Open Journal of Legal Science 法学, 2023, 11(3), 1293-1301
Published Online May 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.113185

Hans汉斯

论数据跨境流动安全保护的实践与思考

孙陈铭

宁波大学法学院，浙江 宁波

收稿日期：2023年3月8日；录用日期：2023年3月21日；发布日期：2023年5月23日

摘　要

网络信息化时代的到来，使得数据跨境流动日益频繁。数据跨境流动带来的问题，不仅仅是世界经济飞速发展等益处，还有各类数据安全保护不当需要面临的挑战。目前，世界各国(地区)政府纷纷出台政策措施应对数据跨境流动问题，如欧盟设立“充分性认证”、日本提出“可信数据自由流动”倡议等。数据安全作为新兴的非传统安全问题，我国应当坚持数据安全流动的基本立场，积极融入数据治理国际合作，健全建立数据跨境流动统一立法，主动加入数据全球化治理进程。

关键词

数据安全，数据保护，数据主权，数据跨境流动

The Practice and Thinking of the Cross-Border Flow Security of Data

Chenming Sun

Law School of Ningbo University, Ningbo Zhejiang

Received: Mar. 8th, 2023; accepted: Mar. 21st, 2023; published: May 23rd, 2023

Abstract

With the advent of the era of network information, the cross-border flow of data has become increasingly frequent. The cross-border flow of data brings not only the benefits of the rapid growth of the world economy, but also the challenges of improper protection of all kinds of data. At present, governments of all countries (regions) around the world have introduced policies and measures to deal with the problem of cross-border data flow, such as the establishment of “Adequacy Decision” by the European Union and the “Data Free Flow with Trust” initiative by Japan. As an emerging non-traditional security issue, China should adhere to the basic position of data security flow, actively participate in international cooperation in data governance, improve and estab-

文章引用: 孙陈铭. 论数据跨境流动安全保护的实践与思考[J]. 法学, 2023, 11(3): 1293-1301.
DOI: 10.12677/ojls.2023.113185

lish unified legislation on cross-border data flow, and actively participate in the process of data globalization governance.

Keywords

Data Security, Data Protection, Data Sovereignty, Data Cross-Border Flow

1. 引言

随着大数据时代的来临，网络安全逐步发展成为国家安全的重大问题。数据作为数字时代网络的核心要素，在国家的现代化进程中，各国也开始将数据作为新的博弈领域。然而，在数据快速增加的情况下，全球一体化的速度也随之加快，过高的数据安全风险也成为大数据时代亟需解决的当务之急。2021年6月10日，作为我国首部关于数据安全的法律，《数据安全法》出台了，该部法律不仅是对中国倡导的网络空间命运共同体理念的践行，还是中国为全球数据治理贡献的中国方案与智慧。《数据安全法》的颁布，进一步完善了我国的网络和信息安全法律制度。数据安全主要侧重于防止通过入侵或泄漏而对数据进行未经授权的访问。数据安全作为大数据新时代的主题，对数据开展科学有效的安全治理，实现数字经济的持续、健康发展，是当前国民经济和社会发展的一个重大课题。其中，《数据安全法》第9条规定了国家意图推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作。下文主要通过对政府、企业和个人三种层面探讨我国数据安全保护的实践，并思考我国现有析数据安全保护法律制度的完善问题。

2. 数据安全的概述

2.1. 数据安全的概念及其性质

2.1.1. 数据的概念

数据具有跨多学科性质的特点，在计算机科学、传播学等方面都有所包含，因此，其概念在计算机系统、信息领域都有所关联。而在法律领域，专家学者对于数据的概念研究虽多，但未达成统一的认识，差异较多，需要进一步理清数据的法律概念。

根据计算机科学的定义，在现代计算机系统中，数据的表现形式已并不局限于数字，也常以文本、图像、音频、视频等多种表现形式呈现，但数据的本质仍然是一种“用于描述事物的符号记录”，只有经过解释，其含义才能获得说明[1]。该种观点即将“数据”与“信息”两种概念相区分，二者作为载体和本体的关系，在计算机科学和传播学中的定义也具有极强的学科专属性。然而，其他学科对“数据”与“信息”概念的相关特征描述能够为“数据”的法律概念提供一定的基础。

在法律领域，“数据”的概念显然不同于其他场合和学科的特定含义和适用范围。从近些年国内外有关“数据”的立法情况来看，“数据”与“信息”的概念逐渐趋于同质性，例如，在国外的相关立法中，2018年欧盟出台的有关个人数据的收集、处理、使用和存储的新法规《通用数据保护条例》(GDPR)中第4条规定，“个人数据”是指任何已识别或可识别的自然人相关的信息；2018年通过的美国最健全的数据隐私法之一《加州消费者隐私法案》第1798.140(q)中“对消费者信息”的处理系指对

“个人数据”或“个人数据集”进行的任何一个操作或一组操作。在我国，2021 年 9 月 1 日正式施行的《数据安全法》中，第 3 条将“数据”定义为任何以电子或者其他方式对信息的记录；2021 年 11 月 1 日施行的《个人信息保护法》中第 4 条将“个人信息”规定为以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。从上述立法中可以看出，目前国内外的立法趋势已不再局限于将“数据”与无意义的计算机符号划上等号，而是逐渐承认“数据”与“信息”具有同质性。因此，有学者指出，“数据”与“信息”的概念区分没有绝对的意义，在网络信息化的背景下，二者可以互相转换，几成一体[2]。

2.1.2. 数据安全的概念

随着数字时代的来临，世界各国对于数据及其安全日渐重视，但是，基于各国国情的差异性，对于数据问题的核心关注重点也各有不同。对于数据安全的定义，目前并不存在统一的认知与权威概念界定。各国对于数据安全的理解总体上与其发展阶段和程度息息相关。然而，不可否认的是，数据安全与所有的安全问题具有相同之处，也就是说，它的实质是一种动态的、平衡的、相对的安全。我国《数据安全法》第 3 条对“数据安全”作了一个界定，即指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。根据这一定义，本文认为，数据安全作为一个状态，需要保证数据的完整性、可用性和机密性，防止在未经授权的情况下被个人或者组织通过各种手段和措施使用或者访问数据。实践中，“数据安全”通常需要关注以下两个方面：一方面是信息系统，如计算机系统、网络和软件；另一方面是通过信息系统进行记录、存储、处理、共享、传输的数据、消息和信息[3]。

2.2. 数据安全的分类

2.2.1. 特别数据安全与一般数据安全

根据数据安全级别进行划分，可以将数据安全分为一般数据安全、重要数据安全和核心数据安全。

《网络数据安全管理条例(征求意见稿)》中第 73 条对重要数据和核心数据的概念进行界定。重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据，具体可以包括为未公开的政务司法数据、出口管制数据、科学技术成果数据、重要行业业务数据、重点行业和领域数据、达到规定的自然环境基础数据、国防数据以及其他重要数据。核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据。除了重要数据和核心数据外，对于其他普通数据的安全保护则是一般数据安全保护。

2.2.2. 政务数据安全、商务数据安全与个人数据安全

根据数据安全的主体进行划分，可以将数据安全分为政务数据安全、商务数据安全与个人数据安全。

我国《数据安全法》虽然未对“个人数据”所作定义，但是从《数据安全法》的体系中可以看出，将“政务数据安全与开放”作为单独的一章，显然是不同意将“数据”的范围限缩在“个人数据”这一范畴的。根据其规定，可以将“政务数据”理解为“国家机关为履行法定职责的需要而收集和使用的数据”。对于商务数据的界定，可以参考 2008 年商务部发布的《网上商业数据保护指导办法(征求意见稿)》中对“网上商业数据”的定义，即“在电子商业活动中产生的、以数字格式存在于互联网的商业信息，如企业财务和经营决策信息、客户个人信息、市场竞争信息、交易记录等”。根据该定义可以看出，商业数据包含个人数据和企业数据[4]。具体而言，商业数据为企业等商业主体在其生产经营活动中存储、整理的大量具有商业价值且不具有识别性的数据[5]，其数据主体是个体工商户、企业、非企业组织等商业主体。

3. 数据安全面临的挑战

在网络信息化数据时代，数据已经成为一种广泛性的存在，对其进行的安全维护更是一个严密、复杂的系统。目前，数据安全面临的主要问题可以划分为数据确权难题、数据垄断困境、数据泄露危害以及数据造假隐患这四类。

3.1. 数据确权难题

强化数据要素赋能，有效维护数据安全之际，首先需要解决的是数据确权问题。国家虽然早已多次提出数据确权的要求，但关于数据的权属认定，目前在相关数据立法中仍留存空白。关于数据确权，即对数据权的内容、权属、权力体系和治理机制等作出明确规范。目前，对于数据确权存在两种理论，一种是将其置于现有的制度规范中予以考察，一种是在现有制度外设立新型的数据财产权。然而，这两种理论并无法解决数据确权的困境。数据确权的困境植根于以意志论、利益论为代表的传统权利理论无法解释新的数据问题[6]。另外，不同主体之间面对着不同程度的数据确权问题。对于国家而言，数据确权问题即数据主权问题，与主要强调的是国家对数据的主权，具体涉及数据的安全管控能力和强化国家特殊和核心数据的资源保护能力等方面。在实践中，针对如何有效维护数据安全、平衡数据开放、共享跨境流动数据的问题存在着不同的分歧。而对于商业和个人而言，数据确权问题就归属于数据的产权问题。但对于涉及的数据特征、数据权利性质的内容以及权力配置结果等方面的重要问题，学界尚未达成统一认识。数据确权问题难以达成统一的规范或者解决方案，需要各国“因地制宜”，根据各国的发展情况制定出相应的解决办法。

3.2. 数据垄断困境

2021 年国务院印发的《国务院反垄断委员会关于平台经济领域的反垄断指南》，对于“数据”这一关键词的频率高达 18 次之多，这表明数据垄断问题在我国已经成为重点关注的核心问题。对于数据垄断的问题，可以将其归纳成为三个系列问题，一是数据增强市场力量，一些企业通过收集、利用数据的途径，研究分析用户或者消费者的喜好，从而提供更加优质的服务，促进市场效率，提高竞争优势。二是数据是否需要作为必要措施，当企业拥有市场力量的前提下，对于企业收集拥有的数据，需要进一步考虑该数据是否应当视为必要措施向其他竞争对手开放。目前，现实中部分企业垄断或支配了数据，并且拒绝向其他企业开放，这就更加造成了数据垄断问题的严重性。三是数据与隐私保护问题，企业在收集、利用数据给用户或者消费者提供个性化服务的同时，也增强了对用户或者消费者的支配能力，此时，用户对于个人隐私的控制能力也削弱了。

3.3. 数据泄露危害

数据泄露是当前数据时代全球共同关心的重要问题之一。互联网给人们生活带来便利的同时，也让数据泄露事件频繁发生，具体包括工业制造、政务数据、军工情报、商业数据、个人数据等方面。数据的泄露，不仅侵犯了网络用户个人信息和隐私，用户被欺诈风险大大增加，网络犯罪屡见不鲜；对于企业而言，数据泄露损失的不仅仅是企业的经济利益，还会产生更多严重的社会问题，如高管可能面临一定的司法责任；对于国家而言，相关政务数据、军工情报的泄露，对国家造成严重的危害，政权安全与主权问题遭受冲击，这更是造成不可挽回的结果。

3.4. 数据造假隐患

数据造假问题目前已成为社会各界广泛关注的问题。首先，数据造假问题已经不断出现在社会多个

领域，如金融数据领域、环境监测领域。在最近全面热潮的短视频平台、电商平台等数据也存在着许多造假现象。不仅如此，在政府有关民意调查中，数据造假事件[1]也出现在公众的视野，大大降低了政府公信力问题。这些行业数据造假行为，让依赖于数据真实性的公众的信任大大降低，严重影响行业发展，影响政府机关对于民众反馈的宏观判断与政策颁布。其次，在人工智能发展中，大量的数据应用于计算机的算法中，真实、有效的数据是保障人工智能正常发展的重要前提。倘若数据篡改或者造假问题出现在人工智能发展中，不仅会造成人工智能发展的落后，还会有更多的问题随之发生。再次，数据造假问题可能会产生新的犯罪手段。现如今，个人信息与数据充斥着人们生活中的方方面面。提供便利的同时，也使得犯罪滋生有机可乘。通过利用人工智能技术对个人信息进行替换、合成，从而破坏个人数据的唯一性和专属性。这不仅容易导致个人身份与信息盗用，还会滋生各种违法犯罪活动，侵害被盗用信息人或者他人的权益。

4. 数据安全保护的主要实践

根据上文分析，数据安全面临着严峻的挑战，使得数据安全问题更加复杂。数据问题不仅涉及主体多元化，覆盖领域面广泛。不仅仅是国家，企业、个人都是数据安全维护的主要实践者，各个的主体专注不同的领域，彼此之间又相互联系，共同维护稳定的数据安全状态。

4.1. 国际层面

目前，全球化背景下，各国数据的跨境流动是实现经济与技术等全球化发展的必备要件。各国不断地通过机制对接，寻找流动与安全的平衡点。因此，数据跨境流动的规制尺度成为数据安全保护的核心问题。在目前阶段，各国基于各国国情的差异、追求的利益与价值观的不同，短期之内无法在联合国或者 WTO 等多边机制的框架下形成各方统一认可的数据流动规则，更不用说形成数据安全规则。但是，各国在基于数据跨境流动背景下数据安全理念的扩散，对于各国探索实践的数据安全规则也在不断制定。

4.1.1. 个人数据的保护

欧盟的 GDPR 从《OECD 指南》逐步发展而来，确立了被称为“世界上采用最广泛的个人数据保护模式”。GDPR 不仅为欧盟个人数据安全提供了有力的保障，有利于防止第三国或国际组织因为对个人数据立法保护水平的差异而造成的对个人数据权利的侵害。虽然各国对于保护的力度各有不同，但大多数国家在国内立法中都在不同程度上适用其原则。此外，在美国的推动下，亚洲太平洋经济合作组织跨境隐私保护规则(CBPR)体系建立，旨在增强个人信息保护机制。在 CBPR 体系下，违反数据保护规则的企业由本国隐私执法机构依照 CBPR 的规定对其进行制裁，企业所属国的隐私执法机构必须通过 CBPR 体系的认证。

4.1.2. 设立数据安全门槛

欧盟 GDPR 通过设立“充分性认证”规则，创建了能够使数据可以自由跨境流动的白名单。白名单上的国家或地区，均已通过欧盟“充分性认证”，具有充分的数据保护水平，其数据之间可以自由流通。除此之外，欧盟限制成员国境内的个人数据向境外传输。目前，通过欧盟充分性认证的国家或地区共有十三个。GDPR 这一做法，在一定程度上为数据的跨境流动设立了“门槛”，进一步起到了保护数据安全的效果。

4.1.3. 兼顾发展与安全的治理框架

作为日本主推的倡议，“可信数据自由流动”已通过 G20 机制并得到了美国与欧盟的认可。在大阪

[1]《安徽省委对亳州市及涡阳县平安建设满意度调查弄虚作假问题严肃问责》，载安徽纪检监察网 2021 年 12 月 22 日，http://www.ahjjjc.gov.cn/ywbb/p/99618.html。

G20 峰会中，日本将数据和数据流动作为核心议题重点推动。2019 年 6 月，G20 贸易与数字经济部长会议重申可信数据自由流动的概念，强调跨境数据流动对促进生产率、创新和可持续发展的重要性。“可信数据自由流动”的倡议，旨在建立消费者和企业之间对数据的保护和安全的信任以及鼓励不同法律框架之间的可操作性。

4.1.4. 全球数据安全倡议

针对全球数据安全领域复杂的国际形势，2020 年 9 月 8 日，中国提出了《全球数据安全倡议》(以下简称《倡议》)，为全球数据安全治理提供方案。该《倡议》期望通过一系列举措，与各方一起共同加强数据安全、个人隐私和国家安全的保护，促进各个国家加强对网络和数据安全的关注。2021 年 3 月 29 日，中国外交部与阿拉伯国家联盟秘书处召开中阿数据安全视频会议，宣布共同发布《全球数据安全倡议》，共同应对数据安全风险挑战。作为全球范围内首个与中国共同发布数据安全倡议的国家，体现了阿拉伯在数据安全保护问题上的意识与中国高度的统一。

4.2. 国家层面

目前，数据安全的重要性日渐显现，各个国家在数据安全保护方面做了许多可能的尝试。以我国为例，主要从以下三个方面对数据安全保护进行实践。

4.2.1. 推进数据本地化措施

随着互联化进入自由发展阶段后，越来越多的数据信息被非法收集、利用发生，出于对国家安全和公民隐私的保护，一些国家陆续出台了数据本地化措施。对于数据本地化，目前尚不存在统一的概念，通常包含了数据中心本地化和数据本地措施两种措施。数据本地化，是为了限制自己国家境内的数据流动，甚至是阻止自己国家的数据对外流出。在我国现有的法律制度下，各种法律法规中都存在着数据本地化的规定。如《国家安全法》《网络安全法》《个人信息保护法》《数据安全保护法》等中，都提出了对数据本地化的明确要求。

4.2.2. 加强数据跨境流动规制

基于对本国数据安全保护的考虑，各国对本国数据对外传输采取相应规则予以限制。具体表现为需经数据主体同意或特殊数据经过审批后才能对外输出。如 2021 年国家互联网信息办公室起草的《数据出境安全评估办法(征求意见稿)》中，要求数据处理者向境外提供数据之前，需要进行安全评估，对于对外传输数据给国家安全、公共利益、个人或者组织合法权益带来的风险，不得出境。

4.2.3. 围绕“长臂管辖”展开较量

长臂管辖的本质是属人管辖权，其概念首次在美国的民事诉讼中被提出。在数据安全领域，长臂管辖主要涉及的是网络犯罪的数据信息取证问题。网络犯罪因其具有的特殊性，为保证能够顺利对数据的取证，防止数据转移，避免正常审批流程周期过长不利于本国的司法审查，而采用长臂管辖。虽有解决网络犯罪数据转移过快的合理之处，但是在一定程度上会产生损害国家主权争议问题。例如，2018 年美国通过了《澄清合法域外使用数据法》(简称 CLOUD 法案)，CLOUD 法案授权美国监管、执法、司法部门通过国内法律程序调取美国公司储存在境外的数据，同时也允许其认可的、“适格的外国政府”直接向美国公司调取数据用于侦查执法以换取这些国家放弃数据本地化的要求[7]。这样的做法容易导致在实践中引发各国司法管辖权冲突的问题。对此，各国采取了相应的对策。以我国为例，2021 年 1 月 9 日出台的《阻断外国法律与措施不当域外适用办法》，以及同年 11 月 1 日生效的《个人信息保护》中，均明确规定了我国加强对向境外司法或执法机构提供个人信息的监管和非经主管机关批准不得提供等的条文。

4.3. 行业层面

除了国家对于数据安全保护的实践外，不同行业对于数据安全的保护方式和侧重方面也各有不同。除去所有需要和个人交互的行业需要保护的个人隐私数据之外，核心在于提升行业领域内的特殊数据和核心数据的安全能力。对此，从下面的一些方面着手。

首先，优化数据安全管理架构。数据安全并非单纯的技术问题，要从治理、管理、执行和监督四个层次进行全面的优化，促进数据安全治理体系发展。首先，对资料安全的管理体系结构进行了优化。

其次，加强数据安全风险评估能力。根据《数据安全法》《网络数据安全管理条例(征求意见稿)》的规定，定期对企业开展数据安全评估。具体方式如通过建立专门的部门或工作小组，时刻将数据安全作为常规评估工作，根据评估结果做好数据资产梳理、重要数据识别、数据分类分级的基础性工作。

再次，积极采用新型技术手段，通过系统升级，部署人工智能、机器学习、分析和其他形式的安全自动化技术，强化数据安全态势感知，如采用文件加密、权限设置、流量同步监测等技术手段杜绝非常规信息数据的输出。

最后，加强对工作人员的数据安全能力培训和考核机制，通过打造针对技术、自动化与安全专业人才的团队建设，维护和减少系统内部漏洞，避免遭受外界恶意攻击篡改、盗取数据；规范数据处理的流程，加强对企业内部人员的数据安全能力培训和考核，增强工作人员的道德素养，避免内部无意识泄露数据的风险发生。企业监察人员应当做好常规巡检，对于涉嫌侵犯、破坏公司数据的刑事犯罪行为，积极配合公安机关做好刑事犯罪侦查、起诉的工作。

5. 我国数据安全保护规制的不足

目前，我国正在不断完善有关数据安全方面的法律规定，力图保障个人数据与重要数据的安全，推动形成数据安全协同治理机制。我国关于数据安全的相关规定，散见于各单行法中。其中，较为完善的立法是关于个人信息的跨境流动，在《网络安全法》《个人信息出境安全评估办法(征求意见意见稿)》《个人信息保护法》等法律法规中，对个人信息的跨境流动进行一定条件的约束和限制，例如信息跨境之前要求进行安全评估和事前批准。这些法律法规的规定，体现了我国对保障数据安全的重视，但从数据安全保护的保障体系来看，我国的数据安全保护的立法与实践仍然处于起步阶段。

5.1. 未形成统一立法，上位法缺失

从我国关于数据保护的零散的单行法看，目前，我国并未形成关于数据跨境流动规制的统一立法，除了《国家安全法》外，《数据安全法》《网络安全法》中既没有在条文中列出“根据宪法，制定本法”，也未明确提出根据某部基本法律制定本法。由此可见，关于数据安全保护的立法中，明显上位法依据缺失。另外，数据安全与网络安全、个人信息保护的关系，无论是在我国的《网络安全法》中，还是在欧美各国的立法中，通常都属于包含或者交织的关系。因此，我国独立制定《数据安全法》时，就同时面临着跟《网络安全法》和《个人信息保护法》的体系协调问题[8]。联系《数据安全法》的立法初衷，其目的指向仍然是安全价值，对于自由的价值位阶较低，由此导致在客观上可能引发限制数据自由流动的后果。

5.2. 规范内容不明晰

目前，我国关于数据安全保护的规定以原则性、概括性条款为主，在具体应用问题上，由于没有明确清晰的法律制度体系，可操作性不强，解决实践能力有待提高。另外，对于一些问题的定性、权利义务的明晰、法律规制等，如数据的权属、数据跨境流动等问题仍然存在许多争议尚未解决。我国对于数据安全保护的法律规制，也主要侧重于“个人信息”的保护，对于商业数据、政务数据的安全保护，虽

然有相应的规定，但过于原则化，不足以弥补实践中出现的疑难问题。在全球经济一体化的背景下，企业进行跨界业务，必然会导致数据的跨界流动。因此，目前数据安全保护立法的核心任务之一，即加强有关企业数据合规动力，指导其完成数据合规工作。

5.3. 未充分对接国际规则

我国目前对于数据安全保护的规制，并不足以对抗当前国际数据全球化的主流趋势，对于部分强权国家的管辖主张并不能有效应对。信息化时代的来临让数据成为当今国家之间争夺的资源，网络技术发达的国家会凭借丰富的数据资源形成新的垄断，制定相应的数据保护规则，达到满足自己国家的数据治理主张，美国的 CLOUD 案即是如此。另外，OECD 指南和 APEC 隐私框架等国家公约所提倡的对数据采用不同的限制模式，我国的国内法律也应对此做出相应的反应，充分对接国际规则，保障我国的企业更好地进行跨国经营活动。

6. 我国数据安全治理框架的完善路径

如上文所述，面对数据跨境流动问题，网络技术成熟的发达国家在规制数据安全保护问题上占据绝对的主导地位，而网络技术发展缓慢的发展中国家只能被迫以一种“防御”的姿态维护本国数据保护利益。在面对数据跨境流动问题上，各个国家制定相关的数据安全保护立法政策的出发点和落脚点是结合本国的现实国情和根本利益。就我国而言，制定我国数据安全保护的治理框架，必须坚持以数据安全流动为基本立场，推进数据跨境流动安全保护的统一立法，充分对接相应的国际规则，积极参与以国际条约为主要内容的国际合作治理，努力形成平等互惠的数据共享协议，确保数据安全不受侵害。

6.1. 坚持数据安全流动为先的基本立场

目前，数据的跨境流动问题不仅包括公民的个人数据信息，还包括商业数据，以及国家政务数据。数据全球化趋势的背景下，各个国家之间的博弈已经不再局限于地理空间上的主权安全问题，而是转战至网络空间，开辟新型的国际竞争。但是，数据作为一种资源，如果不做好相应的保护和规制措施，不仅会削弱本国的综合实力，国家主权问题也将会面临着严峻的风险。因此，必须坚持数据安全流动的基本立场，但这并不意味着否认或者拒绝数据自由流动。相关立法实践表明，在数据全球化的背景下，数据越是本地化，其带来的收益越将衰减，例如，过多的条件限制数据流动必然影响本国企业的海外经营生产。在各类数据密集型技术普及的趋势下，数据的自由流动是保障全球化经济发展的前提条件，因此，在确保数据安全的情况下，不应过多限制数据的自由流动。

6.2. 建立统一的跨境数据流动规则制度

尽管存在着明显的重叠，但隐私权和个人信息保护并没有为数据主权提供法律依据[9]。参考其他国家在数据安全保护问题上的做法，我国可以在《网络安全法》《数据安全法》等法律的基础上，尽快出台关于数据安全保护以及数据跨境流动的安全评估细则，指导、监督相关主体严格落实数据安全保护的法律法规中关于各类数据的本地化存储和跨境流动规则。另外，可以借鉴其他国家的做法，探索建立一个能够规制协调数据流动的行政管理部门，例如，日本设立“个人信息保护委员会(PIPC)”作为独立的第三方监管机构，对数据跨境流动进行规制管理，更具专业化地保护本国的数据安全。

6.3. 优化数据本地化的具体规则

通过对重要数据的跨境流动施加限制，防止一国公民个人信息、产业、经济以及科学技术等重要信息泄露国外以维护数据主权安全，均可以归入数据本地化的范畴。因此，数据本地化的建立，是为了保

护网络技术发展不成熟的一方对本国的网络空间管辖权，能够为本国内的个人信息与数字企业的发展提供一个相对安全的空间。但是，数据本地化可能会带来新的问题，如当地的经济发展与公司的商业利益将得到削弱，同时，也会削减本地数据服务提供商履行安全保护的动力。因此，为了进一步明晰数字服务贸易过程中可能存在的限制性政策以及对数字贸易服务带来的影响，OECD 设立了专门的数字服务贸易限制性指数。而在 OECD 给出的四十二条限制性措施中，我国的数字服务贸易限制性措施数量占据了十八条[10]，这也从侧面反映出我国在平衡数据跨境流动和保护数据安全之间仍有较大的进步空间。因此，我国在优化数据本地化具体规则方面上，不仅可以尝试建立数据跨境流动备案制度，提升监管部门对数据本地化存储和数据跨境流动的监管力度；还可以考虑设立“白名单”的制度，对符合法律法规规定的组织或地区给予认证列入名单，并对名单列入者提供相应的豁免，确保数据在通过认证的组织或地区之间可以自由流动，以此提高数据跨境流动和安全保护的效率。

6.4. 与国际数据治理接轨，引导国际规则发展

在现有国际法准则体系之下，由于缺少国际统一承认的可执行的数据权利标准，对于数据权利的域外标准与解决冲突的诉求，在多边主义中存在许多不同的声音。在具体的实践应用中，国际上通行的做法是通过订立国际贸易条约对数据的跨国流动，直接或间接地调整数据跨境流动关系。目前，我国在网络技术上的发展已经颇具成熟，因此，当前我国的做法应当是以积极主动的姿态加入国际沟通之中，努力争取全球规则的制定权，推动有关数据跨境流动的国际条约与国际治理框架的形成，建立健全电子证据跨国取证等国际协调机制。

7. 结语

从总体上看，数据全球化与数据主权对抗的主要趋势是，主权国家和地区逐步通过完善数据保护法规或重新制定数据保护法规来规制数据跨境流动问题。与此同时，各国政府开始积极应对数据跨境流动对本国带来的影响，例如，禁止数据出境、要求企业必须在本地进行数据存储和处理等。随着各种技术攻击手段的不断更新升级，网络空间受到的传统攻击不断加深，威胁数据安全的严峻形势为维护数据权利、限制数据跨境流通的主张和措施提供了合理性依据，但是，过分管制的政策和采用不合理限制的执法手段也将为全球范围内数字经济和前沿信息技术的发展带来阻碍。各国关于数据管辖权的不同主张，在国际法中也存在着不同的观点，从而给国际关系与世界治理秩序带来隐患。因此，在今后的一段时间里，为了构建一个更加符合我国主权利益和安全利益的数据流动秩序，仍然要以实现信息的安全流通为目标，通过完善、全面的制度规范来促进我国数据自由、安全地流动，加强对我国数据安全的监管。

参考文献

[1] 王珊, 萨师煊. 数据库系统概论[M]. 第 5 版. 北京: 高等教育出版社, 2014: 4.

[2] 梅夏英. 信息和数据概念区分的法律意义[J]. 比较法研究, 2020(6): 151-162.

[3] 马忠法, 胡玲. 论我国数据安全保护法律制度的完善[J]. 科技与法律(中英文), 2021(2): 1-7, 75.

[4] 郑璇玉, 杨博雅. 新兴权利视域下商业数据分类与保护研究[J]. 科技与法律(中英文), 2021(3): 8-16.

[5] 史亚丽. 商业大数据的法律保护探讨[J]. 伊犁师范学院学报(社会科学版), 2020, 38(2): 79-85.

[6] 韩旭至. 数据确权的困境及破解之道[J]. 东方法学, 2020(1): 97-107.

[7] 京东法律研究院. 欧盟数据宪章: 《一般数据保护条例》(GDPR)评述及实务指引[M]. 北京: 法律出版社, 2018: 21.

[8] 翟志勇. 数据安全法的体系定位[J]. 苏州大学学报(哲学社会科学版), 2021, 42(1): 73-83.

[9] Taylor, R.D. (2020) “Data localization”: The Internet in the Balance. *Telecommunications Policy*, **44**, Article No. 102003. https://doi.org/10.1016/j.telpol.2020.102003

[10] 王拓. 数字服务贸易及相关政策比较研究[J]. 国际贸易, 2019(9): 80-89.