

后疫情时代中国企业的数据跨境合规挑战及其因应

汤清瑄

浙江理工大学法政学院、史量才新闻与传播学院，浙江 杭州

收稿日期：2023年2月28日；录用日期：2023年5月16日；发布日期：2023年5月23日

摘 要

2020年，新冠病毒肆虐全球，世界经济受到了巨大冲击。在如今疫情总体上得到控制，人类社会逐渐步入后疫情时代，危险与机会共存。信息技术的高速发展在激发出全球数字经济的潜力的同时也可能导致数据泄露。为了保护我国数据安全，我国立法赞同数据本地化，主张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应当在境内存储。这尽管在一定程度上保护了我国数据安全，但是也给我企业对外投资带来合规方面的挑战。本文通过分析各国之间立法数据跨境立法、我国现有数据跨境制度，从价值目标、细化规则等方面完善立法制度，督促企业形成自查思路，采取更为主动的应对策略，以帮助在进行电子商务、第三方支付等涉及数据跨境业务的我国企业后在疫情时代能更好地“走出去”。

关键词

后疫情时代，数据跨境，企业合规

Data Cross-Border Compliance Challenges for Chinese Companies in the Post-Epidemic Era and How to Deal with Them

Yuxuan Tang

School of Law and Politics, Shi Liangcai School of Journalism and Communication, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: Feb. 28th, 2023; accepted: May 16th, 2023; published: May 23rd, 2023

Abstract

In 2020, the new coronavirus ravaged the world and the world economy took a huge hit. With the

epidemic now generally under control, human society is gradually moving into the post-epidemic era, where dangers and opportunities coexist. While the rapid development of information technology has stimulated the potential of the global digital economy, it may also lead to data leakage. To protect our data security, our legislation endorses data localization and advocates that personal information and important data collected and generated in operations in the People's Republic of China should be stored in the territory. While this protects China's data security to a certain extent, it also poses compliance challenges for Chinese companies investing abroad. This paper analyzes the data cross-border legislation among countries and the existing data cross-border system in China, improves the legislative system in terms of value objectives and refined rules, and urges enterprises to form self-examination ideas and adopt more proactive response strategies to help Chinese enterprises involved in data cross-border business, such as e-commerce and third-party payment, to better "go global" in the post-epidemic era.

Keywords

Post-Epidemic Era, Data Cross Border, Corporate Compliance

Copyright © 2023 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在“后疫情时代”，疫情虽得到了基本控制，但时有反复，这对于各国经济的适应能力提出了更为严格的要求，如何将危机转变成商机成为了重要主题。2020年，疫情蔓延全球，各国经济受到疫情不同程度的冲击。在全球经济下行的形势之下，数字经济却加速增长，有效对冲了全球疫情的冲击。2020年全球经济深度衰退，主要国家经济均出现负增长，然而我国数字经济仍然保持9.7%的高位增长，是同期GDP名义增速的3.2倍多，向全世界展现了我国的数字经济的强大韧性，到2025年，中国数据总量预计将跃居世界第一，全球占比有望达到27%以上[1]。虽然中国的数字经济在产业潜能方面仅次于美国，领先于欧洲和其他国家，但在涉及数据跨境流动时，中国政策往往较为保守，相关法律法规的制定滞后于目前的数字经济产业能力。“走出去”（即对外投资）企业在进行电子商务、云计算、第三方支付、物流平台、软件服务等主营业务时通常会涉及到数据跨境流动活动。因此尽管数据本地化有保护我国数据安全，但是也给我企业“走出去”带来了不利影响。

2. 我国企业“走出去”面临的数据合规挑战

2.1. 企业合规成本增加

合规制度旨在规制企业营业过程的各个环节，从社会、环境、知识产权、反腐败等各方面监管，健全企业治理、预测风险、快速处理，以求实现企业良性运营。新冠疫情使得全球贸易摩擦增加，在参与全球各地的竞争前，我国企业需要了解到他们需要遵守的海外规则和相关法规。然而由于监管方面很多法律法规的不断更新、变化，企业所需要的前期调查工作压力增大、面临的合规风险也在不断提高。计算机与信息技术的高速发展，也倒逼着各国完善各自的数据立法。为了使得防止个人信息失控，数字遗忘权等新设数据权利被提出，数据权利有着上升到基本人权的趋势。这种趋势使得企业需要在每一项数据处理过程中提高其规范性，这往往会导致大量资源成本的消耗。数据保护周期的增长、过高的行为标

准使得企业的负担大大增加。仅针对《一般数据保护条例》(General Data Protection Regulation, 简称 GDPR) 的合规要求, 全球便有 20% 的企业因违反合规要求而导致破产, 甚至出现了美国洛杉矶时报及芝加哥论坛报等企业因 GDPR 合规成本过高而直接退出欧盟市场的现象。此外, 数字化对企业的颠覆性影响以及不断加强的数据隐私条例使得对外投资企业面临的风险环境变得前所未有的复杂。

2.2. 他国反制措施难以预测

疫情导致的治理赤字、信任赤字、和平赤字、发展赤字加剧国际社会的间的矛盾, 西方国家开始兴起“逆全球化”潮流。从本质而言, “逆全球化”其实是资本主义国家为了稳固不平等的世界体系的一种途径。国际一级的地缘政治紧张局势充分证明了相互冲突的模式对互联网、数字技术和数据治理的影响。最值得注意的是美国和中国之间持续的技术和贸易紧张关系。尽管中国在历史上一直采取限制性做法, 禁止几项基于美国的服务, 转而推广本地数字平台和服务, 但美国近年来开始对中国科技公司采取更具攻击性的措施。2020 年 5 月特朗普政府发布清洁网络计划(Clean Network program), 以其安全和美国公民隐私受到“重大威胁”为借口, 旨在从美国的网络中删除不可信的中国应用程序和服务, 并减少中国在美国电信网络和海底电缆中的存在, 最终将导致互联网碎片化。¹ 在这种不稳定的全球局势下, 若采取数据本地化这种但单边性的数据保护措施, 很容易引起他国进行反制措施, 使得国际贸易局势不稳定, 可能增加企业合规风险。

3. 合规挑战原因分析

3.1. 各国立场冲突的必然结果

数据主权逐渐成为“兵家必争之地”。以美国为首的部分发达国家借助其产业国际竞争优势和灵活的保障手段, 对于数据主权问题采取“进攻型”战略, 以自身在数据技术领域的优势加之“长臂管辖”手段不断扩大其跨境数据的执法权利, 为谋取数据霸权。欧盟采取的是“中立型”战略, 以保障个人信息安全的目的, 通过设立“白名单”、签订标准合同等措施在允许跨境数据流动的基础上对其进行严格限制。西方少数国家以强大的经济实力为支撑在数据领域充当着“规则创建者”, 而其他大多数国家则是被动的继受者。大数据中通常包含着涉及军事、国防、资源等重要领域的的数据, 如果任由数据自由跨境流动, 可能会导致发达国家控制发展中国家关键数据, 巩固数据霸权。因此相比于欧美这些发达国家, 中国等发达国家则往往采取更为保守的数据跨境战略, 如利用数据本地化的手段来进行数据治理。因此, 各国对于数据主权所采取的不同立法政策极大地改变了全球数据主权的治理框架, 也在一定程度上加剧了各国间对数据主权问题的冲突[2]。

3.2. 数据跨境流动规则分散

我国现今数据与安全信息领域的法律框架由 2017 年 6 月 1 日起施行的《网络安全法》、2021 年 9 月 1 日起施行的《数据安全法》和 2021 年 11 月 1 日起施行的《个人信息保护法》构成。《网络安全法》重点关注网络本身的安全, 涉及数据在网络上流动与存储的安全。《数据安全法》重点关注数据本身的安全, 内容上覆盖了非电子数据, 比如纸质的信息。而《个人信息保护法》则更注重保护公众的利益, 在确保个人数据安全的基础上, 促进信息数据的合理流通与利用, 更侧重于保护公民利益。在这一法律框架中, 有关数据跨境流动的规定多以原则性、概括性条款为主, 缺乏一定的可操作性, 该制度的构建仍处于起步阶段, 尚没有建立完整而明确的制度体系以解决实践中存在的问题, 对于数据的权属、数据跨

¹See, e.g., Forbes, 17 September 2020, CFIUS and a Tale of Two Internets, available at <https://www.forbes.com/sites/riskmap/2020/09/17/cfius-and-a-tale-of-two-Internets/?sh=5c37db2439fb>.

境流动的特有原则、权利义务关系、监管机构与职责等基本争议也缺乏充分考虑。此外，当前立法也多侧重于保护“个人信息”，对商业数据、政务数据等虽有进行规定，但仍不足以支撑实践。特别是对于企业而言，数据跨境流动是跨国企业开展经营活动的必然要求，如何赋予相关企业充分的数据合规动力，并指导其完成数据合规工作，也是数据跨境流动立法的重要任务之一。对数据域外流动不够重视很可能会引发危机，我国仍需在新一轮数据保护监管浪潮下完善合规性的应对方法。

3.3. 企业合规缺少具体指导

数据的治理在当下中国仍是一个新兴问题，由于缺乏规则及相关指导案例，企业合规自治处在一个摸石头过河的阶段[3]。跨境数据传输安全评估框架的建立，在一定程度上加强了对信息的保护，也提高了对相关公司的合规要求。今后，那些业务需要向国外发送相关信息的公司应注意提高配合安全评估工作的意识[4]。但在实际的数据交流过程中，企业经营者往往以经济利益为中心，在大数据运用过程中的操作不规范问题，也往往抛之脑后，对于数据安全风险缺乏考虑；其次，在数据交流监管层面，监管者的数据安全保障理念，往往还停留在传统静态信息保护阶段，然而由于大数据时代下云计算、物联网等先进科技手段，所带来数据的动态流动、多层级流转特征，缺乏与时俱进的数据保护理念，并不利于数据保护。此外，基于这一传统数据保护理念，相关主体在数据保护手段的适用上、数据安全保护目标上进行简单化认定，从而忽视了在数据流转过程中产生的多路径风险[5]。

4. 我国企业“走出去”合规挑战的破解路径

4.1. 完善我国现有立法制度

4.1.1. 明确数据跨境的价值目标

法治，是我们党治国理政的基本方式，也是我国在面临后疫情时代挑战中需要坚持的理念。我国多部法律法规涉及数据跨境流动，虽然确立了安全、自由的跨境数据流动原则，但在当下，国家大力提倡建立“网络命运共同体”，保守地限制跨境数据流动既不利于“一带一路”建设的同时也不利于中国企业“走出去”，与国家发展战略背道而驰。我国应重视跨境数据流动的国际合作，以开放为合作的基石，积极搭建双边或多边国际合作平台[6]，应对网络安全挑战，把握网络发展机遇，为后疫情时代全球经济复苏贡献力量。

4.1.2. 细化数据分类制度和出境管理机制

数据具有交叉的属性，针对不同的数据内容，应进行不同的限制和规则制定。截至目前，我国在货物、技术进出口方面都制定了出口管制制度，但数据领域的出口管制制度还不够完善，出口管制不完善的根本原因还是目前没有一个成熟的数据分级标准[7]。在《数据安全法》中虽然存在数据分级分类的要求与划分依据，但仅是数据分级分类制度的雏形。《数据安全法》第二十一条第一款明确了数据分类分级保护制度。第二款规定“关系国家安全、国民经济命脉、重要民生、重大公共利益等数据”属于“国家核心数据”。第三款要求各地区、各部门根据该制度，自行确定本地区、本部门及相关行业、领域的重要数据具体目录，并加以实行重点保护。由法条可知，我国通过将重要数据列入保护目录进行针对性保护，但对于不属于核心数据的一般数据如何具体进行判定分类，更为严格的管理制度为何，法律语焉不详。目前的数据分类分级标准的不明确，使得这项制度缺乏可操作性，过于粗略的分类会使得数据面临泄露风险，且过于保守的分类会影响数据的流动，使得数据无法发挥其经济价值，削弱了我国企业对外投资的竞争力。2022年《数据出境安全评估办法》正式施行，它是构建我国数据出境制度的重要一步，它将数据出境适用范围、申报材料、评估内容、具体流程、权益保护进行了更为细致的规定，但其中对

于数据分类识别标准、企业自评估与国家组织评估方法等内容还有待细化。

4.2. 督促企业形成自查思路

4.2.1. 建立企业风险防控机制

在数据安全方面,企业作为数据流动的控制者,应当在跨境数据活动中承担其相应的安全义务。目前,当前企业间尚未具体的跨境数据流动保护制度框架,对于数据安全管理的自律意识也较为薄弱。一方面,企业由于业务众多、数据交互频繁,因此应当保持对各地域数据跨境规则的高度关注,对风险保持敏感。另一方面,我国可以借鉴他国经验,通过在企业内部设置专门数据合规管理人员,建立数据保护官制度,由专职的个人负责使企业保护数据更加专业,对接境外标准更加准确,构建行业自律机制,加强与监管机构的合作对接,推动企业合规,减少违规风险,减轻监管机构的负担,提高企业竞争力。

4.2.2. 引入信用评价体系

现实呼唤行业与企业配合政府的规制进行自治、自律、自查、自省,期待着商事主体以一种更为积极的姿态在市场中进行活动。商誉对于一家企业来说是其整体价值的重要组成部分,是一种至关重要的无形资产。信用体系主要是通过一定模式的计算,对评估对象是否履行义务和信用程度进行评价。近年来,国内部分地区、行业已将信用评价作为数字化发展的一项重要辅助措施。信用体系作为一种较为温和的手段,可以从外部鼓励企业实现内部自律,提高行业与企业合规经营的自觉性与责任感,对于数据安全秩序的构建有着正面的作用。

5. 结论

数据本地化措施虽然保护了我国数据安全,但是却使得我国企业在进行对外投资时面临海外合规风险,本国企业的合规成本上升的同时也需要应对他国的反制措施。在现今的国际环境下,各国对于数据保护的不同立场使得数据主权问题冲突凸显,而国内方面,我国的数据跨境流动规则分散,规定操作困难,企业合规缺少指导,数据安全风险预测能力较弱。为破解我国企业在对外投资中出现的难题,我国企业应当从明确数据跨境价值目标及细化规则两方面完善我国现有立法,督促企业形成自查思路,建立企业风险防控机制,引入信用评价体系,使得我国在后疫情时代更好地“走出去”。

参考文献

- [1] 中国信息通信研究院. 中国数字经济白皮书[EB/OL]. <http://www.caict.ac.cn/kxyj/qwfb/bps/202108/P020210913403798893557.pdf>, 2022-01-04.
- [2] 冯洁菡,周濛. 跨境数据流动规制: 核心议题、国际方案及中国因应[J]. 深圳大学学报(人文社会科学版), 2021(8): 38-40.
- [3] 闫钰菲. 我国数据出境法律监管制度研究[D]: [硕士学位论文]. 绵阳: 西南科技大学, 2022.
- [4] 邓志松,戴健民. 《网络安全法》时代数据跨境传输的企业合规挑战[J]. 汕头大学学报(人文社会科学版), 2017(5): 70-73.
- [5] 朱斌斌. 数据安全保护体系的检视与构建——以《数据安全法》为切入点[J]. 牡丹江大学学报, 2022(4): 61-66.
- [6] 刘俊敏,郭杨. 我国数据跨境流动规制的相关问题研究——以中国(上海)自由贸易试验区临港新片区为例[J]. 河北法学, 2021(7): 76-90.
- [7] 崔晴. 《数据安全法》及《个人信息保护法》要点解读[J]. 中国外资, 2022(5): 68-70.