方式被处理，最终流向何处。^[1]部分跨国公司在个人不知情的情况下采集了相关个人数据，并依托自身的信息优势对其进行跨境转移，它们极有可能对数据进行滥用，以谋求不正当的企业利益。全球范围内，部分商业巨头违规使用个人数据而遭受监管部门处罚的案例屡见不鲜。2019年1月，法国国家信息与自由委员会便以违反数据隐私保护相关规定为由对美国谷歌公司开出了一张5000万欧元的罚单，其认为谷歌公司在处理个人用户数据时存在缺乏透明度、用户获知信息不便、广告订制缺乏有效的自愿原则等问题。^[2]2020年6月，德国最高法院作出裁定，要求Facebook必须遵守德国反垄断监管机构颁布的一项限制收集用户数据的命令，即在特别许可的情况下，停止自动收集WhatsApp或Instagram等应

[1] Neil W. Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory," *California Law Review*, Vol.88, No.2, 2000, p.476.

[2] “谷歌因数据保护违规遭法国重罚5000万欧元”，人民网，2019年1月23日，<http://finance.people.com.cn/n1/2019/0123/c1004-30586053.html>。（上网时间：2020年6月28日）

用程序使用者的数据。^[1] 这些侵犯公民隐私的企业行为层出不穷的原因，实际上是当前的全球数据治理中缺乏对企业使用个人数据体系化的规制。各主权国家对个人数据的保护路径意见不一，个人和企业数据权利未能实现利益协调与合理规范，导致全球数据治理进程中乱象不断，既不利于数据隐私的保护，也不利于数字经济的发展。

第二，主权国家与企业数据资源不对称，数据主权的实现困难重重，依托数据主权实现高效数据治理仍存在现实障碍。一方面，大量的数据被跨国互联网信息巨头实际占有和使用，^[2] 主权国家对部分关键甚至具有战略价值的重要数据缺少实际控制，无法在国家治理层面直接应用企业数据。另一方面，主权国家在不直接掌握部分重要数据的现实困境下，缺乏与企业就数据权利互动沟通的有效机制，从而一定程度上延缓了各主权国家数据战略目标的实现，也阻碍了全球数字经济的充分发展和繁荣。国际数据公司（IDC）2019年1月发布的白皮书显示，到2025年中国将拥有全球最大的数据圈，其中企业级数据圈将从2015年占中国数据圈的49%增长到2025年的69%。^[3] 可见，企业数据在整体数据中占据大部分比例。而这一资源不对称的现状，将使得主权国家在全球数据治理进程中无法切实掌握数据资源并对其展开有效治理。

第三，国家数据主权与个人数据权利不相协调，甚至产生冲突。个人数据权利依赖国家法律法规、政策和相关配套措施的保障，而国家基于保护人权和隐私的目的承担公民个人数据保护的国家责任。然而，国家在治理过程中需要使用大量数据，其中不乏众多个人数据。而个人数据中又含有大量隐私信息，国家调取、查阅个人数据的过程可能造成个人数据信息的频繁流动甚至带来泄露的风险，而且这种获取的过程极有可能是秘密的、信息不对称的，

[1] “德法院裁定 Facebook 需遵守监管命令：限制收集用户数据”，新浪财经，2020年6月24日，<https://finance.sina.com.cn/stock/usstock/c/2020-06-24/doc-iircuyvk0121187.shtml>。（上网时间：2020年6月28日）

[2] 翟志勇：“数据主权的兴起及其双重属性”，《中国法律评论》2018年第6期，第197页。

[3] 根据 IDC 的定义，“数据圈”是指每年被创建、采集或复制的数据集合。相关数据和图表参见 IDC：“2025 年中国将拥有全球最大的数据圈”，2019 年 1 月，<https://www.seagate.com/files/www-content/our-story/trends/files/data-age-china-regional-idc.pdf>。（上网时间：2020年6月28日）

存在侵犯个人数据权利的风险。再如，国家在特定的紧急情况下，为服务公共利益的需要，强制且未经同意地获取特定个人的数据信息，也极易造成国家数据主权与个人数据权利的对立。甚至实践中存在为保护一国的国家安全或重要利益，获取他国国民数据信息的行为。如美国在“9·11”事件之后颁布的《爱国者法案》中就规定，无需数据主体的事先同意，美国政府可以获取任何存储于美国数据中心的信息或者是美国公司所存储的信息。该法案下，政府获取相关信息后，数据主体极可能并不知情。^[1]2013年曝光的“棱镜门”事件更是反映了以美国为首的部分国家非法侵占他国个人数据、破坏个人隐私的事实。总之，当前全球数据治理中，国家数据主权的权力边界仍有待厘清，其与个人数据权利的关系仍有待协调。

三、推动全球数据治理的路径

面对全球数据治理的种种挑战，国际社会尚未形成成熟的治理机制。全球数据治理不仅在主体上呈现多元化，而且没有专门的全球性数据治理机构，已有的治理机制之间也缺乏明确的职能分配和统筹协调安排。有关数据治理的讨论大多被置于全球多边合作的框架之下，因此在探讨数据治理议题时可能会与其他相关议题穿插进行，从而导致有关数据治理的对话与合作趋于泛化，大大降低了全球数据治理的有效性。当前，有关全球数据治理的主张散见于与数据有关的各个具体领域，其中最为突出也最受关注的便是各主权国家在数据跨境流动治理主张上的差异。全球统一的数据跨境治理规则迄今未见雏形。因此，从整体上对全球数据治理体系进行建构，以应对全球数据治理的多重挑战，已十分迫切。具体而言，可以从以下两方面进行应对：

（一）加强整体治理，推动建立全球数据治理规则

未来全球数据治理机制的形成，一定程度上取决于对全球数据治理路径和主张的选择。数字时代，算法和数字平台塑造并约束着相关主体的行为，

[1] Primavera De Filippi and Smari McCarthy, “Cloud Computing: Centralization and Data Sovereignty,” *European Journal for Law and Technology*, Vol.4, No.2, 2012, pp.15-16.

既成的法律往往难以执行，决策者对治理路径的选择将在一定程度上影响数据发展的走向，引导整体治理机制的形成。^[1] 在借鉴和吸收已有的相对成熟的数据治理措施的基础上，面对全球数据治理中的不同主张，各主权国家应当充分结合自身国情，形成并完善自身的数据治理主张，以实现数据主权、数据保护与数字经济发展相统一。此外，各主权国家还可以通过积极参与全球数据治理，将自身数据治理主张推向全球并谋求完善，进而推动全球性数据治理规则的形成。

1. 妥善协调各主权国家的数据发展战略，实现数据价值的共享

在全球数据治理的实践中，不同主权国家或地区业已根据自身利益诉求，制定了相应的数据发展战略，以谋求实现对数据的战略利用，并进一步发挥数据的战略价值，由此导致国家间的不对称和不平等不断加剧。如何防范部分主权国家被剔除出全球数据网络、平衡各国的数据发展战略和国家利益，日益成为全球数据治理层面亟待解决的问题。而反观现实，目前零散的、未成体系化的治理机制并不能发挥协调各方、互助合作和实现价值共享的作用，因而需要重新构建。

具体而言，应推进将联合国及各区域组织作为全球数据治理的重要平台，由其妥善协调组织内各主权国家或地区的数据发展战略，化解各国在数据发展战略上的冲突，促进各方在互利合作的基础上实现战略数据的共享。其中，以联合国为首的全球性数据治理平台，可以更多关注全球各国、各地区数据战略的平衡发展，组织全球数据治理领域的多边洽谈并构建相关洽谈和磋商机制，协调各国、各地区的数据利益，力争使数据经济价值为全球所共享。在联合国整体治理框架下，各区域组织可以发挥其区域内紧密合作的优势，打造更加精细化、具体化的数据治理实施方案。

2. 加快形成全球数据治理整体框架，完善数据保护法律法规

由于借助互联网而获得不断发展的商业活动和国际市场的极大扩张，企业正在收集和传输比以往更多的跨境数据。其结果便是，全球各国政府都在

[1] See Martin Kenney and John Zysman, "The Rise of the Platform Economy," *Issues in Science and Technology*, Vol.32, No.3, 2016, pp.61-69.

积极地制定或完善法律法规以更好地保护公民的个人数据，无论这些数据是私人拥有还是政府拥有，是本地的还是境外的。^[1]自1980年经济合作与发展组织（OECD）率先出台《隐私保护与个人数据跨境流动准则》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data，以下简称OECD准则）这一首份有关信息化背景下隐私保护和数据跨境流动的法律文件以来，无论在国际交往还是国内治理层面，均已产生众多与数据治理有关的法律法规。其中，最具影响力的立法当属欧盟GDPR的颁布，其对数据保护采取的强有力规制，为世界范围内的数据保护立法提供了范本和借鉴思路。

但是，当前全球数据治理的规则机制大部分仍局限于国内或区域层面，全球数据治理的整体框架还未形成，全球层面统一的数据保护法规体系更是未见雏形。这不仅给数据跨境流动造成了障碍，更为全球范围内有关数据纠纷的法律适用带来了困惑。因此，为有效推进全球数据治理，各国除了应当在已有立法的基础上，不断健全和完善国内数据保护相关的法律法规之外，还应通过国际交流、对话和谈判的方式加快形成全球数据治理的整体框架，并发展出相对完善和健全的国际数据保护条约或相关适用机制，从而构建一个合理、协调、高效的全球数据治理体系。

3. 加强数据跨境治理交流与合作，推动全球数据治理规则的完善

数据跨境治理是全球数据治理中的重要内容，妥善处理数据跨境流动问题，既是捍卫数据主权和保护国民数据权利的要求，又是推动全球数据贸易和数字经济发展的关键所在。早在2004年，亚太经济合作组织（APEC）就通过了一项试图构建成员国数据与隐私保护的框架，随后逐渐构建形成了APEC跨境隐私规则体系（The APEC Cross Border Privacy Rules），这在一定程度上推动了亚太地区数据治理的进程。目前，联合国层面已有的关于数据治理的讨论仍散见于不同的重大议题中，比如数字经济、可持续发展、人权与

[1] Jeremy Berkowitz, Michael Mangold and Stephen Sharon, "Data Flow Maps - Increasing Data Processing Transparency and Privacy Compliance in the Enterprise," *Washington and Lee Law Review Online*, Vol.73, 2016-2017, p.805.

平等、人道主义行动等，^[1]但是集中的、体系化的数据跨境治理机制尚未形成，全球范围内的数据跨境治理交流与合作仍存在障碍。

不过，在全球数据治理规则的构建上，国际合作和磋商已初步展开。2019年6月，在日本大阪举行的G20峰会发布了“大阪数字经济宣言”，标志着国际数字经济正式进入“大阪轨道”。在领导人数字经济特别会议上，日本首相安倍晋三提出应在数据自由流通可信规则 DFFT（Data Free Flow with Trust）的基础上，建立允许数据跨境自由流动的“数据流通圈”，意在强调推动建立全球数据流通的相应规则。^[2]

在现有的数据跨境合作方式和全球数据治理规则建构雏形的基础上，全球数据治理应当继续深化和完善。就数据跨境治理而言，一方面，各主权国家或区域组织可以进一步签订专门性的双边或多边协议、条约等，对各方的数据跨境流动问题进行规制；另一方面，各主权国家或区域组织也可以尝试在与其他主权国家或区域组织签订的双边或多边贸易协定中，加入相应的数据跨境流动条款，以规制双方经贸往来中所涉数据跨境流动问题。联合国等治理平台应充分关注数据跨境流动问题，积极引导和形成数据跨境流动国际合作机制。与此同时，随着全球数据领域的相关违法犯罪行为日益猖獗，增强数据跨境治理的交流与合作在一定程度上也是跨境打击数据犯罪、维护全球数据治理秩序的切实需要。就全球数据治理规则建构而言，当前已有的国际磋商与合作仍多局限于科技发达国家或数据强国，众多不发达国家仍未能参与其中甚至遭到排斥，既无法合理表达其对全球数据治理规则的意见，也无法脱离既定规则的影响。因此，下一步应继续拓宽各主权国家和区域组织深层次参与全球数据治理规则制定的渠道，平衡保障各国的数据权益。

（二）创新治理思路，构建多元主体数据协调治理机制

全球数据治理的推进，既要关注主权国家间数据交往矛盾的调和，也必

[1] “数据创新促进发展”，联合国网站，<https://www.un.org/zh/sections/issues-depth/big-data-sustainable-development/index.html>。（上网时间：2020年9月28日）

[2] “安倍总理在G20大阪峰会数字经济首脑特别活动上的演讲”，日本国首相官邸网站，2019年6月28日，https://www.kantei.go.jp/cn/98_abe/statement/201906/_00007.html。（上网时间：2020年6月28日）

须关注全球层面个人、企业和主权国家三者数据权益的协调，找到一条合理高效的数据协调治理路径。综合考虑当前全球数据治理的现状和挑战，全球数据治理的推进可以考虑采用以下三种具体的数据协调治理机制：

1. “人格权先行”数据协调治理机制

全球数据治理推进过程中，无论是企业的数据利用，还是国家层面主张的数据主权，都应当充分尊重个人对数据享有的人格权益，并将此作为全球数据治理的基本原则。这种协调治理主张在当前欧盟以 GDPR 为首的规范中得到了广泛认同，并可以衍生出一系列的数据协调治理规范。第一，主权国家对个人和企业的一般数据使用均应采取“知情同意”原则。这里的一般数据指的是除对一国的国家安全存在实质威胁或不立即强制获取将对社会公共利益造成重大损害外的所有数据。就知情同意的内涵，应理解为：主权国家基于行政管理职能、社会保障需要及其他现代国家机器运行所必须收集的公民个人数据信息，^[1] 应视为已获得“知情同意”。这是因为，若这些数据被视作未经“知情同意”而导致无法被主权国家第一时间使用，那么现代国家的组织管理职能将举步维艰。

但是，对于原本被各类企业收集、存储于一定载体之上且未经企业自主加工的数据，主权国家并不自然享有使用这些特定个人数据的权利，除非个人已经明示或者默示地同意其他主体对该等数据的使用。美国在“9·11”事件之后颁布的《爱国者法案》就实质性违反了上述“知情同意”原则，其结果是对个人数据隐私造成了重大的威胁。

第二，若存在对一国的国家安全产生实质威胁或不立即强制获取将对社会公共利益造成重大损害的特定数据，应当认可主权国家有权获取该等数据并作出处理。这是因为，当公共利益与个人利益发生冲突时，为了实现公共利益，在满足比例原则、利益补偿原则及正当程序原则的基础上，对个人权利进行一定的限制具有正当性。^[2] 因此在这种情况下，人格权和数据隐私需

[1] 例如，公民的姓名、年龄、住址、身份证号、社会保障号等已经被收入相关国家机关数据库中的数据。

[2] 参见范旭斌：“论公共利益与个人利益的平衡”，《云南社会科学》2009年第6期，第43-47页。

要暂时、有条件地让位于国家“数据主权”的行使，以保障国家整体安全。

2. “财产化市场交易”数据协调治理机制

全球数据治理应通过建构具体可行的数据市场化交易机制，以推动全球数字经济的发展。在充分尊重人格权和保障公民个人数据隐私的基础上，全球数据治理应注重数据的财产属性，正视数据所蕴含的经济价值，允许一般数据在市场上自由流动和交易，形成“财产化市场交易”数据协调治理机制。由于数据具有一定的经济价值，企业可以通过国际市场进行数据交易，获取企业生产、经营过程中所需要的数据；数据再加工型企业可以更加便利地利用原始数据进行数据分析，企业数字经济的活力将大大提升；主权国家在非紧急状态下使用个人或企业数据，也同等适用该协调机制，即通过市场化交易的形式获取和使用数据，个人或企业将其对数据享有的权益让渡给主权国家使用。

这种“财产化市场交易”协调治理机制的优势体现为三点。第一，在尊重个人和企业数据隐私的同时，它弥合了国家数据主权与个人及企业数据权利的鸿沟，并充分发挥了数据的经济价值，将有效推动数据流动，促进全球数字经济发展。第二，“财产化市场交易”数据协调治理机制为缓解当前企业与主权国家掌握的数据资源不对称的现实困境提供了重要思路。通过数据的市场化交易，企业所掌握的大量重要数据能够为主权国家所使用，后者利用这些数据能够更好地推进国家治理和全球治理，构建更加完善的公共服务体系。第三，从全球数据治理体系而言，全球范围内的数据交易将被市场化、规范化、透明化，有利于推动全球数据市场的形成和完善。并且从实践来看，在确保安全和不侵犯隐私前提下的数据市场化交易已经得到发展。^[1]WTO于2019年初首次推动制定数据贸易规则，也正是为了规范当前市场化的数据交易。^[2]

[1] 例如，2014年末，中国第一家大数据交易所——贵阳大数据交易所成立，截至目前该交易所的大数据交易量十分巨大。

[2] “WTO将制定数据贸易的国际规则”，中国国际贸易促进委员会网站，2019年1月8日，http://www.ccpit.org/Contents/Channel_3673/2019/0108/1110574/content_1110574.htm。（上网时间：2020年9月28日）

3. “匿名化战略利用”数据协调治理机制

在信息化时代，战略优势将属于那些在信息的生产、传输、加工、存储和使用环节中占据主导地位的政府和行为体。^[1] 由于主权国家的数据发展战略需要强大的数据资源支撑，全球数据治理应当正视主权国家对数据资源的战略需求，并通过构建一项对主权国家获取相应战略数据的豁免机制——“匿名化战略利用”数据协调治理机制，以协调各主权国家数据主权与个人数据权利的矛盾。具体而言，主权国家可因特定战略需要，向个人和企业收集和使用匿名化的数据信息，组成统一数据以实现优化公共管理、统筹战略部署等目标。

所谓匿名化，指的是被主权国家所征用的数据必须是“去标识化”的，既不能通过单一数据信息精准定位到个人，也不能通过所征用的多种数据信息识别出特定个人。而且，在匿名化处理的过程中，若产生了相应的数据处理成本，应当由主权国家负担而不能转嫁于企业，否则将会不合理地增加企业运行成本。从实践上来看，个人数据的“匿名化”已经被多个国家和地区纳入数据治理体系内，^[2] 并被赋予相应的标准，^[3] 具有一定的实践基础。这种“匿名化战略利用”数据协调治理机制的优势在于，其既能有效保护公民的个人隐私，又充分发挥集合数据的战略价值，为主权国家提供了战略上的参考，能够一定程度上消解个人与主权国家在数据治理议题上的矛盾。

【完稿日期：2020-11-4】

【责任编辑：肖莹莹】

[1] [美] 罗伯特·基欧汉、约瑟夫·奈著：《权力与相互繁荣》，门洪华译，北京大学出版社，2012年，第241-246页。

[2] 如欧盟GDPR在前言第26段、第28段以及正文第4条、第11条均就“匿名化”的个人数据问题进行了规定，明确数据保护的原则不应当适用于匿名化数据。

[3] 美国、日本、新加坡和英国的立法或监管机构也对匿名化数据设定了各自的标准。参见王融：“数据匿名化的法律规制”，《信息技术》2016年第4期，第40页。