国观智库
GRANDVIEW
INSTITUTION

数据之重:美中两国数据治理和网络安全方法

国观智库

美国中美研究中心

联合课题组

2023年2月

目　录

执行摘要

数据是数字经济的命脉。随着中国和美国都试图在定义第四次工业革命的关键数据产业中占据优势，数据也成了策略竞争的舞台。习近平主席谈到数据革命给生产流程、生活方式和社会治理方式带来的深刻变化，并强调了深化互联网、大数据和人工智能与实体经济融合的必要性。美国国家安全顾问杰克·沙利文(Jake Sullivan)称数据是一种“力量倍增器”技术，在未来十年将尤为重要。正是由于数字化带来的巨大利益，中国和美国都大步迈向数字前沿，但是他们的方式并不相同。在主权、监管和安全——释放和保护数据价值的三大关键要素上，中国和美国的做法异远大于同。

中国将数据视为独立的“生产要素”，这一做法独特且颇具远见卓识。中国采取的数据治理和网络安全的方法是自上而下的，由国家以协调一致的方式推动。方法也是全面的，旨在在安全性、隐私性、包容性和商业等相互竞争的因素之间取得微妙的平衡。在隐私和个人信息保护方面，中国采取了规范性的做法。虽然大多数非个人数据或多或少被允许自由跨境流动，但个人数据只有在目的地国被认为拥有具有内置保障措施的类似数据保护制度的情况下才能自由跨境流动。此类数据，特别是关于敏感和其他“重要数据”必须通过安全评估，且这种安全评估涵盖范围广泛而严格(尽管不针对任何特定的国家)。中央领导层在数据治理和网络安全方面的总体目标是制定一个深入、流动和开放的市场的长期参数，在这个市场中，数据要素可以进行有效和可信赖的国内和跨境无缝交易，同时防止数据误用、滥用或成为对抗国家的武器。

相比之下，美国的数据治理方法更加自由放任，由私营部门主导。一方面，美国政府极力保护数据畅通无阻的权利，包括畅通无阻的跨境流动。在数字市场准入方面的立场激进，监管宽松。除了有限的安全和执法例外情况，例如不得将敏感数据传输给外国对手，以及政府可以无条件访问受美国管辖的机构和个人可能存储在海外的数据，数据可以不受阻碍地移动。个人数据和非个人数据的处理没有实质性的区别。另一方面，美国在国家层面缺乏全面的数据保护和隐私制度。数据相关规则由联邦和各州相关法律、美国联邦贸易委员会的裁决、特定行业的隐私义务和机构级数据保护标准“拼凑”而成。

中国和美国对数据治理和网络安全的不同愿景和方法阻碍了多边层面跨境数据流动规则的发展。在各自的国内监管框架——特别是在安全和隐私框架方面——进一步统一之前，多变层面推行跨境数字贸易自由化流动相关规则仍将十分艰难。在这种情况下，推出区域层面的规则成为退而求其次的选择。《数字经济伙伴关系协定》(DEPA)和《全面与进步跨太平洋伙伴关系协定》(CPTPP)等区域框架正逐渐成为跨境数据治理规则制定方面的事实标准。在这一前提下，美国和中国可以通过第三方框架探索跨境数据流领域的潜在合作机会——尽管必须指出，任何一方都不容易克服这其中的诸多障碍并在第三方平台上协调他们方法。

网络安全合作的情况也是如此。近年来，网络安全已成为数据治理中越来越重要的组成部分。由于频繁的勒索病毒攻击、数据泄露等安全事件，数据正日益直接影响社会稳定、经济发展和国家安全。然而，围绕核心网络安全规则达成全球共识一直很难，迄今为止提出的各种建议和倡议通常都是自愿、无约束力的。不管愿不愿意，全球网络安全规则的制定将不得不由在国内范围执行的规则和标准的拼凑而成，或者最多是由区域范围的规则和标准拼凑而成。但愿与跨境数据流动的情况一样，大型数字生态系统之间的网络安全规范可以逐渐实现趋同。如果没有这种融合，这些生态系统之间至少可以形成一种基本的共存。

在可预见的未来，无论是在中美层面还是在全球层面，为数据治理规则和规范铺路从而应对数字政策挑战仍将是一项具有挑战性的工作。然而，鉴于数据对 21 世纪生活方式以及社会、工业和经济进程的深远影响，必须以饱满的智慧和决心寻求全球、区域和双边治理规则和规范的协调。

第一部分——数据治理和网络安全给国家来带新问题与新挑战

在全球大宗商品价格攀升、核心通胀高企、经济增速减弱的世界中，总要有些亮点来呵护大家对未来的信心。数字经济就被寄予这样的厚望。

随着主要经济体竞相建立由 5G、人工智能(AI)、云计算和物联网(IoT)等一系列创新推动的数字经济，数字前沿成为一个充满机遇和挑战的领域。预计到 2025 年，新数字技术构成的全球市场规模预计将达到数万亿美元，数字市场将具有巨大的增长潜力。作为全球排名前两位的经济体，中美两国都不愿错过数字经济大潮，各自迅速推动本国经济以及国际经济的数字化。中国将发展数字经济置于“双循环经济”愿景的核心，美国强调数字贸易是其新的印太经济框架(IPEF)的核心组成部分。

中美两国各自构建起基于数字经济的庞大愿景，而要将愿景变为现实，数据治理和网络安全是难以回避的问题。数字经济驱动全球发展，数据则负责驱动数字经济。数据治理和网络安全就是基于数据这个基本要素进行规划管理与协调合作，保障数据能在安全有序运行。

一． 数据治理和网络安全研究对象和范围

数据治理的概念最早在 20 世纪 90 年代网络大爆炸的时代就已被提及。按照国际标准化组织的定义，数据治理是指对数据资产管理行使权力和控制的活动集合，包括规划、监督和执行等，旨在为组织的数字化转型奠基并赋能，助力实现数据资产的价值最大化，并拓展数字化应用的想象空间。也有研究认为，数据是一种资产，通过服务产生价值，数据治理是在数据产生价值的过程中，治理团队做出的评价、指导和控制。

数据的价值在于流动与汇聚，这通过数据开放、交换和交易等形式实现。但流动与汇聚如果只遵循市场规则，会在一国市场内会造成数据垄断，在全球范围内会带来数据霸权，就需要针对数据流动中存在的问题进行数据治理，衍生出网络安全问题。数据垄断会导致数据滥用，

出现“大数据杀熟”“诱导性推送”等问题，甚至是个人数据非法采集等问题，于是需要通过有效监管，规范网络安全，促进数据使用安全。

全球数据治理和网络安全是个全新的领域，范式建构也是开放的。作为数字经济驱动力的数据产生规模大，随着物联网、人工智能的推进，每时每刻都有新的数据产生，数据总量指数级增长。现有的数据储存、分析和使用方案需要不断迭代，才能满足需求。因此数据治理和网络安全不能只立足现实，还要放眼未来，在构建数据市场规则和提高数据治理水平方面建立开放型讨论框架。

二． 数据治理和网络安全研究目的

数据治理和网络安全是对数据资产进行规划、监控、执行、管理的一种带有强烈目的性的实践活动，目的是释放并保护数据的价值。为实现这一目标，需要重视数据“3S”因素，即主权（Sovereignty）、监管(Supervise)和安全(Security)。

当数据被认为是国家的一种战略资源后，不但赋予数据广阔的开发与增长的空间，同时也带来新的领域：在国家间如何对涉及跨境的数据属权进行有效分割，这就是数据主权问题。数据主权是国家主权在网络应用中的自然延伸，国家拥有对本国信息资源进行保护、开发和利用的权力，全部包本国信息不受该国干涉，自主进行信息的生产、加工、存储、流通、交换和传播，同时对本国数据的输出和国外数据的输入进行监管的权力。

对数据的监管是国家主权利益的重要组成部分，体现出对数据的掌控和分析能力。审慎监管的基础是数据确权。在境内需要厘清数据归属权、使用权和收益权于个人还是平台，或者是公共产品。数据治理需要政府、企业、个人三方广泛参与，但三方的诉求虽然都集中在数据领域，但治理重点却有所差异。政府的切入点是数据的监管权，平台专注推动信息要素自由流动，而个人则要充分保护自身数据。

数据治理就是要保障目标三角尽量满足各方需求，通过覆盖数据全生命周期中的各种过程和状态，利用手段和活动释放、保护数据的价值。目前的共识是在保证有效监管的前提下，在推动数据自由流动和保护个人数据权利之间进行权衡，即在效率与公平间调整。

当前云端数据对数据监管构成进一步挑战，云计算和云存储将数据的所有权和控制权分隔开。用户可以随时访问储存在云端的数据，而对数据的控制权却掌握在提供云存储服务的服务商手中。发生数据跨境流动的情境下，涉及各方都会主张拥有数据权利，会形成数据主权声索的重叠乃至冲突。以类似 GDP 的 GDD（Gross Domestic Data）的模型进行划分，是数据监管在实施上较为可行的方式。

近年来网络安全在数据治理中占据的考量越来越大，数据跨境流动给治理和安全带来了诸多挑战，对传统安全观来说，这是一个全新的领域。数字经济时代，数据已经成为国家基础性战略资源和新型生产要素，伴随而来的数据安全风险日益升级，勒索软件攻击、数据泄露等安全事件频繁发生，直接影响到社会稳定、经济发展和国家安全。社会各方面对于用户画像、算法推荐等新技术新应用高度关注，对相关产品和服务中存在的信息滥用和安全漏洞等问题反映强烈。如何在保障安全和隐私前提下推动数据合理有效利用，数据安全如何体系化、具体化的落地，如何使用关键技术来满足全数据应用场景的安全需求等，成为数据安全治理实践方面的新思考、新挑战。

三． 数据治理和网络安全研究方法

由于数字经济被视为重要战略领域，针对“3S”因素近年来中国和美国相继出台了一系列政策文件和法律文件，这些体现公共意志的文件也构成了分析北京和华盛顿在数据治理和网络安全框架的基础性文本。通过研究政策形成路径，以及决策过程中的关键参与者和部门，能更清晰地了解中美两国在数据治理和网络安全方面的重点和脉络。

政策文件和法律文件构成了数据治理和网络安全国内文本，在这方面还有一部分文本是两国签订的相关双边和多边贸易协定。数字经济已经成为国际贸易中的重要组成部分，各国在保障数据跨境贸易和加强协同监管方面做了不少尝试，但目前得到都只是阶段性的成果，并没有建立起固定的框架。

最新的一次尝试是在 2022 年 6 月中旬，中美两国都参加了世贸组织第 12 届部长级会议。会议中各国讨论了《关于电子商务的工作计划》，
（https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/W23.pdf&Open=True）

各方同意在 2023 年底之前召开第 13 次部长会议之前，维持目前不对电子数据传输征收关税的做法。

四．相关政策建议

中国和美国都采取了各种严格的方法来进行数据治理，并全力保护数据安全，但由于在地缘政治竞争时代，北京和华盛顿的数据治理像是两台在不同点上开凿隧道的工程车辆，彼此之间几乎没有协调，再加上数据治理领域拥有一定话语权的欧盟则在第三点开凿，这种分头行动使全球数据治理和网络安全的前景仍然充满挑战。

本研究的初级结果是要了解中美在数据治理和网络安全方面政策法规的不同，正视差异。对不同国家的数据治理和网络安全政策加深了解，是研究的出发点。要意识到在形成统一的标准、均衡考量各国情况差别和利益述求之前，实现真正的数据自由跨境流动并不容易。

本研究的中级结果是为管控相关分歧提供框架。国际上多轨并行的数据治理和网络安全政策，容易导致并此间的政策误读，带来数字前沿的脱钩，甚至发生数字对抗。了解分歧产生的根源，可以更有效地控制分歧烈度，尽量降低数据资源争夺的成本。

本研究的高级结果是要探索中美在数据治理和网络安全领域潜在的合作机会。数字化时代中美两国都面临数据治理和网络安全面临的挑战，而随着全球化的退潮，区域化成为不得已而求其次的选择。在数据治理方面，CPTPP 等区域性框架逐渐搭建，这成为目前数据治理中关于跨境流动的天花板。中美两国在达成双边数据治理和网络安全协议前，区域平台是形成合作的现实渠道——虽然从目前看即使在同一平台上对对话合作也并没那么容易。

第二部分——中国和美国在数据治理和网络安全方面的做法

一、中国

前言

中国的数字发展令人震惊。从数字基础设施建设到数字经济的规模，再到数据生成的规模，中国国家数字化的状况在过去的十年获得飞速发展。

在数字基础设施建设方面，截至 2021 年，中国拥有 1，425，000 个 5G 基站，占全球总数的 60%，以及 4.55 亿 5G 用户。300 多个城市安装了千兆级光纤，3460 万用户接入了千兆级固定宽带。互联网用户总数从 2012 年的 5.64 亿增长到 2017 年的 7.72 亿，2021 年达到 10.32 亿——互联网普及率为 73%。数字经济也同样迅猛发展。ICT 硬件和设备制造以及软件开发和收入的年度总值从 2017 年的 27.2 万亿元人民币(占 GDP 的 32.9%)增长到 2021 年的 45.5 万亿元人民币(占 GDP 的 39.8%)。这一非凡的数字发展的基础是数据生成的爆炸性增长。中国网络空间的原始数据产量从 2017 年的 2.3 兆字节(ZB)跃升至 2021 年底的 6.6 兆字节，占全球数据总量的 9.9%。大数据行业的收入也增长了近两倍，达到 1.3 万亿元人民币。如今，数据生成，更广义地说，数据基础设施系统，作为一种新的“生产要素”，正融入中国经济的肌理之中。

支撑中国数据基础设施体系的数据治理和网络安全的基本方法也同样令人惊叹。就像深度、流动性和开放的资本市场一直是美国金融优势的标志一样，中国在网络领域旨在逐步培育一个类似的深度、流动性和开放的数据元素市场。数据不仅仅是数字经济的命脉；它与土地、劳动力、资本和技术并列，是一种成熟的新“生产要素”。中国拥有 14 亿多潜在的数字消费者，成为“网络超级大国”指日可待。

中国数据要素市场的政治框架由四大支柱构成。

- 建立现代**数据产权制度**，旨在促进数据持有权和数据使用权的有序分离，从而促进数据的高效市场化流通。这种基于权利的制度将促进公共、私人和企业数据的有区别、分级和授权使用。
- **中国社会能够公平访问和平等使用数据要素的系统**，其目标是扩大基于市场的数据要素分配的范围，并保护贡献资本或劳动力的数据要素的收入和生计。此外，预计大型数据企业将承担更大的社会责任。
- 在关键问题安全和明确的监管红线的基础上，**建立现代数据安全治理体系**，为所有数字社会参与者创造一个安全可信的环境。
- **数据要素国际流通和交易系统**，旨在建立可靠的跨境数据流通系统，确保数据来源可确认，使用范围可界定，流通过程可追踪，安全风险可预防；同时可以促进数字规则制定和标准制定机构以及数据安全、数字货币和数字经济税收方面的国际交流和参与。

简言之，隐私、商业、包容性和安全是中国数据治理和网络安全的核心。在这个矩阵中，安全被放在最突出的地位，其后是关于隐私和个人信息保护的详细规则。随着数据安全、数据所有权和数据使用规则或多或少地到位(并经常更新)，监管的焦点现已转向数据流动规则的制定，特别是促进国际商务的跨境数据流动规则的制定。

与此同时，相关机构正在依据“同行业、同规则”的原则起草防范金融科技导致的金融稳定风险的法规，打击大型科技公司的反竞争商业行为。全国人民代表大会常务委员会 2022 年 6 月也通过了对《反垄断法》的修订，规定对大型科技公司收购和市场集中行为进行审查。相关机构采取多种措施为人工智能(AI)应用程序、算法推荐引擎和反对深度伪造技术的传播制定规则。

1.中国数据治理和网络安全制度的法律框架

支撑中国数据要素市场及其数据基础设施系统的法律框架的起源和构建可以追溯到 2015 年 7 月 1 日的新《国家安全法》。该法律引入了国家安全的概念，创建了有利的法律基础设施，并废除了过于侧重于反间谍活动的 1993 年版《国家安全法》。新《国家安全法》第三条阐明了国家安全与经济、文化和社会安全之间的直接联系。其附属条款(**第二十五条**)要求建立一个“国家网络和系统安全保障体系”，目标是“实现核心网络和信息技术、关键基础设施、重要领域的信

息系统和数据的安全和可控”，“惩罚网络上的违法犯罪活动”，以及“维护网络空间主权、安全和国家的发展利益”。第五十九条提到了关于侵犯外国投资、关键材料和技术以及互联网或信息技术产品和服务的国家安全审查程序。

2017 年 6 月，第十二届全国人民代表大会常务委员会通过了配套的**《国家情报法》**。2019 年 10 月，**《密码法》**出台。

根据美国政府的说法，“迫使”中国公司和公民协助国家安全和情报工作的法律法规

美国国家安全和司法部高级官员不时发布警报报告声称中国是美国最大的反间谍威胁。在这个问题上他们过度紧张。在他们看来，“每一个中国公民和公司”，包括“表面上的私营公司、研究生和研究人员”，更不用说中国的情报部门和国有企业了，都被法律“强迫[引导]”去“协助国家安全或情报工作”。为了支持自己的观点，中国安全和情报法律中的违规条款被一一列举出来:

2021 年 6 月通过的《数据安全法》第三十五条:“公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。”

2017 年 6 月通过的《国家情报法》第七条:“任何**组织和公民都应当依法支持、协助、配合国家情报工作**，保守所知悉的国家情报工作秘密。”

另一方面，值得注意的是，第八条规定，国家情报工作应当依法进行，尊重和保障人权，维护个人和组织的合法权益。

2016 年 11 月通过的《网络安全法》第二十八条:“网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。”

2015 年 7 月通过的《国家安全法》第十一条:“中华人民共和国公民……有维护国家安全的责任和义务。”

这份列表既不独特，也不令人惊讶。所有主要国家都有各种类似的法规来帮助执法机构进行调查和/或保护数字和国家安全。例如，美国的《CLOUD(澄清境外合法使用数据)法案》可以强迫服务提供商（比如谷歌），上交用户存储在外国司法管辖区的内容和元数据，而不必遵守那个国家的隐私法。在国内，美国政府已经不仅在保密的民事案件中，而且通过秘密的外国情报监控法院(FISC)授权的秘密裁决强迫科技公司交出源代码。至于网络间谍活动的广度和深度，没有国家能比得上棱镜门、方程式组织、ECHELON 或以色列 NSO 集团的飞马间谍软件的窃听或监视操作。

2016 年 11 月通过的《网络安全法》网络安全法(CL)是中国网络监管和执法制度的核心。《网络安全法》源于《国家安全法》，由 79 条法律组成，分七章。这一基本和总括性的“基本法”的关键要点如下:

- **倡导网络空间主权原则**:该法倡导“网络空间主权”的概念，通过建立一个框架来监管中国境内的互联网，并确保技术的安全和可控发展，以加强网络安全。
- **网络运营商和网络产品及服务提供商的安全保护义务**:法律规定网络运营商有义务保护网络免受干扰、破坏或未经授权的访问，并防止数据泄露、盗窃或篡改。至于网络产品和服务的提供商，他们必须遵守“国家标准”，并确保产品安全。“网络关键设备和网络安全专用产品”必须经过更高级别的认证。
- **保护关键信息基础设施(CII)**:该法律将关键信息基础设施宽泛地定义为“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、公共利益的基础设施”，并对关键信息基础设施运营商及其供应商规定了严格的规则。关键信息基础设施运营商在采购网络产品和服务时，还需要与供应商签订安全和保密协议。
- **保护个人信息**:该法律规定了网络运营商的一些数据保护义务，包括以下义务:

  (a)不得泄露、篡改、毁损其收集的个人信息，

  (b)未经被收集者同意，不得向他人提供个人信息，

  (c)删除非法收集的信息并修改不正确的信息。还规定违规行为出现时应按照规定及时告知。
- **数据的跨境传输**:该法律要求关键信息基础设施运营商在中国境内存储在运营过程中收集或生成的“个人信息和重要数据”。出于运营原因需要进行的离岸数据传输应接受安全评估。
- **网络标准化和互操作性**:该法律促进网络基础设施的互操作性，并鼓励企业、机构和大学参与网络安全标准的制定。

《网络安全法》从设计上就具有宽泛和总括性的特点。此后，网络安全监管机构国家互联网信息办公室(CAC)发布了两版实施条例(**《网络安全审查办法》**)，以微调该法的宽泛条款。最新修订的《办法》是 2022 年 1 月由国家互联网信息办公室与其他 12 个机构联合发布的，其中规定了计划在海外上市且拥有超过 100 万用户个人信息的网络平台运营商应考虑的网络安全风险审查因素。“核心数据”或“重要数据”被外国政府恶意使用的风险就是风险审查因素之一。《办法》出台的起因据认为是 2021 年 7 月，滴滴出行不顾中国官员向滴滴提出延期上市和进行网络安全检查的非正式要求而在纽约证券交易所上市。

2021 年 6 月通过的《数据安全法》(DSL)是中国 2016 年 11 月通过的《网络安全法》的补充，是中国数据治理机制三大基本支柱中的第二大支柱。该法的 55 个法条的目的是规范可能涉及国家安全的数据处理活动。《数据安全法》的关键条款有:

- **第二十一条，**根据不同类型的数据对国民经济、国家安全和公共利益的重要性，建立数据分类和分类保护制度来管理数据。该法条引入了一种新的数据类别“国家核心数据”(层级位于“重要数据”之上)，指的是关系“国家安全、国民经济命脉、重要民生、重大公共利益”的数据。国家数据安全工作协调机制负责协调这方面相关机构。
- **第二十六条，**允许对在与数据、数据开发和技术使用有关的投资和贸易等事项上对中国实施歧视性措施的国家和地区采取对等措施。
- **第二十七条**，要求数据处理实体遵守网络安全等级保护制度(MLPS)的数据安全要求，该制度根据网络对国家安全的相对影响对物理上位于中国的网络进行分类。2016 年的《网络安全法》首次引入了等级保护制度。
- **第三十六条**，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。
- **第四十五条和第四十六条**列举了对违反与保护“国家核心数据”有关的要求以及违反关键信息基础设施和非关键信息基础设施数据处理实体跨境传输“重要数据”有关的规则的严厉罚款。

中国基础数据治理制度的第三个支柱是 2021 年 8 月通过的**《个人信息保护法》(PIPL)**。它类似于欧盟的《通用数据保护条例》(GDPR)，特别是涉及域外范围的条款，并侧重于保护处于中国领土的个人和组织的人员信息。根据中华人民共和国国家互联网信息办公室发布的“标准合同”，《个人信息保护法》为处理与跨境传输(即在中国境外进行的数据处理活动)相关的个人信息提供了法律依据，根据数据的*来源*而不是其存储或处理的地点在域外实施管辖权。

《个人信息保护法》列举了个人信息处理者和数据处理者必须遵守的一些数据保护原则——包括合法、公平、必要、诚信(第五条)；目的限制和数据最小化(第六条)；公开性和透明度(第七条)；准确性和完整性(第八条)；安全和问责制(第九条)；有限的数据保留(第十九条)。与此相关的是，它赋予“数据主体”处理其私人信息的各种权利。大型互联网平台运营商承担第五十八

条规定的责任。最后，结论性条款概述了个人和组织因违反《个人信息保护法》可能受到的处罚以及诉讼期间举证责任的分配。

2.“雷声大，雨点大”:中国积极建立数据治理和网络安全法规

2021 年和 2022 年是中国数据治理制度监管建设的繁忙时期，发布了一些基于《网络安全法》、《数据安全法》和《个人信息保护法》条款的草案和最终规则以执行这些法规。

2021 年 7 月初，中共中央办公厅印发了《**关于依法从严打击证券违法活动的意见》，**这在一定程度上是由之前滴滴出行的美国存托股票(ADS)在纽约证券交易所(NYSE)开始(未经批准)交易引发的。2021 年 7 月 10 日，中国国家互联网信息办公室(CAC)发布了**《网络安全审查办法（修订草案征求意见稿）》**。该《办法》的最终版本于 2022 年 1 月 4 日发布。2021 年 10 月，中国国家互联网信息办公室发布了**《数据出境安全评估办法（征求意见稿）》**，在稍作修改后，正式版本于 2022 年 7 月 7 日发布。该《办法》规范了数据处理者的数据出境活动，特别是关于“重要数据”和国内用户个人信息的安全评估的规则。此外，前述**《数据安全法》**和**《个人信息保护法》**也分别于 2021 年 6 月 10 日和 2021 年 8 月 20 日颁布。

最引人注目的是，2021 年 11 月 14 日，中国国家互联网信息办公室发布了一份庞大的包含 75 个条款的《**网络数据安全管理条例（征求意见稿）》**，涵盖了从个人信息保护(第 3 章)到“核心数据”和“重要数据”的安全(第 4 章)，跨境数据流的安全管理(第 5 章)，互联网平台运营商的义务，如对反竞争行为的检查(第 6 章)，数据处理者、网络管理者和国家监管机构的监督、管理和法律责任(第 7 和第 8 章)等内容。该《条例》是欧盟《通用数据保护条例》、《数字市场法案》和《数字服务法案》等法规的结合，最终版本尚未出台。

中国最近在数字监管方面的惊人步伐可能会给人留下这样的印象，即领导层和高级官员注重展示其维护重要数据系统的网络安全和保护国内个人信息完整性的决心。这个解读不完全准确；这些当然是非常重要的考虑因素，但不是全部。**对国内数据和网络安全进行全面、分级和系统性分类的一个基本前提是，要建立一个更为精细的基础，不仅要确保那些(基本)数据要素必须安全可控地存储在中国管辖范围内，还要确保所有其他(非基本)要素可以自由地传输到国外。**从这个意义上说，这一分类系统还兼作负面清单系统，以确保数据要素的稳健和可靠跨境流动，从而促进数字商品和服务的国际贸易。

通常，各种规则和法规中对网络或数据安全进行更严格评估的触发阈值与以下因素相关:

- 数据处理公司处理“重要数据”;
- 数据处理公司寻求海外上市;
- 该方/处理公司/平台运营商是国家机关的云计算服务提供商或关键基础设施的运营商;
- 处理公司/平台运营商为“大型互联网平台运营商”，即日活用户达到 1 亿的平台运营商;
- 平台运营商使用人工智能、虚拟现实和深度学习等新技术开展数据处理活动。

同时，“重要数据”也有了的指导性定义。它包括但不限于:

- 未公开的政务数据、工作秘密、情报数据、执法司法数据;
- 出口管制数据，涉及出口管制项目的核心技术、设计方案、生产工艺及其他相关技术的数据，以及密码学、生物学、电子信息、人工智能等领域的科技成果数据
- 与工业、能源、电信、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域运行相关的数据，以及关键系统组件和设备的供应链数据;
- 人口与健康、自然资源和环境的国家基础数据，比如基因，地理，矿产，气象。
- 其他可能影响国家政治、土地、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、空间、极地、深海等安全的数据。

然而，“重要数据”的定义仍在不断变化。多个政府机构负责确定各自行业和部门中的“重要数据”——如能源、电信、交通、金融等，各自进行自己的意见征集工作。在这一过程中，汽车和金融行业遥遥领先。“重要数据”定义的成熟和固定可能还需要相当长的时间。全面、清晰的“核心数据”的定义可能更加遥远。

3.中国的数据治理机制:初步结论

中国将数据视为独立的“生产要素”，这一做法独特且颇具远见卓识。数据治理和网络安全的方法是自上而下的，由国家以协调一致的方式推动。方法也是全面的，旨在在安全性、隐私性、包容性和商业等相互竞争的因素之间取得微妙的平衡。中央领导层的目标是制定一个深

入、流动和开放的市场的长期参数，在这个市场中，数据要素可以进行有效和可信赖的无缝交易，同时防止数据误用、滥用或成为对抗国家的武器。

尽管这种方式颇具远见卓识，但政府主导的协调方式也并非完美无缺。这主要源于监管者与被监管者之间的沟通不畅。诚然，中国的大型科技公司已经超越了“监管沙箱”时代，需要谨慎监管。但是数字领域的监管措施，虽然推行的晚，却十分雷厉风行和严格。

中国尽管在数据治理和网络安全制度的发展方面取得了开创性的进展，但未来在建设中国国家数据要素市场和数据基础设施系统方面仍有许多细致的工作要做。

二、美国

1.联邦法律层面

自从美国公司开始在全球数字经济中发挥先锋作用以来，美国一直大力推动数据国际间自由流动，将数据国际间自由流动作为首要原则。随着时间的推移，新出现的挑战促使美国监管机构在各个领域设定标准，以平衡行业的增长倾向与个人隐私、负责任的内容审核、打击虚假信息和保护国家安全等问题。然而，传统上的监管工作是针对特定部门的，行业本身承担数据治理的首要责任。只有当数据处理者违反数据流规则和标准时，数据监管者才会介入并惩罚他们。因此，在控制和处理消费者数据的过程中，美国科技巨头享有很大的空间，拥有相当大的自由度和豁免权。

美国监管机构在商业数据流方面设定了标准，但这种标准往往局限于特定的行业或数据类型。例如，1996 年的《健康信息流通和责任法案》(HIPAA)产生了与医疗记录的存储和访问有关的宽泛的隐私标准。美国联邦贸易委员会(FTC)也开始按照 1999 年《格雷姆-里奇-比利雷法案》(GLBA)的要求相对严格地管理金融数据，该法案确立了金融机构存储和保护客户信息的规则。联邦贸易委员会在其他部门执行其他联邦一级的框架，但主要是通过事后惩罚性执行措施。以联邦贸易委员会对广告技术公司 Kochava 的诉讼为例，该公司涉嫌出售精确的地理位置数据，违反了保护客户敏感数据免遭暴露的标准。联邦通信委员会(FCC)在互联网服务提供领域享有类似于联邦贸易委员会的权力，有权处罚管理客户个人信息不当的互联网服务提供商。

除了这些规定数据处理者应如何保护客户个人信息的行业监管措施(大多源自 20 世纪 90 年代通过的法律)，**联邦层面的商业数据最近受到了新的限制，这些限制将国家安全置于纯粹的自**

由放任做法之上。虽然在过去 20 年的大部分时间里，行业利益相关者和政府一直同意需要一个自由和公平的竞争环境，但面对中国等强劲的数字领域竞争对手的发展，美国呼吁在科学和新兴技术等敏感领域制定新的数据流规则。例如，自 2018 年以来，“软件”和“大数据”被定为属于出口管制的范围。这意味着，没有商务部工业和安全局的出口许可证，任何敏感的科学或技术数据都不能传输到美国境外的服务器。2018 年的《外国投资风险审查现代化法案》(FIRRMA)特别指出对涉及“关键和敏感数据”的外国收购和投资进行安全审查。联邦政府远离自由放任政策的另一项举措是 2018 年的《澄清海外合法使用数据法案》（简称“云法案”），该法案允许执法部门通过授权令或传票访问美国通信服务提供商(CSP)的商业数据，无论这些数据是否存储在美国境外的服务器上。

行业利益相关者目前对于如何平衡开放的数据流和日益增长的对消费者隐私和国家安全的担忧颇为矛盾。几个利益相关方的提案或原则在数据监管方面有着共同的主题:公司在使用数据方面的透明度；客户选择退出数据收集的权限；数据安全通知要求；以及联邦贸易委员会在执法中的中心地位。尽管对消费者隐私越来越敏感，科技巨头仍然继续支持立法否定合理隐私标准。行业对监管数据收集和使用的看法可以从他们对加利福尼亚州和弗吉尼亚州数据隐私法的不同态度中看出。加州的法律在一定程度上效仿了欧盟严格的**《通用数据保护条例》(GDPR)**，赋予个人就数据泄露起诉公司的权利，确保能够简单退出所有数据收集，并创建了一个新的州立机构来执行这些措施。亚马逊、微软和优步都向游说反对该法案通过的团体提供了大笔捐款。另一方面，弗吉尼亚州的法律最初是由微软结合亚马逊的意见编写的，不包括私人起诉权，保留了人工选择退出的方式，只授予州司法部长执行权力。虽然行业利益相关者没有完全都去支持约束性较弱的立法 (DuckDuckGo、Yelp 和 Spotify 等公司支持加州的法案)，但最大的参与者对弗吉尼亚州法律的支持具有很大的影响力，大多数州级数据法都在起草过程中反映了弗吉尼亚州的法律，而不是加州的法律(见下文关于“州法律”的部分)。

未来几年，美国对跨境商业数据流动的做法将继续受到历史上自由放任倾向与应对新出现的全球挑战的影响，伴随这些挑战而来的是更多的韧性和与安全相关的政府行动。虽然由于行业利益相关者的作用，立法已经要求一些领域交出了自主权，但这种妥协是为制定更全面、更严格的立法争取时机。虽然数据世界不再由美国公司垄断，但拥有从数据自由流动中获利的重大机会的最大利益相关者仍然喜欢开放的市场，即使自由市场使他们容易受到外国参与者和公众监督的影响。然而，尽管通过行业获得的标准和主要惩罚性执法来监管商业数据的整体模式

可能会继续存在，但随着越来越多的美国数据在美国司法管辖范围之外的服务器上流通，联邦贸易委员会可能会加大在跨境案件中的职权范围和积极性。

由于在联邦层面没有全面的立法或法律框架，**美国通常被认为对数据保护和隐私法律采取“拼凑”的方法。**现有的联邦立法通常侧重于特定的参与者(例如政府机构或特定行业)或特定类型的数据(例如金融数据或儿童在线数据)。此外，有限的几个州颁布了全面的州数据保护立法，但没有迹象表明所有或大多数美国管辖区将颁布效仿。**尽管如此，国会山正在逐渐形成一股关于在联邦层面通过全面隐私立法的声势。**国会议员花了大量时间设计联邦隐私立法，两党合作的《美国数据隐私和保护法案》(ADPPA)可能是最好的例子。《美国数据隐私和保护法案》致力于解决此前困扰隐私法案的两个问题:**是否让个人享有依法起诉科技公司的权利；以及联邦隐私法令是否应该推翻现有的州隐私条例。**关于前者，《美国数据隐私和保护法案》将允许个人起诉科技公司的违规行为，只要他们在提交申请时通知州和地方官员，然后等待两年以落实补救措施。这可以为公司提供喘息空间，纠正相关的不当做法。关于后者,《美国数据隐私和保护法案》将只推翻那些与联邦法律直接冲突的州规则，其他条款保持不变。

回顾过去，美国国内对现代隐私法的需求最早出现在 20 世纪 70 年代。直到 20 世纪 90 年代，美国颁布了许多法律来解决具体的隐私问题，从限制政府访问敏感信息的权限，到特定行业的监管需求，例如金融和医疗行业。**随着时间的推移，这些法律形成了国内数据和隐私保护的基础，或是因为它们被解释为适用于数据和数字化交易，或是因为国会后来专门颁布了修正案，以扩大法律的范围。**

表 1：20 世纪 70 年代颁布的信息隐私法

背景：

- 信息时代的到来产生了保护信息隐私的需求。
- 最高法院决定为信息隐私提供有限的宪法保护，催生了立法行动。

年份	立法	适用范围	相关内容
1970	公平信用报告法案	消费者信用报告和消费者报告机构	消费者报告机构有义务调查消费者有争议的信息，有义务在根据信用报告采取不利行动时通知消费者，有义务仅为该法规定的目的披露信用报告中的信息。
1974	家庭教育权和隐私权法案	接受联邦拨款的教育机构	父母有权检查、审查、质疑和限制披露其子女的教育记录。
1974	隐私法	美国政府	该法案规定了政府机构在收集、维护、使用和传播个人身份数据方面的要求和准则。
1978	金融隐私权法案	美国政府	该法案限制了美国政府获取个人金融信息的权限，美国政府若想获取个人金融信息，除非在执法调查和其他有限的例外情况下，须经过法律通知或个人的书面同意。

小结：

- 这些法律主要关注政府和公共部门行为体。
- 这些早期法律有助于在美国宣传和确立信息隐私的一些基本原则，例如:
    - 个人应有权审查收集到的敏感信息，质疑信息的准确性，并寻求对信息的修改。
    - 只能出于特定目的披露敏感信息，且最好获得个人的(书面)同意。
    - 收集的敏感信息应在一段合理的时间后失效。

表 2：20 世纪 80-90 年代颁布的信息隐私法

背景：

- 对某些行业监管的解除导致需要额外的保护措施来防止滥用个人信息。
- 国会调查了监管特定领域信息隐私的必要性，发现无论是应对特定事件(如一系列滥用公共驾照数据)，还是应对不断上升的风险和担忧(如在线收集儿童信息)，都需要保护信息隐私。

年份	立法	适用范围	相关内容
1984	《有线通讯政策法案》	有线电视行业	“其他条款”的第 631 条规定： • 有线电视运营商应仅在提供有线电视服务需要时收集消费者的个人身份信息。 • 有线电视运营商还必须向消费者提供一份书面声明，说明这些信息是如何收集和使用的。
1994	《驾驶员隐私保护法》	公共驾照数据库	该法案禁止在未经个人明确同意的情况下披露公共驾照数据库中的个人信息
1996	《健康信息流通和责任法案》	患者健康信息	美国卫生与公众服务部有权制定保护患者敏感健康信息的国家标准，并为此目的制定隐私和安全规则。
1998	《儿童在线隐私保护法》	在线收集儿童数据	美国联邦贸易委员会为商业网站和在线服务制定关于收集、使用和披露儿童个人信息的条例和准则。
1999	《格雷姆-里奇-布里利法案》	金融机构	该法案要求相关金融机构向客户披露其信息收集和共享政策，并制定适当的程序来保护客户的敏感信息

小结：

- 保护信息隐私的早期原则现在除了适用于政府和公共行为体之外，还适用于特定行业的私人行为体，如有线电视行业和金融机构。
- 20 世纪 90 年代，相关机构越来越多地承担起为特定行业制定和实施具有约束力的信息隐私和安全规则的责任和权力。

随着 20 世纪 90 年代互联网的使用和商业化的快速发展，美国颁布了许多专门针对数据保护和隐私的法律。其中包括:

- 1998 年《儿童在线隐私保护法》,指导美国联邦贸易委员会(FTC)制定关于收集、使用和披露儿童在线数据的法规和指导方针
- 2002 年《电子政务法》和 2002 年《联邦信息安全管理法》,两部法律均强化了政府在电子传输和存储时代的数据保护和隐私方面的责任。
- 2009 年《健康信息技术促进经济和临床健康法案》,该法案修订了 1996 年《健康信息流通和责任法案》,并扩大了政府对健康信息技术的使用权限。

如前所述，尽管自 21 世纪以来做出了多种努力，全面的数据保护和隐私立法在联邦层面的出现一直很缓慢(直到最近)。**因此，美国联邦贸易委员会(FTC)——美国消费者权利的主要监管机构——已经成为保护消费者数据保护和隐私权的主要机构。除了有限的例外情况[①]，美国美国联邦贸易委员会拥有广泛的权力，可以针对“不公平或欺骗性的行为或做法”，包括“不公平或欺骗性的”数据保护和隐私做法，做出行政裁决并实施补救措施。**例如，联邦贸易委员会裁定，公司受数据隐私和数据安全承诺的约束，并且公司不能对之前收集的个人数据追溯适用重大修订的隐私政策。此外，根据《格雷姆-利奇-布利勒法案》,联邦贸易委员会负责执行《消费者金融信息隐私规则》,该规则对消费者金融信息的使用、披露和收集、隐私通知要求以及数据保护义务等方面进行监管。

总之，数据保护和隐私的联邦法律和法规可以归纳为三类:首先，是 20 世纪 70 年代至 90 年代颁布的信息隐私法，这些法律有助于定义“隐私”的概念以及保护个人隐私权背后的原则，这两者后来都扩展到了数据保护和隐私。第二，20 世纪 90 年代和 21 世纪初针对具体行业的数据隐私法，为政府机构以及儿童的在线数据、健康信息和金融信息规定了具体的义务和责任。最后，由于缺乏全面的数据保护制度，机构层面——主要是通过联邦贸易委员会——出台了一些监管裁决和其他执法行动以填补空白。

① 即公共运营商、非营利组织和金融机构。虽然联邦贸易委员会对消费者权利的保护权限不包括金融机构，但联邦贸易委员会负责根据《格雷姆-利奇-布利勒法案》执行其《消费者金融信息隐私规则》(隐私规则)，因此有权管理与金融机构有关的数据保护和隐私事务。

在推动制定联邦隐私法的同时，**国会内部也在努力推动大型科技公司为其传播的内容和使用的算法承担更大的责任。**例如，从根本上改革 1996 年《通信规范法》第 230 条，该条款保护脸书和谷歌等平台以及网站主机免于为第三方提供的在线内容承担法律责任。这种“中介责任盾牌”最近在两个主要问题上受到了政治右翼和左翼的严厉批评:首先，它为脸书和谷歌等大型科技平台不明确且不一致的审核做法提供了许可证和掩护。第二，这些大型科技没有认真对待平台托管的激增的非法和有害内容，致使受害者往往获得很少或干脆没有获得任何民事补救措施。

有人建议对第 230 条的一些方面进行改革。这些措施包括激励在线平台加强对非法和有害内容的监督；澄清联邦政府对非法内容的执法作用；限制所提供的豁免和/或将特定类型的损害排除在责任保护范围之外；更新平台和在线行为标准；以及创建一个数据访问框架，以监督和监管由人工智能驱动的基于算法的自动决策系统。尽管在国会山，就这些改革达成共识一直很难。

2.州法律层面

在欧盟于 2016 年通过《通用数据保护条例》(GDPR)后，美国加利福尼亚州立法者开始承认，由于新技术和实践的出现，加州的现有法律不足以监管“个人信息的扩散”。因此，加州颁布了《2018 年加州消费者隐私法案》(CCPA)，自 2020 年起生效。《2018 年加州消费者隐私法案》规定了所有行业的数据隐私和保护的全面权利，包括个人有权知道企业如何收集、使用和分享他/她的个人信息，有权删除从自己这里收集的个人信息，以及有权选择不出售个人信息。2020 年 11 月 3 日，《加州隐私权法案》(CPRA)对此作了修订。《加州隐私权法案》对企业施加了额外的数据保护和隐私义务，包括允许消费者阻止企业共享特定的“敏感个人信息”。此外，该法律还创建了加州隐私保护局，以实施和执行加州的数据隐私法。

《加州消费者隐私法案》的颁布促使美国其他一些州颁布了全面的数据保护和隐私法律，这些法律或多或少是以《加州消费者隐私法案》为蓝本的(尽管具体的保护级别和权利各不相同)。截至 2022 年年中，美国已有六个州颁布了全面数据隐私法[②]:

② 需要明确的是，2019 年的《纽约盾牌法》提出了一些数据隐私要求，但主要侧重于数据泄露义务。目前正在进行立法工作，以制定一项全面的州数据隐私法。

- 2018 年《加州消费者隐私法案》和 2020 年《加州隐私权法案》
- 2019 年《纽约盾牌法》（《阻止黑客入侵并改善电子数据安全（盾牌）法案》）
- 2021 年《弗吉尼亚州消费者数据保护法》(CDPA)(2023 年 1 月 1 日生效)
- 2020 年《科罗拉多州隐私法案》(CPA)(将于 2023 年 7 月 1 日生效)
- 2022 年《康涅狄格州数据隐私法》(将于 2023 年 7 月 1 日生效)
- 2022 年《犹他州消费者隐私法案》(将于 2023 年 12 月 31 日生效)

州级监管机构目前正忙于起草拟议中的法规，这些法规将为这些隐私和个人信息保护法注入活力。一些书面意见的截止日期和规则制定听证会定于 2023 年的前几周和前几个月举行。

注意：与中国或欧洲的方法相比，美国的数据治理制度，包括个人信息保护和隐私制度，可以说是既不足又过多。一方面，美国政府极力保护数据不受阻碍地流动(包括不受阻碍的跨境流动)的权利，但在国家层面缺乏全面的数据保护和隐私制度。另一方面，联邦法律系“拼凑”而成，再加上联邦贸易委员会的裁决、行业特定的隐私义务和机构层面的数据保护标准，造成了数据保护和隐私规则交织，也为执法目的的域外适用奠定了基础。与此同时，各州层面有一些执行行为者和框架，尽管它们大体上遵循类似的治理和保护原则。

此外，国家安全考虑占据了更重要的位置。“由外国对手[包括中国]拥有或控制或受其管辖或指挥的人设计、开发、制造或提供的”互联软件应用程序被视为对“美国的国家安全、外交政策和经济”的威胁。根据这一决定，拜登政府于 2021 年 6 月发布了一份与外国来源的互联软件应用程序相关的潜在风险指标清单，作为其“保护美国敏感数据免受外国对手侵犯”行政令的一部分。显然，美国的数据治理制度仍在发展中，行政部门针对抖音的行动和立法部门的措施(如《美国数据隐私和保护法案》)的命运将是美国应对数字前沿快速发展的技术和地缘政治发展的治理方法的重要指标。

第三部分——全球数据治理、跨境数据流和网络安全方法

一、数字商务

2022 年 8 月 18 日,《数字经济伙伴关系协定》(DEPA)成员智利、新西兰和新加坡宣布组建准入工作组，考虑中国加入协定的申请，智利担任工作组主席。中国商务部对这一决定表示欢迎，并表示要进行实质性的谈判，为加入协定做好充分准备。中国早在 2021 年 11 月提交了加入该协定的申请。

《数字经济伙伴关系协定》是首个数字经济协定，由智利、新西兰和新加坡于 2020 年 6 月签署。协定包含 16 个“模块”,涵盖了从数字商业和贸易便利化到个人信息保护、新兴技术和趋势、包容、建立信任、透明度和争端解决的各种规则。《数字经济伙伴关系协定》是亚太地区为数不多但不断增长的独立数字经济协议之一，其他协定包括《新澳数字经济协定》(SADEA)和《美日数字贸易协定》，旨在利用亚太地区电子商务革命的力量。

根据亚洲开发银行(ADB)2021 年 2 月发布的《亚洲经济一体化报告》，亚太地区正处于历史性的电子商务热潮中，在线交易和服务甚至在新冠疫情封锁之前就已经快速增长。总体来看，2019 年全球 B2C 平台(电子商务、在线旅游、广告技术、交通、电子服务和数字媒体)总收入为 3.8 万亿美元，其中 1.8 万亿美元来自亚洲。整个区域的电子商务收入为 1.1 万亿美元，中国占这些电子商务交易的 45%。其他亚太国家也不甘落后。菲律宾、印度尼西亚和越南有望在 2022 年跻身全球增长最快的五大电子商务市场。与世界任何其他主要经济区域相比，亚洲的在线销售在零售总额中所占的比例更大，数字平台的使用及其用户数量也在持续上升。事实上，全球超过一半接触广告技术的互联网用户(使用社交媒体应用程序的用户)都在亚洲。**总体而言，数字经济预计将在未来十年为本区域的国内生产总值增加 1 万亿美元，B2C 电子商务与区域跨境 B2B 电子商务交易将齐头并进。**

数字贸易出口的爆炸式增长——仅在东盟地区，2007 年至 2020 年间，可数字交付的 B2B 服务出口就以每年 16%的速度增长——突显出制定监管这些跨境交易的规则和标准的必要性。

《数字经济伙伴关系协定》是越来越多的数字规则制定倡议之一，更广涵性的优惠贸易协定，如《区域全面经济伙伴关系协定》(RCEP)和《全面与进步跨太平洋伙伴关系协定》(CPTPP)也包含相关内容。通常，这些数字经济协定或贸易协定中有关数字的章节条款可以归为四类:

- 首先，是**旨在促进数字贸易的条款**，如数字产品的非歧视性待遇和取消电子传输关税。这一类别中包括的其他措施是与电子认证和电子签名有关的规则，以及建立不会造成不必要负担的国内监管框架的规则。尽管如此，协定并没有包含具体的监管方法。
- 其次，是**试图限制政府措施范围的条款，从激励的角度来看，这些措施可能会干扰跨境数据流动的增长**。在这方面，最重要的一条是禁止把规定计算设施设在一缔约方的领土上作为在该领土上开展业务的条件。其他条款包括禁止数据本地化和禁止强制传输源代码和专有加密信息(尽管这在数字经济协定中并不统一)。这些条款的目的是消除阻碍数字贸易流动的壁垒。
- 第三类条款是**保护消费者和用户利益**的条款。通常，这些条款包括在线消费者保护、个人信息保护和防止未经允许的商业电子邮件，目的是为数字用户提供隐私和个人信息安全，从而增强他们对在数字平台上从事商业活动的信任。
- 最后一类条款是**维护政府监管数字空间以及在其境内发生或产生的跨境流动的主权**。通常，这些条款分散在相关的协定或章节中，包括安全例外、审慎例外、一般税收相关权利以及以监管自主权为名追求“合法公共政策目标”的例外。

各个数字经济协定，或者说贸易协定中有关数字的章节，都不尽相同。**数字协定中的*黄金标准协定*，如《数字经济伙伴关系协定》(DEPA)**和**《新加坡-澳大利亚数字经济协定》（SADEA）**，与**《区域全面经济伙伴关系协定》(RCEP)** 等*普通协定*相比，包含更严格的规则和标准，例如:

- 《数字经济伙伴关系协定》和《新澳数字经济协定》都包含禁止要求的条款，比如禁止要求共享源代码和/或算法。通常，相关条款声明，任何一方均不得以要求国外供应商转让或获取外国供应商拥有的源代码或软件作为市场准入或国内销售的条件。《区域全面经济伙伴关系协定》没有这项规定。

- 《数字经济伙伴关系协定》和《新澳数字经济协定》都包含禁止数据本地化相关要求的条款，例如禁止要求将处理数据的计算设施设在本地。这方面的典型条款规定，任何一方都不得要求涉事人在该方领土内使用或设置计算设施，以此作为在该领土内开展业务的条件。《区域全面经济伙伴关系协定》在这方面的规定较弱，它(名义上)禁止将要求计算设施设置于一放的领土内作为开展业务的条件，但一项附属条款模糊了这一点，该附属条款指出，各方也可以自由使用关于位置的措施“以确保通信的安全和保密”。
- 《数字经济伙伴关系协定》和《新澳数字经济协定》都包含禁止实施禁止公开加密产品的规定。通常，相关条款声明，对于为商业应用而设计的加密产品，任何一方不得强制或维持技术法规或合格评定程序，把外国供应商与当地实体合作、转让特定技术或生产流程或集成特定当地加密算法或密码作为市场准入或国内销售的条件。《区域全面经济伙伴关系协定》不包含这一条款。
- 《数字经济伙伴关系协定》和《新澳数字经济协定》还包含比《区域全面经济伙伴关系协定》更强硬的措辞，要求各方执行与隐私、消费者保护和网络安全保护有关的国内法律。

二、在数字经济协定中保留“监管权”

尽管数字贸易领域的黄金标准协定和普通协定之间存在差距，但是这种差距不应该掩盖这样一个事实，即这两种类型的协定通常都是用“尽最大努力”的表述，而不是“有约束力”的条款。**鉴于网络领域创新、流程和实践的动态性和流动性，数字经济协定的重点一直是在激励商业跨境数据流动与保留监管这些流动的权利之间达成平衡。**

- 数字经济协定中任何一方都不得要求将转让或获取源代码作为进入市场的条件的条款还包含一项附属条款，该条款不排除政府机构、监管机构或司法机关要求外方保存或提供相关源代码，以供调查、审查以及司法或行政执法行动使用。

- 同样，禁止数据本地化相关要求的规定通常不排除政府机构实施与此类计算设施位置相关的措施，只要这些措施旨在“实现合法的公共政策目标”并且“不施加……超过实现目标所需的限制”。

- 同样，禁止公开加密产品的条例还附有一项附属规定，不妨碍一方的执法机关要求使用加密的服务提供商根据该方的司法程序提供未加密的通信。

这种对监管政策空间的一再顺从，本身就是对数字领域动态和快速变化的监管步伐的屈服——无论是在反垄断保护、隐私和数据保护、金融科技相关的金融稳定风险管理、人工智能(AI)应用规则的制定，还是要求算法系统的结构、使用和影响透明方面。例如，现在监管界越来越接受的是，由于互联网平台依赖基于人工智能(AI)和机器学习(ML)的工具进行内容审核、广告定向和投放以及内容排名和推荐，因此为了分享和使用数据的大众的利益，应该制定法规，允许经过审查的研究人员访问此类平台数据，以确保对平台算法系统的问责。在五年前，制定法规访问这些算法“黑箱”是不可想象的。

随着监管思维的进步，一度被视为标准的语言的中介服务提供商（非）责任等表述，也不再出现在最近的数字经济协议或章节中，即便出现，也越来越受到质疑。美国主导的每一项数字经济协定或谈判（《美国-墨西哥-加拿大协定》；经谈判达成的《跨太平洋伙伴关系协定》；《美国-日本数字贸易协定》）都包含这样一项条款“任何一方均不得采取或维持将交互式计算机服务的供应商或用户视为信息内容提供商的措施，以确定与该服务存储、处理、分发或提供的信息相关的损害的责任。“快进到 20 世纪 20 年代，《数字经济伙伴关系协定》和《新加坡-澳大利亚数字经济协定》都没有明确规定中介服务提供商的责任保护。随着美国于 2017 年 1 月退出《跨太平洋伙伴关系协定》，《全面与进步跨太平洋伙伴关系协定》的剩余缔约方也从其最终文本中删除了关于中间人责任保护的措辞。

华盛顿方面也倾向于反对这种责任保护。随着两党对《通信规范法》第 230 条的批评不断增加（中介责任保护条款就是在该条款的基础上制定的），这一条款在未来由美国主导的数字贸易协定中被取消只是时间问题。印度-太平洋经济繁荣框架(IPEF)贸易支柱的数字章节可能是第一个以美国为首的数字贸易文本，就没有这一条款。

在这种背景下，**国家采取或维持的措施可能与跨境数据流动不协调，但却是"实现合法公共政策目标所必需"的——"合法公共政策目标"的范围不断演变——已成为数字经济协定中的一项程式化或既定原则。**这些"合法公共政策目标"超出了标准的一般和安全例外（包括保护自身"

基本安全利益"的例外），这些例外通常包含在贸易协定中，自 1940 年代末《关税与贸易总协定》制度建立以来，一直是全球贸易体系的重要组成部分。

数字服务税——一个独立的监管领域

2020 年 6 月，美国贸易代表办公室(USTR)依据新 301 条款对奥地利、巴西、捷克共和国、欧盟(EU)、印度、印度尼西亚、意大利、西班牙、土耳其和英国已采用或即将采用的数字服务税展开调查。美国贸易代表办公室认为，这些税收相当于“不公平贸易做法”,即:

- 歧视美国数字公司
- 不符合国际税收原则，如域外适用以及适用于营业收入而非个人收入
- 对美国商业造成负担和限制。

根据(301 条款)法令，301 条款调查中不法行为的门槛是做法不合理。“不合理”的对外贸易做法可能只是一种不公平的做法，“但不一定违反……美国的国际权利。”一旦发现这种贸易做法“不合理”，总统有权实施单边措施，包括关税措施，以抵消不合理的外贸做法的影响。

许多发达国家和发展中国家政府推动征收数字服务税，因为它们希望对在其管辖范围内经营 B2C 数字经济部门的跨国公司的收入和利润征税。普遍的看法是，大型科技公司和其他跨国公司从这些管辖区的消费者那里获得的收入和利润没有被充分征税，也没有被重新分配回这些管辖区。为了补救这一损失，经济合作与发展组织(OECD）领导 136 个国家于 2021 年 10 月签署了一项双支柱税收协定，将跨国公司的一些征税权从其母国分配到它们开展业务活动并赚取利润的市场——无论这些公司是否在那里有实体存在。

在这种情况下，需要注意的重要一点是，数字税收是一个独立的监管领域。它由财政部管理，在很大程度上与负责贸易、商业或数字事务的其他部委保持一定距离。标准数字经济协定通常也指出，“[相关数字贸易协定]中的任何内容都不适用于税收措施”或“影响任何税收协定下任何一方的权利和义务”。

另外，世界贸易组织正在暂停对电子传输(包括从软件、电子邮件、数字电影和音乐到视频游戏的所有内容)征收关税。这项暂停令自 1998 年起生效，每两年延期一次。最近一次延期是 2020 年 6 月在日内瓦举行的第 12 次世贸组织部长级会议上。

三、关于数字商务的多边规则制定

各方始终没能在多边层面将数字贸易相关的请求-提供承诺变为有约束力或最佳努力规则。世界贸易组织的全球电子商务谈判已经进行了将近 25 年，但在这方面几乎没有什么具体的成果。1998 年 5 月的第二次部长级会议通过了一项关于全球电子商务的宣言，使世贸组织总理事会于 1998 年 9 月制定了一个工作计划。此后，世贸组织各机构就电子商务问题进行定期讨论，这些讨论按功能分为四个部分，分别是:

- **自由化**——不对电子传输征收关税；数字产品的非歧视性待遇；通过电子手段实现信息自由跨境传输；禁止数据本地化；市场准入。
- **便利化**——电子签名和认证；电子文件/无纸贸易；获得电子支付解决方案。
- **信任和可靠性**——个人信息保护；防范未经请求的商业电子信息；保护商业秘密，包括源代码和专有算法。
- **透明度**——关于监管措施的公告；技术援助和能力建设。

一些想法相同的世贸组织成员也根据《电子商务联合声明倡议》进行了讨论。根据该联合倡议，占全球电子商务贸易 90%以上的 86 个成员(截至 2021 年 1 月)也一直就电子商务贸易相关方面进行谈判。澳大利亚、日本和新加坡是该倡议的共同召集人。提出的问题分为六个主题:扶持电子商务；开放性和电子商务；信任和数字贸易；交叉问题；电信；和市场准入。

另一方面，20 国集团(G20)国家也在关注此事。在 2019 年 6 月由日本主持的 G20 峰会上，《大阪数字经济宣言》发布，包含“信任的数据自由流动”(DFFT)构想的“大阪轨道”框架启动了。“信任的数据自由流动”的目标是“实现数据的自由流动，同时确保公众对隐私和安全保护的信任。“尽管在概念上很吸引人，但‘信任的数据自由流动’构想未能获得足够的支持，也未能产生具体的结果。印度、印度尼西亚和南非甚至没有签署上述《大阪数字经济宣言》，目前担任 20 国集团主席国的印度尼西亚的数字转型工作的重点是面向平等(缩小数字鸿沟、改善竞争/反垄断政策、数字能力建设援助等)而不是信任的数据自由流动。

多边层面未能就跨境数据流动做出具体承诺，部分原因是这个由 160 多个处于不同国家发展阶段的成员组成的共识驱动型组织的决策过程繁琐。另外，**世贸组织中的主要经济体——美国、欧盟和中国——不仅在电子商务自由化方面采取了不同的做法，而且在监管方面也采取了各种不同的做法。**

例如，美国在数字市场准入和放松监管方面采取了激进的立场。这种监管对国内和跨境流动或多或少是自由放任的(尽管美国联邦贸易委员会的任务是在国内起诉违法行为)。个人和非个人数据的处理没有实质性的区别(尽管随着联邦隐私立法的通过，这种情况可能会改变)。数据的跨境流动只受到非常有限的安全例外的限制，例如不可将敏感数据传输给外国反对势力，以及执法部门无条件访问受美国管辖的机构和个人存储在海外的的数据。

另一方面，欧盟和中国对商业、安全和隐私三管齐下的数据治理的监管方法更具规范性。这在隐私和个人信息保护领域尤为明显。虽然大多数非个人数据或多或少被允许自由跨境流动，但只有当目的地国被认为拥有充分可接受的数据保护制度时，个人数据才能自由跨境流动。此类数据必须通过的安全评估，尤其是关于“重要数据”的安全评估，包括的范围也更广、更严格(尽管它不是针对对手的)。在国内监管框架——特别是在安全和隐私框架方面——进一步统一之前，跨境数字贸易自由化流动相关规则融入多边层面仍将十分艰难。

四、全球网络安全规范

2015 年 9 月 24 日至 25 日，美国前总统巴拉克·奥巴马(Barack Obama)接待了习近平主席的国事访问，两国元首就一系列全球、地区和双边议题交换了意见。这次国事访问的主要成果之一是网络安全承诺，特别是关于恶意网络活动的承诺。双方同意，两国政府都不会为了给公司或商业部门提供竞争优势而进行或故意支持通过网络窃取商业秘密或其他机密商业信息等知识产权的行为。双方还承诺共同努力在国际社会中进一步确定和促进网络空间国家行为的适当规范。为落实该谅解，双方建立了打击网络犯罪及相关问题的高级别联合对话机制，美国国土安全部部长和美国司法部长在美国方面主持对话，中国公安部、国家安全部和司法部推选部长级官员在中国方面主持对话。

2015 年 9 月的谅解是美中网络安全关系的巅峰。自那以后，双边网络安全关系或多或少一直在下滑，特别是特朗普政府当选后。在国际社会范围内共同确定和促进国家在网络空间行为的适当规范的双边努力基本上以失败告终。**大量政府间和非政府倡议填补了这一空白，以应对*网络不安全*，特别是利用商业信息技术系统开展恶意网络活动带来的挑战。**

以下是一些比较著名的加强国际网络安全规范的政府间和非政府工作组、倡议和提案:

（1）联合国信息通信技术不限成员工作组(OEWG):2021 年 3 月，信通技术 OEWG 发布了网络空间负责任国家行为最终共识报告。报告指出，信息和通信技术的发展对联合国工作的三大支柱(和平与安全、人权和可持续发展)都有影响，并建议在若干问题领域实施一些自愿的、不具约束力的规范。这些是:

- 信息安全领域的现有和潜在威胁以及为应对这些威胁可能采取的合作措施；
- 进一步发展国家负责任行为的规则、规范和原则的手段；

- 国际法应如何适用于国家对信通技术的使用；
- 信任构建措施；
- 能力建设措施；
- 以及在联合国支持下建立广泛参与的定期机构对话的可能性。

在这方面一项重要建议是，各国不应开展或故意支持违反国际法规定义务的信通技术活动，故意损坏关键基础设施或以其他方式破坏用于向公众提供服务的关键基础设施的使用和运行。此外，各国应继续加强措施保护所有重要基础设施免受信通技术威胁，并增加关于此类重要基础设施保护最佳做法的交流。

（2）网络空间信任和安全巴黎倡议《巴黎倡议》是由法国总统埃马纽埃尔·马克龙（Emmanuel Macron）于 2018 年 11 月在联合国教科文组织和巴黎和平论坛举行的互联网治理论坛期间发起的一项公私联合努力。该倡议旨在将网络空间的利益相关者聚集在一起，共同努力采取负责任的网络行为，并实施适用于现实世界的原则。在这方面，还提出了网络空间监管的愿景，以及九项具体原则供采纳。《网络空间信任和安全巴黎倡议》的九项原则是:

- **原则一 保护个人和基础设施**——防止恶意网络活动对个人和关键基础设施造成重大、任意或系统性损害并对已造成的损害进行修复。
- **原则二 保护互联网**——防止故意严重损害互联网公共核心的可用性或完整性的活动。
- **原则三 保护选举进程**——加强能力，防止外国行为体恶意干预，通过恶意网络活动破坏选举进程。
- **原则四 保护知识产权**——防止通过信通技术窃取包括商业秘密或其他机密商业信息在内的知识产权，从而为公司或商业部门提供非法竞争优势。
- **原则五 恶意软件和做法不扩散**——开发方法防止恶意软件和伤害性做法扩散。
- **原则六 加强数字生命周期安全性**——加强数字流程、产品和服务在其整个生命周期和供应链中的安全性。
- **原则七 支持网络卫生**——支持所有参与者提高网络卫生水平。

- **原则八 禁止私人黑客入侵**——采取措施防止包括私营部门在内的非国家行为体出于自身目的或代表其他非国家行为体进行黑客入侵。

- **原则九 促进国际网络规范**——促进负责任行为国际规范以及建立信任措施在网络空间的广泛接受和实施。

在撰写本报告时，“巴黎倡议”得到了 81 个国家以及许多私营部门实体和民间团体组织的支持。

(3)全球网络空间稳定委员会(GCSC): 全球网络空间稳定委员会于 2017 年 2 月启动，在《网络空间稳定性》系列报告发表后，于 2021 年 12 月结束活动。该委员会的目的是促进致力于国际网络安全相关问题的各个网络空间团体之间的相互认识和理解。全球网络空间稳定委员会通过将国际安全对话与网络空间创造的新团体联系起来，以支持与网络空间的安全和稳定有关的政策和规范的一致性。2019 年 11 月，全球网络空间稳定委员会发布了一份详细的最终报告，提出四项指导原则(承担责任；克制自身；行动要求；尊重人权)和六项建议。这些建议是:

①国家和非国家行为体应通过加强克制和鼓励行动，采纳和实施提高网络空间稳定性的规范。

②国家和非国家行为体必须根据其责任和局限性，对违反规范的行为做出适当反应，确保违反规范者面临可预见和有意义的后果。

③国家和包括国际机构在内的非国家行为体应加大工作人员培训和建设能力的力度，促进对网络空间稳定重要性的共同认识，并考虑到各方的不同需求。

④国家和非国家行为体应收集、分享、审查和公布关于违反规范行为及其影响的信息。

⑤国家和非国家行为体应建立和支持利益共同体，以确保网络空间的稳定。

⑥建立一个常设的多利益主体参与机制来解决稳定性问题——在这个机制中，国家、私营部门(包括技术群体)和民间团体都要充分参与并发表意见。

联合国不限成员工作组(OEWG)、网络空间信任和安全巴黎倡议以及全球网络空间稳定委员会(GCSC)只是全球网络安全治理领域中一些较为突出的举措。

虽然这些举措获得了足够多的参与，但与数字商务领域的多边规则制定情况类似，它们未能在可操作的可交付成果方面产生具体结果。他们的提议通常是以自愿的、非约束性的条款表达的，并且将一直如此。在多边治理面临二战结束以来最大压力的时候，很难想象主要的发达国家和发展中国家参与者以及非政府行为体能够在中短期内在这方面取得重大进展。网络安全的全球规则必然要在发展和完善一系列规则和标准的基础上实现，这些规则和标准由主要经济参与者在国家层面执行，并在区域层面实现多元化。眼下，私营部门应该参与者参与，和公共部门携手合作，共同保护技术系统和关键基础设施免受攻击。

第四部分——结论：寻找数据安全定律的途中

1950 年艾萨克·阿西莫夫提出“机器人三定律”的时候，虽然人工智能领域仍是一片荒芜，但“三定律”确实在半个多世纪后，成为人工智能逻辑设定时需要参照的最重要的原则之一。

人工智能与数据治理和安全密切相关，数据治理和安全也需要努力找到本领域能影响半个多世纪发展的定律，这样对公司、行业以及国家来说都有裨益。而通过前面三章的周密研究，我们努力从中找出一些规律的影子。

——数据治理和安全是为信息产业的健康发展和全球繁荣服务的。

信息技术革命带来的全球化浪潮，已经将全球紧紧联系在一起。在经历了大约 30 年狂野西部式的块速发展后，数据治理和安全是在以滞后的方式对监管与合规进行总结。现在从网络基础设施硬件提供商到社交网络服务商，从手机生产商到智能汽车制造商，越来越多的行业和企业都遇到了数据治理和安全问题，明确了数据治理和安全才能更有利于这些行业的发展。

美国的数据治理可以追溯到上世纪 70 年代起陆续出台的一系列健康信息、儿童信息等垂直领域的保护规则，并随着技术的发展将这些规则在大数据时代以新的技术方式进行适配和应用。而中国的数据治理体系则是近十年来陆续发展起来的，从一开始针对的是数据时代的规则，并将数据治理的规则实施到各细分领域中。中美两国数据治理体系形成的顺序虽有差异，但都是为了让数据规范地发挥作用，更好促进产业的发展。

——在不违背第一条的前提下，管控好双边和多边跨国数据治理和安全中的差异。

如之前研究所展现的，中美欧各方当前在数据治理和安全方面政策框架存在大量不同之处。和数据收集使用引发的问题可能成为中美间爆发争端的潜在领域，在这方面要加强沟通与互信，对可能的冲突做好管控。从 2021 年美国政府发布报告称中国政府支持了对美国天然气管道运营

商的网络攻击，到 2022 年中国称美国国安局针对中国西北工业大学的网络攻击行为窃取超 140GB 数据，数据安全相关问题越来越多出现在外交场合中，以低烈度对抗性的方式展现出来。

美国将中国视为网络安全领域的威胁，中国则表达强烈不满的坚决反对，这已形成数据安全领域一种常见的“刺激—反应”模式。从目前看对于这类数据争端难以完全避免，但可行的方式是以最大公约数的方式商定数据安全的底线规则，将相关争端限制在信息与通讯技术（ICT）层面上，防止影响外溢和激化。

——在不违背第一条和第二条的前提下，寻求数据治理和安全方面的合作。

中美都是网络攻击的主要受害国，也是全球数据治理和安全规则的主要制定方，这是书房进行合作的主要契合点。

数据治理与安全的合作是长期的，因为受到技术驱动，数据领域处于快速发展变化中，合作也需要逐步建立；数据治理与安全的合作是广泛的，在关键基础设施和个人信息保护、企业境外数据存储和调取、供应链安全等多个领域都可以推进，在一个方面合作受阻时可以寻求在其他方面取得进展；数据治理与安全的合作是脆弱的，受主权、安全和监管的影响，需要不断调整才能维持。

这项关于数据治理和安全研究或许并不能成为类似“机器人三定律”的伟大预言，但希望至少能为新的数据安全定律的形成奠定一些基础。（完）

参考文献

[1] *Work Programme on Electronic Commerce, Draft Ministerial Decision of June 16, 2022*, WT/MIN(22)/W/23, World Trade Organization, June 16, 2022, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/W23.pdf&Open=True.

[2] Patrick McGee, "US regulator sues data broker over sale of location information," *Financial Times*, August 29, 2022, https://www.ft.com/content/c37668b7-d2f7-4784-99eb-a06255d78cc8.

[3] "Framework for Responsible Data Protection Regulation," Google, September 2018, https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf.

[4]"The 10 Principles of Data Privacy," U.S. Chamber of Commerce, September 21, 2021, https://www.uschamber.com/technology/data-privacy/the-10-principles-of-data-privacy.

[5]Lulu Chang, "Amazon, Microsoft, Uber donate to oppose the California Consumer Privacy Act," *Digital Trends*, June 17, 2018, https://www.digitaltrends.com/computing/tech-opposes-california-privacy-act/.

[6]Todd Feathers, "Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious," *The Markup*, April 15, 2021, https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious.

[7]Ibid., Diane Bartz, "U.S. bill to rein in Big Tech backed by dozens of small and big companies," *Reuters*, June 13, 2022, https://www.reuters.com/technology/dozens-companies-small-business-groups-back-us-bill-rein-big-tech-2022-06-13/.

[8]*Data Protection Law: An Overview*, R45631, Congressional Research Service, March 25, 2019, https://crsreports.congress.gov/product/pdf/R/R45631.

[9]*Fair Credit Reporting Act*, 15 U.S.C. §§ 1681-1681x, Federal Trade Commission, August 2022, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

[10]Daniel J. Solove and Woodrow Hartzong, *Breached!: Why Data Security Law Fails and How to Improve It*, Oxford: Oxford University Press, 2022.

[11]"Facebook, Inc., In the Matter of," FTC File Number 092 3184, Federal Trade Commission, April 28, 2020, https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter.

[12]"California Consumer Privacy Act (CCPA)," Office of the California Attorney General, https://oag.ca.gov/privacy/ccpa.

[13]"Digital Economy Partnership Agreement Joint Committee commences Accession Working Group for China," Ministry of Trade and Industry of Singapore, August 18, 2022, https://www.mti.gov.sg/Newsroom/Press-Releases/2022/08/Digital-Economy-Partnership-Agreement-Joint-Committee-commences-Accession-Working-Group-for-China.

[14]*Asian Economic Integration Report 2021: Making Digital Platforms Work for Asia and the Pacific—Highlights*, Asian Development Bank, 2021, https://www.adb.org/sites/default/files/publication/674421/aeir-2021-highlights.pdf.

[15]"DEPA text and resources," New Zealand Ministry of Foreign Affairs & Trade, 2020, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/.

[16]“Singapore-Australia Digital Economy Agreement (SADEA),” Ministry of Trade and Industry of Singapore, 2022, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.

[17] “Regional Comprehensive Economic Partnership (RCEP),” ASEAN Secretariat, 2019, https://rcepsec.org/legal-text/.

[18]“U.S.-Japan Digital Trade Agreement Text,” Office of the U.S. Trade Representative, October 7, 2019, https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text.

[19]“Section 301 – Digital Services Taxes,” Office of the U.S. Trade Representative, https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes.

[20]“International community strikes a ground-breaking tax deal for the digital age,” Organisation for Economic Co-operation and Development, August 10, 2021, https://www.oecd.org/tax/beps/international-community-strikes-a-ground-breaking-tax-deal-for-the-digital-age.htm.

[21]“Work Programme on E-Commerce,” World Trade Organization, 2022, https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm.

[22]*Osaka Declaration on Digital Economy*, World Trade Organization, June 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf.

[23]Deborah Elms, D*igital Sovereignty: protectionism or autonomy?,* Hinrich Foundation, September 2021, https://static1.squarespace.com/static/5393d501e4b0643446abd228/t/615f394c5533a623afeac00b/1633630545286/Digital+sovereignty+protectionism+or+autonomy+-+Hinrich+Foundation+-+Deborah+Elms+-+September+2021.pdf.

[24]"FACT SHEET: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[25]*Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report*, A/AC.290/2021/CRP.2, UN General Assembly, March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[26]"Paris Call: For trust and security in cyberspace," Paris Call, November 12, 2018, https://pariscall.international/en/.

[27]*Advancing Cyberstability: Final Report*, Global Commission on the Stability of Cyberspace, November 13, 2019, https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.