数据跨境监管初探

朱扬勇[1,2]，熊赟[1,2]
1. 复旦大学计算机科学技术学院，上海 200438；2. 上海市数据科学重点实验室，上海 200438

摘要
随着对数据价值的认识日益增强，数据跨境越来越受到关注。一方面，数据跨境是经济全球化和数字经济发展的必由之路；另一方面，数据跨境有可能危害国家数据安全。因此，需要对必要的、合理的数据跨境和恶意的、有害的数据跨境等进行研究、界定，并制定相应规制。首先分析并给出了当前数据跨境的两种类型和4种渠道，然后提出了基于数据分类的数据跨境监管措施，为数据跨境监管和数据跨境立法提供了支持。

关键词
数据跨境；数据跨境监管；数据跨境类型；数据跨境渠道

中图分类号：TP302　　文献标识码：A　　doi: 10.11959/j.issn.2096-0271.2021010

Primary exploration of transborder data folw supervision

ZHU Yangyong[1,2], XIONG Yun[1,2]
1. School of Computer Science, Fudan University, Shanghai 200438, China
2. Shanghai Key Laboratory of Data Science, Shanghai 200438, China

Abstract
With the increasing awareness of the value of data, transborder data flow has attracted more and more attention. On one hand, transborder data flow is necessary for economic globalization and the development of the digital economy. On the other hand, it may cause damage to national data security without effective supervision. Therefore, it is necessary to distinguish between reasonable transborder data flow and malicious one, and formulate appropriate regulations. According to the analysis, two types of current transborder data flow and four transborder data flow channels were given. Furthermore, a classification supervision method for transborder data flow was proposed. This work provides the support for transborder data flow supervision and the legislation for transborder data flow.

Key words
transborder data flow, transborder data flow supervision, type of transborder data flow, transborder data flow channel

1 引言

跨境数据流动(transborder data flow, TDF或cross-border data flow)[①]概念在1980年经济合作与发展组织(Organization for Economic Co-operation and Development, OECD)颁布的《关于保护隐私与个人数据跨境流动的准则》里首次被提出，其被界定为个人数据的跨越国界流动[1]。1980年至今，关于跨境数据流动的研究主要聚焦在对跨境流动的法律机制的研究。各国跨境数据流动法律、法规的历史根源、立法模式、规制方式以及司法确认各不相同。每个国家的经济、政治和文化环境不一，因此所采取的应对跨境数据流动的管辖模式不一样，数据保护标准也不统一[2-3]。Estadella-Yuste O[4]指出相关部门需要动态审视关于跨境数据流动的法律法规是否符合跨境数据流动的发展，并制定与其发展相匹配的法律机制。单寅等人[5]指出，国际上对跨境数据流动的监管并未形成统一框架，不同国家采取的监管模式各不相同，他们认为各国以维护各国利益为出发点设计跨境数据监管制度，对不同类型的数据采取分级和分类监管，确保跨境数据流动不会危害国家安全和公共利益。Feldman M B等人[6]指出，出于各国经济、文化以及个人隐私权等方面的考虑，需对跨境数据流动进行监管，并认为不同国家实行不同的管理机制能够更好地管理和定义跨境数据流动；Kuner C[7]指出因为各国之间的法律法规和文化不同，对跨境数据流动的监管也不尽相同，认为世界各地使用不同的跨境数据流动监管机制会引起许多问题，使得这类跨境数据流动的法律不能成为全球认同的统一规定。各国数据规章制度存在显著差异，且各国之间限制数据跨境传输的规则存在冲突，使得通过政府间谈判取得共识的跨境数据流动的全球治理机制难以实现，导致跨境数据流动治理面临风险与挑战[8]。

虽然最初数据跨境被界定为个人数据的跨越国界流动，但是现在国际上对跨境数据流动的理解已经完全超越了个人数据。付伟等人[9]指出，自1980年OECD在《关于保护隐私与个人数据跨境流动的准则》中提出个人数据跨境流动就是个人数据的跨越国界流动，至今有关跨境数据流动的具体定义尚未形成统一的意见；Estadella-Yuste O[4]指出随着计算机技术和通信技术的进步，跨境数据流动成为国际上一个需要被重新定义的问题，认为跨境数据流动可以被定义为机器可读形式的跨越国界的数据和信息的传输。Casalini F等人[10]指出跨境数据流动对于跨国公司的日常运行非常重要，认为数据有许多类型，就贸易而言，个人信息、企业信息、财务信息和健康信息是该领域相对比较重要的数据信息，跨境数据传输甚至还催生了一种新型的微型企业，即微型跨国企业；张郁安等人[11]指出数据出境风险管理制度起源于对信息跨境流动下的个人权益保护，但在巨量的数据资源中已经不仅只包括个人数据了，也包括采购信息、地理位置等数据，且其中相当一部分数据涉及国家安全、公共安全。事实上，除人员跨境引发的数据跨境外，还有商业、资本和服务的跨境流动引起的数据跨境，尤其是跨国企业经营中涉及的数据跨境，跨国企业往往业务众多、数据交互频繁，既涉及个人数据，也涉及商户数据、商品数据、支付数据、物流数据等。因此，当前的数据跨境是指所有类型的数据跨境。一些数据蕴含着企业甚至国家的经济运行状况和趋势，涉及国家政治、社会、经

① 本文中，数据跨境和跨境数据流动的含义及英文一致。

济多个方面，这些数据的跨境流动是否会影响企业的竞争？是否会影响国家安全和社会稳定？由此带来的挑战成为国际政治、经济讨论的议题。要应对这些挑战，需要弄清楚数据跨境有哪些类型，当前的数据跨境有哪些方式，然后再研究什么数据可出境、什么数据应当被限制出境，出境后如何限制使用。本文从数据本身和数据技术角度对数据跨境类型和跨境方式进行分析，分析了两种类型的数据跨境和4种数据跨境渠道，提出了跨境数据的分类监管措施；还提出将数据自治模式运用于数据跨境，在强调数据主权（data sovereignty）的前提下，按照市场化方式实现数据跨境运用。本文旨在探索数据跨境治理以及为其立法研究提供技术支持，提升相关立法的可操作性。

2 数据跨境不可避免

数据跨境是指数据跨越一个国家的地理边境。这里就存在一个数据主权[12]问题，一个国家境内生产的数据是该国人、物和事件在网络空间中的记录，理应受领土主权的管辖权管理。因此，数据主权是领土主权的组成部分，是国家主权的一种呈现。数据主权一般指在一国范围内产生的数据，其跨境传输、加工和消除的全过程均按照该国的法律法规进行。此外，数据和土地、能源一样具有非常高的价值，是一个国家的新型基础性资源[13]。数据的运用对经济发展、社会治理、人民生活产生了重大而深刻的影响[14]，这意味着任何主体对数据的非法干预都可能构成对国家核心利益的侵害。数据安全已成为事关国家安全与经济社会发展的重大问题。从20世纪70年代德国黑森州的相关规制设立后，欧洲地区已经进行了一系列针对数据保护、隐私保护和跨境数据流动的机制性探索。欧盟为构建全球数据跨境治理的框架提供了极具参考价值的蓝本与标准[15]。美国虽然强调数据自由跨境，但这不意味着美国完全放任数据跨境。事实上，美国十分强调对跨境数据流动的控制，例如，美国现在实施的在出入境闸口审查笔记本电脑和手机就是对跨境数据的管控。但是，在全球化的大趋势下，从一国地理边界上物理硬性截断数据流动是一种逆全球化行为，显然是不合适的，数据跨境是不可避免的。

简单看电子数据交换（electronic data interchange，EDI）系统下产业链的运行，EDI字面上的含义就是数据交换。如果经济贸易活动是跨境的，那么其数据交换就是跨境的。在EDI体系下，A国家的一个工厂通过计算机通信网络接收到来自B国家用户的一笔EDI订货单，工厂的EDI系统随即检查订货单，并决定接受订货，然后向用户回送确认信息。工厂的EDI系统根据订货单的要求安排生产，同时向K个国家的零部件和配套设备厂商发出EDI订货单；向铁路、海运、航空等部门预订车辆、舱位和集装箱；以EDI方式与保险公司和海关联系，申请保险手续和办理出口手续；为用户开EDI发票；同银行以EDI方式结算账目等。全部过程都由计算机自动完成。值得注意的是，在互联网出现之前，EDI系统就在全球产业链上运行了，EDI也是跨国公司运行的基础支撑。

不难看到，产业链上的任何一个国家如果截断了EDI的数据交换，这条产业链就不能运行。跨境数据流动问题在EDI体系运行之初就存在了，差不多有50年的历史，比互联网出现得早。2015年，瑞典[16]出台报告，提出跨境数据流动是发达国家在

全球价值链上的新需求，服务作为中间产品越来越频繁地通过互联网进行传输，而旧的国际贸易规则无法适应全球价值链发展的需要，限制数据跨境流动的措施给贸易带来障碍。

为打破不同国家及地区在数据跨境传输上的壁垒和限制，推动全球数字贸易便利化，更有效地实现数据跨境流动的执法合作，满足企业间数据跨境传输的实际需要，经济合作与发展组织、亚太经济合作组织（Asia-Pacific Economic Cooperation，APEC）等国际组织制定了一系列的指南和政策，积极推动跨境数据传输自由化。

商业软件联盟（Business Software Alliance，BSA）提出数字贸易的推进计划，指出对跨境数据流动的限制是阻碍数字贸易发展的主要壁垒之一。该计划包括：一是确保数据无障碍跨境流动；二是以市场为主导，采取全球技术标准；三是扩大信息技术协议的范围。

美国信息技术与创新基金会（Information Technology and Innovation Foundation，ITIF）分析了数据泄露的5种情形，说明了数据的本地化存储并不能保证数据的安全，呼吁世界各国在立法中取消数据本地化存储的规定，以确保数字贸易正常进行[17]。

联合国跨国公司中心给出的定义是：数据跨境流动是跨越国界地对存储在计算机里的机器可读的数据进行处理、存储和检索[18]，即机器可读的数据通过互联网和信息系统跨越国家边境的运动。这个定义既给出了数据跨境的概念，又包括了跨境方式，较为混乱。从国际组织及其他国家对跨境数据流动的管理制度来看，跨境数据流动有两种跨境方式：一是跨越国界地传输和处理数据；二是数据在一国境内，但能被他国主体访问[17]。

3 数据跨境的类型

从大的类别来看，数据跨境可以被分为两大类：跨境业务下的数据跨境（称为第一类数据跨境）和无跨境业务的数据跨境（称为第二类数据跨境）。

（1）跨境业务下的数据跨境

第一类数据跨境是发生在国家之间的各种跨境业务行为导致的数据跨境，包括：个人旅游访问、健康医疗活动、银行支付、物流、金融市场、跨国公司日常运营、科学研究活动、全球变化应对等。第一类数据跨境的特点一般是日常性的、小规模的，在互联网出现之前就存在了，如始于20世纪60年代末的EDI电子商务。

互联网出现以后，第一类数据跨境随着全球交流和全球产业链的发展而迅速发展。例如，美国企业消费者信用信息收集机构与日本信用组织签署协议，允许相互利用对方的数据库，以核查居住在本国的对方侨民的信用记录。为了降低高昂的劳动成本、节约资源，一些企业会把部分工作外包给其他国家的机构，将包括身份证、信用记录、税务、保险等个人数据跨国转移至一些人工成本相对较低的热门地区，如印度、菲律宾等国。这种境外安排将工作拆分为数个能够有效管理的部分，使企业能够将有限的资源集中在核心领域，大大提升其市场竞争力[19]。

第一类数据跨境具体包括如下几种。

- 业务交流引起的数据跨境：经过信息化进程的广泛深入发展，各项业务交流都被信息化了，而信息化必将产生数据，因此业务的跨境交流就形成了数据跨境。例如，人员跨境涉及护照、机票、酒店等数据的跨境；全球供应链EDI数据跨境等。

● 产品使用与维护引起的数据跨境：有许多产品实行全球销售、使用和维护工作，这也将引起数据跨境的发生。例如，Windows软件、Epson打印机等产品维护系统的补丁软件就通过网络全球发放，用户还可以随时将使用信息和意见发给生产商，这就形成了数据跨境；通用电气公司跟踪飞机发动机，形成了数据的全球无国境传输等。

● 互联网业务：互联网业务是一大类创新业务，其本身就是无国境的数据流动体，无论是电子商务的全球采购和销售还是各类社交网络，都形成了大量数据跨境。

● 媒体传播：互联网更多的是被当作新媒体来看待，从利用Web页面信息传播到自媒体再到社交网络都是媒体的性质，这类媒体传播实际上就是数据的传播，数据跨境随时都在发生。

（2）无跨境业务的数据跨境

第二类数据跨境是不涉及跨境业务的纯粹的数据跨境，即一个数据集的出境/入境，包括：跨国企业数据中心迁移、中立国数据备份、商业数据资源交易、跨国数据采集、携带物理设备出境。第二类数据跨境是非日常的、大规模的，可以考虑在边境进行审查。需要注意的是，在技术上，第二类数据跨境可以伪装成第一类数据跨境。

第二类数据跨境具体包括如下几种。

● 数据中心迁移：跨国企业根据业务需要和成本考量，将数据中心从一个国家迁移到另一个国家，形成大规模数据跨境。

● 数据备份：为了数据安全，跨国企业可能会将数据备份到第三国。另一个情形是为了防备战争，将一个国家的重要数据备份到中立国。数据备份会形成数据跨境。

● 数据资源交易：各类数据资源购买、交换，包括政治、经济、科学、社会等数据在国家之间的交易、共享等引起的数据跨境。

● 携带设备出境：出境者携带电脑、移动硬盘出境，引起数据跨境，可以分为数据滞留和数据不滞留两种。如果出境者回归，但数据留存国外，则数据滞留（可以将数据滞留看成数据资源交易来处理）；如果随着人员的回归，数据就回归了，则数据不滞留。

4 数据跨境的渠道

当前，数据跨境的渠道主要有：通过数据的物理载体（便携式电脑、移动硬盘、U盘等）将数据携带出境/入境；通过互联网直接将数据传输出境/入境（包括数据跨境访问和处理）；通过专用的通信卫星将数据传输出境/入境（包括数据跨境访问和处理）；通过暗网将数据传输出境/入境。

（1）通过数据的物理载体

通过数据的物理载体将数据携带出境/入境是一种相对便利和安全的数据跨境方式。采用该方式主要考虑到两个方面：一是数据规模大，网络传输难以完成；二是网络传输的不安全性。对于前者，除了便携式电脑、移动硬盘、U盘等，也出现了如亚马逊数据硬盘集装箱的物理载体方式，这为大规模的数据传输提供了一种补充的解决方案。对于后者，在数据跨境方式的安全性方面，USB接口介质和计算机信息系统之间的数据传输控制成为涉密计算机信息系统信息输入输出控制的关键。研究者已经结合输入输出控制系统和管理措施，开发了由USB驱动程序、USB监控服务程序、USB授权管理程序和USB注册管理程序等组成的专用软件系统，在涉密计算机信息系统上结合“集中输入输出控制软件系统”使用，根据管理要求对USB接口介质和计算机信息系统之间的信息流向进行控制。

（2）通过互联网

互联网已经成为承载种类繁多的数据

和海量应用的综合网络。通过互联网直接将数据传输出境/入境，是一种常用的数据跨境方式，也是跨境业务下最直接的数据跨境方式。由于大多数情况是利用公开的互联网环境，因此该方式在数据传输安全方面面临更大的挑战。互联网根据用户需求和业务特征对网络资源进行智能分配，从而提高资源利用率和服务质量。对于跨境数据流动而言，网络运营商、数据服务器、路由等都是数据跨境方式涉及的重要因素。面向公开的互联网环境，加强数据传输的安全性（包括数据加密等）十分重要。但是，过度的数据加密和保护可能会带来跨境数据应用和监管的困难，因此需要平衡数据的使用和保护。

（3）通过专用的通信卫星

卫星通信是无线电通信站之间将人造卫星作为中继而进行的通信，是宇宙无线电通信的一种形式，工作在微波频段。与其他通信方式相比，卫星通信具有通信距离远、覆盖面广、工作频带宽、通信容量大、具有多址连接能力和广播特性等优势。通过专门的通信卫星将数据传输出境/入境成为数据跨境的主要方式。

卫星通信已经成为军队信息化战争中最重要的信息传输纽带，可以将指挥控制机构、各军兵种、作战单元、侦察卫星、无人侦察机、潜艇等作战元素结合在一起，形成将陆海空天地融为一体的信息化战场态势。可以看出，这种方式的数据跨境可以进一步加强涉及国家安全的跨境数据与信息化战争的有效融合，例如能够考虑进行各兵种联合战斗、各种武器系统联合作战、信息共享。卫星通信系统与各种武器平台、情报分析与指挥系统的结合更加紧密，各种战场信息能够及时有效地通过卫星系统传输给各个用户。

为了解决卫星信道传播时延较长、信道误码率较高的问题[20]，新型的宽带多媒体卫星通信系统逐渐发展起来。宽带多媒体卫星通信系统可提供更加丰富的业务服务，如可视电话、视频接入、交互式多媒体应用等。用户数据传输速率高达每秒几十比特，用户终端主要是固定式的，也包括PC终端和移动终端。

对于这种数据跨境方式，考虑到一些涉密的跨境数据，还需要借助军事专用的卫星通信系统，因为这些系统具有很强的抗干扰能力。此外，随着电子元件和新技术的不断发展，通信终端的体积将更小、重量更轻、功耗更小，便于携带、安装和应用。

（4）通过暗网

暗网（hidden web[21]或deep web[22]）是难以被搜索引擎等公开渠道访问和检索的网络空间，是互联网的一个有意隐藏的部分，只能通过暗网技术或特殊的浏览器进行访问。暗网最初是为了保护互联网用户的隐私免受流量分析攻击而发展起来的。暗网在不同程度上实现了匿名性，即隐匿源/目的地址和通信双方身份[23]。为实现匿名，暗网中的通信都会通过多个站点转发流量，在传输过程中还会执行多次加解密，使得每个站点只知道部分信息，从而保护用户的隐私，隐匿使用者的身份和通信数据信息，为用户提供匿名性支持。

暗网限制了标准技术的适用性，其域名不公开发布，暗网存在的时间短或经常更改，具有高度动态性，与明网之间几乎没有链接。因此，考虑到业务竞争、数据隐私、数据安全保护等问题，采用暗网的方式实现数据的跨境。

但是因为其强大的匿名性，暗网能够屏蔽其在互联网上的位置，使这些网站能够承载恶意和非法的内容，容易被不法分子所利用，这对于网络安全监管而言是一个极大的挑战。值得注意的是，对于暗网的隐匿性来说，已经有Tor、IP和ZeroNet

等匿名网络进行暗网域名收集[24]，因此技术都具有两面性，一方面暗网保护了跨境数据的安全性，另一方面，为了应对网络安全的监管，需对暗网进行域名收集和追踪等。

5 跨境数据的分类管理

对于第一类数据跨境问题，其数据主权的界定是一个难点。例如，数据是A国家的跨国公司在B国家的业务活动而生产的，如果这个数据的主权属于B国家，那么数据将脱离生产主体，这会带来一系列问题，例如商业秘密泄露；如果这个数据的主权属于A国家，那么B国家的数据安全将受到严重挑战。因此，一个可能的选择是双方共有，即要求跨国公司留一份完整的数据副本在B国家，B国家可以审查数据的国家安全性问题，但负有对数据保密的责任。数据与领土、领空、领海差异很大，数据主权要求独立自主地处理数据，但数据是国际交往、经贸往来的记录，在数据跨境流动中，难以实现独立自主地处理数据，需要通过协商谈判解决[25]。另外，数据自治模式是政府数据开放和企业数据流动的一种可行的模式[26-27]，可以考虑将数据自治模式用于数据跨境。

主权国家有权对境内数据行使主权。为了避免国家陷入封闭的经济社会，需要考虑对数据跨境进行分类管理，并研究技术可行性。那么，怎样的数据跨境是必要的、合理的？怎样的数据跨境是恶意的、有害的？

（1）数据跨境的监管挑战

表1展示了数据跨境类型及跨境渠道，分析如下。

首先，通过互联网跨境是主要的数据跨境方式，这完全符合互联网快速发展的状况，事实上，互联网本质上就是为了实现数据全球流动而创造的。由于互联网数据流量非常大，在不大幅度影响网络速度的情况下，对网络中流动的数据内容进行监管是非常困难的。

其次，对专用网络（包括早期通过电话拨号联网、现在的卫星联网）的数据跨境监管目前还没有很好的技术手段；因为暗网本身不合法，所以要尽量切断暗网。

再次，对利用物理载体进行数据跨境的监管，可以通过对设备进行检查的方式，检查物理载体中的数据内容。这是目前唯一能够有效进行监管的数据跨境类型。

最后，对于携带设备出境的管理，可以参照物理载体出境的监管方式，对出境设备进行检查，无论数据是否滞留境外，都按照滞留境外对待。

综上，数据跨境的监管挑战在于通过网络的数据跨境需要规制和技术协同监管，在无法通过技术实现监管的情况下，可以规制先行。

（2）跨境数据的类型

目前，还无法从技术上针对数据跨境方式进行有效监管，尤其是通过网络的数据跨境的监管几乎还没有可行的方法，只能先行建立可行的规制，因此应将重点放到对跨境数据进行分类管理。在国家数据主权的框架下，建立规制以对境内数

表1 数据跨境类型及跨境渠道

数据跨境类型	方式	物理载体	互联网	专用的通信卫星	暗网	特点
第一类数据跨境	业务交流	√	√	√	√	日常性小规模
	产品使用与维护		√	√		
	互联网业务		√		√	
	媒体传播		√		√	
第二类数据跨境	数据中心迁移	√	√	√	√	非日常大规模
	数据备份	√	√	√		
	数据资源交易	√	√	√	√	
	携带设备出境	√				

据进行分类管理。可考虑将数据分成必须跨境、禁止跨境、可选跨境3种类型。

● 必须跨境的数据。国家之间在协议框架下进行的各类实体业务往来、人员流动、科技人文交流引起的数据跨境是必需的，否则这些协议就无法执行。为行使数据主权，一种可行的做法是要求当事主体在跨境前将相关数据在本国数据中心上做一个数据备份，例如印度尼西亚2012年通过的《电子系统与交易操作政府条例》明文规定，提供公共服务的电子系统运营者应当把数据中心设置在印度尼西亚境内。此外，针对这些必需的数据跨境，需要从国家数据安全的角度重新审视之前形成的协议是否会由于数据跨境而影响国家数据安全和个人隐私安全，如果存在安全问题就需要修改之前的协议，否则就允许数据跨境。

● 禁止跨境的数据。显然，涉及国家安全的任何数据都是不允许出境的。由于目前还难以从技术上甄别具体的跨境数据是否涉及国家安全，因此，一些国家就硬性禁止数据离境。例如，俄罗斯国家通信委员会要求电子通信和网络提供商配备数据留存设备，以实现数据的收集操作，并且在服务器上保留12 h以上；澳大利亚2012年生效的《个人控制电子健康记录法案》明文规定，不得将个人电子健康记录移至澳大利亚境外，也不得在境外加工或处理这些记录。

● 可选跨境的数据。虽然禁止数据跨境的做法保护了数据安全，但也会影响正常的人文交流和经济往来。从规制和技术方面不能确定数据跨境是否涉及国家安全时，可以将数据跨境的选择权下放给当事主体，由当事主体自行决定是否允许数据跨境。例如韩国2011年生效的《个人信息保护法》规定，涉及个人数据跨境的数据必须获得数据主体的同意。这种做法是有益的，例如一个病人可以将自己的电子病历数据携带出境，并提供给境外医疗机构。

数据跨境是必然趋势，但需要在保障数据跨境利益得以实现的同时，确保国家数据安全、公民隐私不被泄漏。前已述及，如果仅仅从数据保护以及法律规制的方面考虑，将直接制约数据跨境，这是因为目前还没有合理有效的数据跨境监管手段，数据跨境将增大跨境国家数据安全和公民隐私泄露的风险。然而，过度的数据保护又将制约数据跨境利益的实现。

6 结束语

数据和土地、能源一样具有高价值，是一个国家的新型基础性资源。数据的运用对经济发展、社会治理、人民生活都产生了重大而深刻的影响，这意味着任何主体对数据的非法干预都可能构成对国家核心利益的侵害。跨境数据流动是一类涉及国家数据安全的、规模最大的、范围最广的数据流动行为。对于数据跨境，在战略上必须要有主权意识，在战术上则需要根据经济社会和技术的发展状况灵活把握。

数据的收集、存储、使用、传输等行为已经遍及全球，超越了国家及地域的界限，使得数据跨境流动问题已非一国或一个地区的内部力量就能彻底解决。单靠某个国家或地区，或者几个国家，几乎不可能有效地实施合理的数据跨境解决方案，需要国际社会、各个国家的共同努力和积极参与。2020年9月8日，我国提出了《全球数据安全倡议》，数据安全的中国方案值得期待。

参考文献:

[1] KUNER C. Regulation of transborder data

flows under data protection and privacy law: past, present, and future[J]. SSRN Electronic Journal, 2010(10).

[2] MELTZER J P. The Internet, cross-border data flows and international trade[J]. Asia & the Pacific Policy Studies, 2015, 2(1): 90-102.

[3] 许多奇. 论跨境数据流动规制企业双向合规的法治保障[J]. 东方法学, 2020(2): 185-197.
XU D Q. Legal guarantee for two-way compliance of enterprises subject to regulation of cross-border data flow[J]. Oriental Law, 2020(2): 185-197.

[4] ESTADELLA-YUSTE O. Transborder data flows and the sources of public international law[J]. North Carolina Journal of International Law, 1991.

[5] 单寅, 王亮. 跨境数据流动监管立足国际, 看国内解法[J]. 通信世界, 2017(14): 24-25.
SHAN Y, WANG L. Cross-border data flow supervision is based on the international, here are domestic solutions[J]. Communications World, 2017(14): 24-25

[6] FELDMAN M B, GARCIA D R. National regulation of transborder data flows[J]. North Carolina Journal of International Law and Commercial Regulation, 1982, 7(1).

[7] KUNER C. Regulation of transborder data flows under data protection and privacy law: past, present, and future[J]. TILT Law & Technology Working Paper, 2010.

[8] 许多奇. 个人数据跨境流动规制的国际格局及中国应对[J]. 法学论坛, 2018(3): 130-137.
XU D Q. International pattern of personal data cross-border flow regulation and China's response[J]. Legal Forum, 2018(3): 130-137.

[9] 付伟, 于长钺. 美欧跨境数据流动管理机制研究及我国的对策建议[J]. 中国信息化, 2017(6): 55-59.
FU W, YU C Y. Research on the management mechanism of cross-border data flow between the United States and Europe, and my country's countermeasures[J]. iChina, 2017(6): 55-59.

[10] CASALINI F, GONZÁLEZ J L. Trade and cross-border data flows[J]. OECD Trade Policy Paper, 2019.

[11] 张郁安, 宋恺. 对新时期数据跨境流动风险的思考[J]. 中国信息安全, 2018(11): 79-82.
ZHANG Y A, SONG K. Thoughts on the risks of cross-border data flow in the new era[J]. China Information Security, 2018(11): 79-82.

[12] TRACHTMAN J. Cyberspace, sovereignty, jurisdiction, and modemism[J]. Indiana Journals of Global Legal Studies, 1998, 5(2): 566.

[13] 朱扬勇. 大数据资源[M]. 上海: 上海科学技术出版社, 2018.
ZHU Y Y. Data resource[M]. Shanghai: Shanghai Scientific & Technical Publishers, 2018.

[14] 朱扬勇. 旖旎数据——100分钟读懂大数据[M]. 上海: 上海科学技术出版社, 2018.
ZHU Y Y. Charming data-to understand big data in 100 minutes[M]. Shanghai: Shanghai Scientific & Technical Publishers, 2018.

[15] BIRNHACK M D. The EU data protection directive: an engine of a global regime[J]. Computer Law & Security Review, 2008, 24(6): 508-520.

[16] National Board of Trade (Sweden). No transfer, no production-a report on cross-border data transfers, global value chains, and the production of goods[R]. 2015.

[17] 刘博. 国际贸易中的跨境数据流动规制及其对中国的启示[D]. 北京: 对外经济贸易大学, 2016.
LIU B. Transborder data flow regulations in international trade and the enlightenments to China[D]. Beijing: University of International Business and Economics, 2016.

[18] Centre on Transnational Corporations, United Nations. Transnational corporations and transborder data flows: a technical paper[Z]. 1982.

[19] SAMARATI P, DI VIMERCATI S D C. Data protection in outsourcing scenarios: issues and directions[C]// The 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2010: 1-14.

[20] DAI H, SHEN Q, WANG C Z, et al. Towards satellite-based quantum-secure

time transfer[J]. Nature Physics, 2020, 16(8): 88-852.

[21] FLORESCU D, LEVY A Y, MENDELZON A O. Database techniques for the world-wide web: a survey[J]. ACM SIGMOD Record, 1998, 27(3): 59-74.

[22] BERGMAN M K. The deep web: surfacing hidden value[J]. Journal of Electronic Publishing, 2001, 7(1).

[23] ZERFOS P, CHO J, NTOULAS A. Downloading textual hidden web content through keyword queries[C]// The 5th ACM/IEEE-CS Joint Conference on Digital Libraries. Piscataway: IEEE Press, 2005: 100-109.

[24] OMAR Z M, IBRAHIM J. An overview of darknet, rise and challenges and its assumptions[J]. International Journal of Computer Science and Information Technology, 2020, 8(3): 110-116.

[25] 沈逸, 姚旭. 大国战略互信与跨境数据流动管理新模式探索: 以“数据主权”为核心推进网络安全战略建设[J]. 信息安全与通信保密, 2018(12): 12-16.
SHEN Y, YAO X. Exploration of strategic mutual trust between major powers and a new medel of cross-border data flow management: promoting the construction of cyber security strategy with “data severeignty” as the core[J]. Information Security and Communication Privacy, 2018(12): 12-16.

[26] 朱扬勇, 熊赟, 廖志成, 等. 数据自治开放模式[J]. 大数据, 2018, 4(2): 3-13.
ZHU Y Y, XIONG Y, LIAO Z C, et al. Self-governing openness of data[J]. Big Data Research, 2018, 4(2): 3-13.

[27] 沈逸, 姚旭, 朱扬勇. 数据自治开放与治理模式创新[J]. 大数据, 2018, 4(2): 14-20.
SHEN Y, YAO X, ZHU Y Y. General design of self-governing openness of data and the exploring of the new mode of governance[J]. Big Data Research, 2018, 4(2): 14-20.

作者简介

朱扬勇（1963- ），男，博士，复旦大学计算机科学技术学院教授、学术委员会主任，上海市数据科学重点实验室主任。《大数据》期刊副主编，大数据协同安全技术国家工程实验室副理事长，中国自动化学会国防大数据专业委员会副主任，农业大数据产业技术创新战略联盟副理事长兼首席科学家。2004年开始从事数据科学研究，2008年提出数据资源保护和开发利用，2009年发表了数据科学论文《Data explosion, data nature and dataology》，并出版数据科学专著《数据学》。第462次香山科学会议“数据科学与大数据的理论问题探索”的执行主席。《大数据技术与应用丛书》主编，《大数据资源》主编，大数据科普图书《旖旎数据——100分钟读懂大数据》作者，参与国家和地方多个大数据规划编制。目前主要研究方向为数据科学和大数据技术，近期研究重点方向为数据真实性、数据财政、数据资产、数据自治与数据跨境等。

熊赟（1980- ），女，复旦大学计算机科学技术学院教授、博士生导师，上海市数据科学重点实验室副主任。2004年起从事数据领域方面的研究工作，作为项目负责人，主持多项国家自然科学基金项目、上海市科学技术委员会发展基金项目以及企业合作项目。在国际权威期刊和会议论文集上发表论文80余篇，出版著作3本。目前主要研究方向为数据科学和大数据。

收稿日期： 2020-09-22

通信作者： 朱扬勇，yyzhu@fudan.edu.cn

基金项目： 国家自然科学基金资助项目（No.U1636207, No.U1936213）；上海市科学技术委员会发展基金资助项目（No.16JC1400801, No.19511121204）

Foundation Items: The National Natural Science Foundation of China (No.U1636207, No.U1936213), Shanghai Science and Technology Development Foundation (No.16JC1400801, No.19511121204)