

## 区域性公共产品与欧盟数据保护的路径\*

汪晓风\*\*

**【内容提要】** 全球性公共问题的解决有赖于全球性公共产品的有效供给,当数据保护公共产品的全球供给严重缺失时,区域路径可以提供替代性选择。欧盟个人数据保护的经验和展示了公共产品区域供给的有效性,可以从制度层面促进区域合作顺利开展,有效应对区域公共产品的外部性,确保区域合作激励机制的执行,以及更好地促进功能性合作的外溢,对区域层面的反应也更迅速,对跨区域交易的保障也更有力。

**【关键词】** 欧盟;个人数据保护;区域性公共产品;美欧数据贸易

**【Abstract】** The solution to global public problems depends on the effective supply of global public goods. When the global supply of data protection public goods is insufficient, the regional path can provide an alternative option. The experience of the EU data protection has demonstrated the effectiveness of regional supply of public goods. It can promote the smooth development of regional cooperation from the institutional level, effectively respond to the externalities of regional public goods, ensure the implementation of regional cooperation incentive mechanisms, and better promote the spillover of the functional collaboration. It also can respond more quickly at the regional level, and provide stronger protection for cross-regional transactions.

**【Key Words】** EU; Personal Data Protection; Regional Public Goods; PRISM Project

---

\* 本文是国家社科一般项目“美国棱镜计划的系统分析与综合应对研究”(15BGJ049)的阶段性成果。

\*\* 汪晓风,复旦大学美国研究中心副研究员。

对于特定全球性公共问题,有效的治理取决于所需公共产品的充分供给,而在全球性公共产品供给不足的情况下,区域性公共产品是替代性选择。作为一个全球共享的公共领域,网络空间已经成为经济社会发展的重要平台,其全球连接的物理特性决定了研究者往往从全球治理角度进行思考和寻求解决方案,而促进网络发展和维护网络安全的现实需求又促使决策者以民族国家为核心制定政策。当前网络空间治理的全球性公共产品供给严重不足,而国家治理又难以满足网络空间互联互通需求,区域合作的解决方案或可提供一种新的思路 and 选择。本文从区域性公共产品供给的角度,考察欧盟个人数据保护政策从《个人数据保护指令》到《通用数据保护条例》的演变,并分析其对于个人数据保护和网络空间全球治理的启示和意义。

## 一、作为公共产品的数据保护

网络时代的人际交往、商务交易、社会治理、公共管理乃至国际关系都离不开个人数据。随着信息通信技术的广泛应用,尤其是互联网与社会生活各领域的全面融合,个人数据的不断采集、大量存储、深度分析和跨境传输已成为各方竞相争夺的热门业务,个人数据的规模化开发利用也成为利润丰厚的产业。同时,与之相伴的滥用、窃取和泄露个人数据等问题大量出现,对个人隐私甚至社会稳定造成威胁,已经成为社会关注的焦点。欧盟和美国较早就为个人数据保护制定专门法律,中国也陆续出台相关法律保障个人数据相关的隐私权和财产权。由于个人数据数字化、网络化和国际化趋势不断发展,个人数据频繁的跨境流动引发各种技术和法律问题,个人数据的合理使用以及有效保护也已跨越国界,成为世界各国共同面临的全球性公共问题。

首先,个人数据所有权、控制权和受益权的分散复杂分布。个人数据基本信息的部分所有权属于数据主体,而使用各种网络应用中产生的个人数据则依约定决定权属,控制权或管理权一般为运行数据采集或经营数据处理、存储和应用等业务的企业或实体,而受益权可能归属于数据主体,也可能经授权转移给数据专营企业。当数据需要跨境转移时,分散的

权属关系即会带来合法性的诸多难题,诸如管理者如何取得授权,授权如何符合时效性,收益的分享和成本的分担,等等。

其次,各国数据保护法的独立性和冲突。确定个人数据跨境转移时的管辖权往往引发各国法律之间的冲突,尤其在线使用境外服务器上的应用产生的数据传输,或是一些应用系统需要调用分布于多个国家的程序或数据的情形时。这类源于各国个人数据保护适用法律引发的冲突,包括涉及多国法律都应管辖的“积极冲突”和没有一国法律可以管辖的“消极冲突”。<sup>①</sup>建立相应的冲突解决机制可能成为一种解决办法,鉴于目前国际社会尚未就选择一家国际组织承担该项职责进行讨论,也没任何一个现有的争端解决机制得到授权处理国家间的数据冲突,所以建立全球数据冲突解决机制的设想仍需时日。

第三,滥用和非法使用个人数据的预防和追责。如果上述两个难题可以通过双边和多边途径就拥有交叉管辖权的数据签订谅解协议,还可能找到可行的解决方案,那么对于非法使用数据或通过网络窃取数据的问题,迄今既没有可以援引的国际法、国际条约或国际协定<sup>②</sup>,也无法诉诸国际争端解决机制,只能通过单边的国内法和双边司法互助协定解决。

数据保护面临各种难题,为个人数据的跨境流动造成很多困扰,尤其那些经营全球业务的互联网公司。诚然一些大企业试图建立能够兼容各国法律的企业和行业标准来保护个人数据,但企业作为数据控制方或管理方,其提供的方案很难成为“上位”的规范,而迄今也没有一国政府接受其他国家法律管辖的企业制定标准的先例。全球性公共问题的解决有赖于全球性公共产品的有效供给,而当前数据保护的全球供给即便不是空白,也是非常不足。因而区域路径成为一种可行的补充或过渡,面对数据保护的诸多难题和国际机制的缺失,作为替代选择的区域性公共产品应运而生。

区域性公共产品是利益惠及一个确定区域的公共产品,布鲁斯·拉西特(Bruce Russett)和哈维·斯塔尔(Harvey Starr)提出建立地方性和区

---

① 郭瑜:《个人数据保护法研究》,北京大学出版社2012年版,第250页。

② 2001年11月欧洲委员会通过的《网络犯罪公约》(Cyber-crime Convention)可以为成员国之间处理数据相关犯罪提供协助,但迄今该公约签字国并不具有普遍性,且在数据保护方面没有可以直接援引的条款。

域性机构以获得公共产品的路径<sup>①</sup>,由域内国家联合供给的区域性公共产品,可以按照成本分担的模式划分为三种类型:第一种是以欧盟为代表的核心国主导供给模式,作为推动欧盟一体化进程的两大核心,法国和德国着眼于推动欧盟一体化进程和发挥欧洲的整体影响,主动承担并推动区域性公共产品的联合供给,形成欧盟经贸、货币、司法和安全四大领域的合作机制。第二种是以北美自由贸易区为代表的霸权国主导供给模式。第三种是以东盟及“10+”为代表的小国联盟主导供给模式。三种模式提供了区域合作不同层次和类型的公共产品,欧盟提供作为满足特定个人数据保护需求的区域性公共产品,一体化的决策和执行机构可以提供相应制度保障,明显更有效率且更有持续性。

如果将全部区域性公共产品看作一个整体,或一个连续性的动态供给过程,那么根据各个公共产品在这个连续过程中所处的不同环节可将其分为供直接消费的最终区域性公共产品,如环境保护、水资源、金融稳定、公平贸易,等等,以及作为最终公共产品来源的中间区域性公共产品,中间区域性公共产品既可以服务于区域性公共产品,也可以服务于全球性公共产品,如地区投资和贸易协定、地区和平机制等。从这个角度而言,个人数据保护属于一种中间公共产品,既是实现个人隐私和公民权利的机制,也可以保证个人数据合法和安全地跨境传输,为数字经济增长提供动力。

托德·桑德勒(Todd Sandler)根据是否具备非排他性和非对抗性的属性,将国际公共产品划分为纯粹公共产品和准公共产品。由于非排他性公共产品的供给者无法阻止不合作者获取收益,因而会导致公共产品供应不足或停止供给。<sup>②</sup>区域性公共产品以区域内国家为服务对象,内含了一定的排他性,然而一旦外部消费者加入,从区域性公共产品中取得收益,则仍有可能导致该公共产品的供给受阻。在区域内实行共同的个人数据保护政策,可以实现竞争性收益,因而可以看作一种俱乐部产品。

---

<sup>①</sup> Bruce Russett, Harvey Starr, *World Politics: The Menu for Choice*, Cengage Learning Inc., 2002. p.422.

<sup>②</sup> Todd Sandler, “Regional public goods and international organizations”, *The Review of International Organizations*, 2006, Vol.1(1), p.7.

## 二、欧盟数据保护的路径演变

欧盟很早就开始建立个人数据保护制度,制定个人数据保护政策法规。因为欧洲社会公民权利意识根深蒂固,注重个人隐私保护。同时,欧洲国家在信息通信技术和应用领域具有一定竞争力,但单个欧洲国家又难以独立与美国竞争。此外,欧盟也试图建立统一的数据保护法规,在司法层面推动欧洲一体化进程。

### (一) 欧盟《个人数据保护指令》

个人数据保护虽以公民权利保护为基本出发点,但从政策制定者的角度,却是要实现一种平衡,即一方面确认在收集、处理、存储和传输个人数据的过程中要保护个人权利,另一方面也要促进合法、必要的数据流动。20世纪90年代初,新科技革命方兴未艾,信息通信技术已经在各个领域广泛应用,互联网商业运行也启动,个人数据规模和流动快速增长,而各国立法的差异一定程度上影响了个人数据的跨境流动,过多强调个人隐私的各种限制也成为银行、保险等重要经济行业的障碍。当时,欧盟决定制定个人数据保护政策,与其说是为了保护个人数据,毋宁说更重要的目的是防止各成员国以保护公民隐私的名义阻止或中断数据的国际流动,从而影响这一潜力巨大产业的发展前景。

欧盟1995年推出的《个人数据保护指令》就明确体现了上述两个目标:一是要求各成员国保护公民的基本权利和自由,特别是与个人数据处理相关的隐私权,二是各成员国不得以保护为由限制或禁止成员国之间个人数据的自由流动。<sup>①</sup>该指令由欧洲议会和欧盟理事会推出,意图在于从欧盟和成员国两个层面建立一致的立法依据,为当时欧盟各国立法保护个人数据和保障数据自由流通设立了最低标准。

该指令也存在诸多不足,由于共同司法体系是欧盟一体化进程的薄

---

<sup>①</sup> The European Parliament and the Council of the European Union, "Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities*, No.L281, November 1995, p.38.

弱环节,该指令并没有建立欧盟层面统一的执法程序,也未提供成员国相应指导标准,成员国仍然从各自法律制度来执行指令,使得个人数据在成员国享有不同层级保护水平,指令一致性大打折扣。事实上不仅各国依据指令的最低标准执行指令的力度最小。进行数据处理和转移的企业的合规成本也并未降低,因为成员国将指令转化为内容不完全一致的国内数据保护法规,企业仍然需要自行与各国数据保护政策法规对接,完成在欧盟各成员国内的合规性程序。事实上该指令颁布后,各国保护个人数据的法律的差异性并没有得到根本改观,从而很大程度上影响了数据保护的实际效果,欧盟内数据自由流动也没有达到预期水平。

## (二) 欧美《数据安全港协议》和《隐私保障框架》

《数据保护指令》施行以后,外国企业如要进入欧盟开展可能涉及进行数据跨境传输业务时面临的一些限制。如该指令第 56—57 条规定,个人数据的跨境流动对扩大国际贸易是必要的,但只有第三国确保提供适当水平的保护,才能将欧盟个人数据转移至第三国,且同时禁止将欧盟个人数据转移至不能提供适当水平保护的第三国。<sup>①</sup>这实际上是要求其他国家的政府为本国企业背书,承诺对传输到本国境内的欧盟个人数据实行与欧盟相当的保护,保证该国企业不会违反欧盟的数据保护标准。

为帮助美国企业进入欧盟经营数据业务,1998—2000 年期间,美国商务部和欧盟及瑞士谈判达成了《数据安全港协定》<sup>②</sup>,做法是由美国商务部建立一个公共目录,隶属于联邦交易委员会和交通运输部管辖的任何机构和组织,只要承诺遵守“数据安全港”规则,即可列入公共目录,成为“数据安全港”的成员,可以接收、处理和传输来自欧盟的个人数据。“安全港”的目标是在确保美国企业达到欧盟的较高保护标准的同时,维持美国长久以来一直采用的自律机制。从公共产品的角度看,《数据安全港协议》一定程度上削弱了欧盟《数据保护指令》的排他性,如根据《美国爱国者法案》规定,美国企业收到外国情报监视法庭的传票,令其向情报机构提供特定

<sup>①</sup> “Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, pp.36—37.

<sup>②</sup> US Department of Commerce, “The Safe Harbour Privacy Principles”, July 21, 2000, [https://2016.export.gov/safeharbor/eu/eg\\_main\\_018475.asp](https://2016.export.gov/safeharbor/eu/eg_main_018475.asp), 2018-06-22.

数据时,美国企业必须予以配合。<sup>①</sup>由于美国政府对欧盟的承诺和其为反恐制定的法律之间存在着矛盾,这导致《欧盟数据保护指令》面临失效的风险。

2013年6月,美国情报界大规模的电信和互联网网络监控项目被曝光,包括监控美国公民及在美外国人对外通话的“棱镜”(PRISM)、从光纤主干网收集数据的“上游”(Up Stream)、监控互联网重要节点的“关键得分”(X-Keyscore),等等,监控对象从各国政要到普通公众无所不包,盟友伙伴、竞争对手和敌对国家概莫能外,尤其是对德国总理、罗马教皇等欧洲政要的电话监控,以及对法国和西班牙公众的大规模数据搜集激怒了整个欧洲。2015年10月,欧盟法庭认为美国未能为传输到境内的欧盟个人数据提供有效保护,欧洲公民的个人数据在美国被大规模地搜集,鉴于美国政府没有达到《个人数据保护指令》的要求,故判决欧美《数据安全港》协议失效。<sup>②</sup>美国企业不能再以政府背书而直接使用和传输欧盟公民数据。直至2016年7月,欧美经过谈判重新签订欧美《隐私保障框架》,除了强调企业为将欧盟公民个人数据传输到美国承担更严格的数据保护责任之外,还对美国政府访问有关数据设定了责任条款,并要求欧盟和美国政府每年就框架的执行情况进行联合评估。<sup>③</sup>

### (三) 欧盟《通用数据保护条例》

随着社会信息化水平的进一步提高,原欧盟《个人数据保护指令》越来越难以满足个人数据保护和数字经济发展的需求。2012年,欧盟提出改革个人数据保护政策,以帮助公众更有效地保护个人数据,同时推进欧盟单一数字市场的发展,协助欧盟企业在统一市场上提高竞争力。

经过四年反复讨论和修改,欧盟成员国司法及内政事务部长会议就数据保护的新框架达成一致,确立了五项基本原则:1)“同一个大陆,同一

---

① U.S. Public Law 107-56, “Uniting and Strengthening America by Providing Appropriate Tools Required Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001)”, October 2001.

② Court of Justice of the European Union, “The Court of Justice declares that the Commission’s U.S. Safe Harbour Decision is invalid”, October 6, 2015, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>, 2018-06-22.

③ “EU-US Privacy Shield”, July 12, 2016, [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en), 2018-06-22.

套法规”，在欧盟内实施统一的数据保护法；2）“被遗忘权”，用户可以要求互联网企业从网络搜索结果中移除个人信息，除非有明确法律允许互联网企业保留相关信息；3）“欧洲境内适用欧洲法律”，无论企业或机构是否设在欧盟内，只要在欧盟范围内提供服务，均需遵守欧盟法律；4）“强化各国数据保护机构权力”，允许各成员国的数据保护机构对违法者进行处罚；5）“一站式服务”，企业和用户仅需面对一个成员国的监管机构。

2016年4月，欧洲议会和欧盟理事会通过欧盟《通用数据保护条例》。与《数据保护指令》相比，该条例更加重视个人数据保护，赋予欧盟公民更广泛的保护个人数据的权力，该数据保护条例将负有保护责任的数据控制者扩展到几乎涉及所有的公司和机构，大到跨国公司，小到家庭企业和个人，只要有收集和使用欧盟个人数据的行为，都必须遵循该条例的标准。《通用数据保护条例》把个人权利与企业义务绑定在一起，增加了对个人数据保护的力度，强调被遗忘权、个人数据的复制权、个人信息泄露后的通知义务、处理个人信息的知情权，等等。欧盟还设立了一个欧洲数据保护委员会，同时每个欧盟成员国都必须设立一个与欧洲数据保护委员会相对应的监管机构，以保证《通用数据保护条例》在欧盟和成员国层面都得到执行。此外，条例中没有条款来严格明确如何对个人数据保护实施技术和组织措施，这被称为条例的“技术中立”原则，任何数据控制者以及进行收集、处理、储存和转移数据的企业将自行决定如何正确保护个人信息，这也符合信息技术发展迅速、各企业和实体的数据格式与处理程序千差万别的现实。

### 三、数据保护区域公共产品的启示

从全球层面看，网络空间治理驻足不前，无论是建立网络空间国际行为规则，还是应对网络攻击和网络恐怖主义，抑或消除数字鸿沟的发展援助以及保障数据安全有序流动的的全球规范，迄今未见显著进展。究其原因，或是全球性公共产品供给路径不清晰，或是网络大国单独供给的意愿不强，或是集体供给的动力不明确。而欧盟在数据保护区域公共产品供给方面的实践，可以提供一些有益的启示。



首先,从制度层面促使区域合作的顺利实现。

与全球性公共产品相比,区域性公共产品具有几个优点:一是涉及成员较少,更容易促成公共产品的供应;二是区域集体对话与合作机制可以避免领导国通过霸权将之私物化的风险;三是区域性国际公共产品的涵盖范围较小,各国的收益和成本比较清晰,一定程度上能够减少“搭便车”现象。<sup>①</sup>欧盟成员国数量适中,文化背景和价值观相近,经历数十年的一体化进程,成员国之间建立了较为充分的信任,普遍认同和尊重个人自由的权利,欧盟委员会、欧洲议会、欧洲理事会等一体化机制已经能够制定和执行共同的货币、贸易和外交政策。这些成为欧盟就个人数据共同保护政策展开协商谈判的基础,从而使之较快进入个人数据保护的基本原则和保护措施的谈判进程,避免了因利益和目标存在根本差异而无法进行实质性谈判的困境。

其次,有效应对外部性。

欧盟制定严格的个人数据保护法规,鼓励个人数据在欧盟内自由流动,对于个人数据向欧盟以外的流动设置高门槛,一个很重要目的是为了遏止美国信息技术企业向欧洲的扩张势头,增强欧盟成员国企业的竞争力。<sup>②</sup>欧盟的个人数据保护直接适用于欧盟各成员国,旨在加强对自然人的数据保护,并一统此前欧盟内零散的个人数据保护规则,同时降低企业的合规成本,欧盟企业和个人均能从中受益。在竞争环境下,一些人的生产或消费使另一些人受益而又无法向后者收费的现象,或一些人的生产或消费使另一些人受损而前者无法补偿后者的现象,是公共产品的正外部性或负外部性的表现。外部性往往会损耗公共产品的有效供给,从而导致合作受挫。区域性公共产品“在一个有限地理范围内所产生的非竞争性和非排他性收益”<sup>③</sup>,欧盟的个人数据保护政策既提供了个人数据权益的保护,也为个人数据合法流动制定了通道,包括向欧盟之外转移。当

---

① 黄河:《区域性公共产品:东亚区域合作的新动力》,《南京师范大学学报》,2010年第3期,第64页。

② Dorothee Heisenberg, *Negotiating Privacy: the European Union, the United States and Personal Data Protection*, Lynne Rienner Publishers, 2005. p.10.

③ Todd Sandler, *Global and Regional Public Goods: “Global and Regional Public Goods: A Prognosis for Collective Action”*, *Fiscal Studies*, Vol.19, No.3, 1998, p.222.

外部企业或实体处理和转移欧盟个人数据,被要求执行欧盟标准时,实际上按约定支付了数据转移合规的成本,亦即支付了它消费公共产品的成本。不仅如此,欧盟数据主体不仅使个人权益得到有效保护,也能得到从授权企业或实体处理或转让个人数据而带来的精准服务等好处。

### 第三,确保激励机制执行。

公共产品供给不足的一个重要原因是受“搭便车”影响,公共产品的融资和管理难以持续,分类和有针对性的激励机制可以鼓励各国供给公共产品,而建立对合作国家有约束力的协议和制度是达成合作供给的激励机制之一。<sup>①</sup>欧盟《个人数据保护指令》和《通用数据保护条例》由欧洲议会和欧盟理事会制定。欧洲议会是欧盟的立法、监督、预算和咨询机构,目前其成员均由欧盟成员国直选产生,欧盟理事会是欧盟的主要决策机构,由各成员国的部长组成。因而欧盟数据保护法规是所有成员国的共同意志表达,对外则代表统一的欧洲的力量,凡提供产品或服务的过程中涉及欧盟境内个体数据均需要遵守。如违反《通用数据保护条例》的企业或机构,轻则将受到1 000万欧元或上一年度全球营收的2%(两者取其高)的罚款,重则受到2 000万欧元或上一年度全球营收的4%(两者取其高)的罚款,正是基于欧盟“一个声音”的整体实力和欧盟单一市场的总体影响力,才能制定如此高额处罚力度并确保得到执行。从《个人数据保护指令》到《通用数据保护条例》,从欧美《数据安全港协定》到《隐私保障框架》,欧盟数据保护的约束对象从企业扩展到企业、个人、机构、实体,及至外国政府部门。完善而有强制力的协议、制度和法律,保证了作为区域性公共产品的欧盟数据保护的有效供给。

### 第四,促进功能性合作外溢。

在区域一体化进程中,供给区域性公共产品是开展功能性合作的重要方式。功能性合作中不断强化的角色感有助于域内各国相互依赖感的形成,使越来越多行为体能够认识到自己是区域利益攸关方,并最终导致集体认同。<sup>②</sup>欧盟数据保护的初衷是加强个人数据保护和促进数据合法自

<sup>①</sup> 杨海燕:《区域公共产品的供给困境与合作机制探析——基于合作博弈模型的分析》,《复旦国际关系评论》,2015年第1期,第33页。

<sup>②</sup> 贺平:《区域性公共产品与东亚的功能性合作》,《世界经济与政治》,2012年第1期,第47页。

由流动,但在此过程中建立的原则、规范、标准和流程也具有广泛的适用性,随着欧盟个人数据规模及其所蕴含商业价值的不断增长,越来越多在欧盟经营涉及个人数据业务的企业和实体以欧盟原则重构业务流程,并沿着企业经营范围向相关行业扩展,在零售、保险、航空、银行等行业形成同等数据保护标准,而一旦形成路径依赖,则会逐渐建立该领域共同遵守的规范。同时,发展和治理过程中产生的最佳实践也是扩展合作的重要动力之一,欧盟实践也会成为其他国家、地区以及国际机构效仿的对象,从而促进欧盟原则向国际规范演变。事实上,鉴于欧盟《通用数据保护条例》树立了一个高标准的个人数据保护法律模板和严格的数据跨境传输规范,一些国家已经决定跟上欧盟的步伐,以免在数据利用方面受到限制。因而条例出台以后,已有日本、韩国、印度等国家同欧盟接触,展开交流,试图学习欧盟数据保护实践的经验,或寻求与欧洲标准的对接。2018年4月美国的一份调查表明,当被问及“《通用数据保护条例》使欧盟公民能够更好地控制企业如何使用他们的个人数据,你是否希望在美国颁布类似法律”时,68%的美国人给出了肯定的回答。<sup>①</sup>这显示了区域性公共产品存在跨区域转换的能力。

## 结 语

个人数据保护的意义随着网络空间的不断发展而更加重要,因而需要寻求有效的解决方案。斯蒂芬·克雷斯勒(Stephen D.Krasner)认为,在基本原则存在分歧、权力分配高度不均的领域难以形成国际制度。<sup>②</sup>从全球层面看,网络空间利益主体多元化、权力分配高度不均是一个不争的事实,这一定程度上可以解释为何国际社会对于网络空间全球治理抱有很多期待,但从“伦敦进程”到联合国信息安全政府专家组,似乎都没有探

---

<sup>①</sup> Janrain, “Consumer Attitudes Toward Data Privacy Survey 2018”, May 7, 2018, <https://www.janrain.com/resources/industry-research/consumer-attitudes-toward-data-privacy-survey-2018>, 2018-06-22.

<sup>②</sup> Stephen D.Krasner, “Global Communications and National Power: life on the Pareto Frontier”, *World Politics*, Vol.43, Issue 3, 1991, p.337.

索出一种有效的治理模式。而从地区层面看,情况却大有不同,同一地理区域的国家文化背景相似度更高,经济发展水平更为接近,社会信息传播更为便利,政府间的互动更为频繁,显然也更具备持续供给数据保护公共产品的意愿和能力。一体化进程有助于区域性公共产品的机制化供给,促进功能领域合作的稳步推进和逐渐扩展,反过来又可以为一体化进程提供更多动力。总之,全球层面推进网络空间治理阻力重重,而区域路径前景更可期待,其原因在于区域性国际公共产品更具适用性,对于区域一体化机构或主导国家而言,可以取得比全球层面的努力更好的收益。