法商研究 Studies in Law and Business
Vol. 39 No. 2(2022)

数据保护的国际软法之道

敖 海 静*

摘 要:数据自由流动与本地化存储以及隐私保护之间的矛盾是国际社会在数字时代共同面临的治理难题,基于各国数据治理的硬法规则相互冲突的客观现实,国际软法成为在国际层面加强数据保护的较优选择。在对当前分别侧重效率和安全的两种软法谱系及其模式进行分析的基础上,结合本国主体性原则的考量,中国应当选择以侧重效率同时兼顾安全的软法规制模式为蓝本,积极主动地参与以经济合作与发展组织《关于隐私保护和个人数据跨境流动准则》和亚太经济合作组织《隐私框架》为代表的国际数据保护软法框架及其外部—内部双层实施机制的建构,促进数据的自由流动。中国应当考虑加入作为亚太经济合作组织《隐私框架》国际实施机制的《跨境隐私规则》体系,通过"软硬兼施"的途径完善数据保护法律体系,并在其他多边协调机制中推动数据保护领域多元兼容的国际软法规则的形成。

关键词:数据保护 隐私保护 国际软法

一、问题的提出

在数据资源主导的全球化时代,数据不仅仅直接关涉到个人的隐私安全和生活安宁,更因重大的战略价值而成为重塑国际政治经济格局的关键因素。然而,关于数据安全自由流动的保护规则,全球远未达成共识,各国发生冲突的现象甚至已渐成常态。欧盟虽然试图以数据保护事关基本人权为由遮掩其反对数据自由流动的真实动机,但《欧盟一般数据保护条例》(以下简称《欧盟条例》)关于该条例适用的地域范围①和数据跨境传输条件的严苛规定,还是凸显出其在数字经济落后于中美的背景下企图通过新的贸易壁垒赢得未来国际竞争的残酷现实。与此同时,作为全球最大的数字经济体,美国认为网络空间应是创新的公平竞技场,各国不得在信息自由流动

* 中国人民大学法学院博士后研究人员、讲师
基金项目:教育部哲学社会科学研究重大课题攻关项目(17JZD031)

① 参见欧洲数据保护委员会:《关于〈一般数据保护条例〉适用的地域范围的指南》,敖海静译,《经贸法律评论》2020年第2期。

与网络安全之间作出选择。[①] 但理想化的数据自由论由于认可既定优势反而固化了恃强凌弱的国际秩序。就数据调取来说，美国通过制定《澄清境外数据合法使用法》确立了数据控制者标准，凭借技术和市场优势，将长臂管辖权扩张至任何有美国参与的数据市场，[②]却仍以属地管辖原则来确保本土数据市场管辖权的独占性，限制境内数据外流。由此观之，数据的本地化存储与自由流动这一对本就难以消解的矛盾随着欧美相关法律的制定变得愈发激烈和突出。

因各国有关数据保护的硬法间存在冲突，数据的跨境流动缺乏相应的国际机制，阻碍了以互联网为基础的全球经济的发展，[③]故有学者将眼光投向作为全球问题新兴解决手段的软法，希望以软法规制的灵活性来协调数据本地化存储与自由流动间的矛盾。从逻辑上讲，这种规制的灵活性既是网络安全解决方案有效性的内在需求，[④]也是国际网络空间现有硬法相互冲突乃至协调各方利益的硬法渊源根本缺失[⑤]背景下的较优选择。这种主张既注意到了推动软法兴起的社会背景，也利用了软法相对于硬法的特殊优势，有助于发挥软法在数据保护问题上的作用。那么，当前国际数据保护的软法实践呈现怎样的框架结构？包括中国在内的国际社会，在建构该框架的过程中，应以何种软法规制模式为基础？应该受到何种原则的约束？又该如何具体型塑其实施机制？一言以蔽之，从中国的国情和全球化时代的经济政治格局出发，我们需要一套怎样的国际数据保护软法？这正是本文要探究的问题。

二、国际数据保护软法的基础框架

在国际数据保护法领域，《欧盟条例》是当前最具代表性的硬法规则，对全球数据保护实践产生了深远的影响，但如果论及该领域的软法规则，那么经济合作与发展组织（以下简称经合组织）制定的《关于隐私保护和个人数据跨境流动准则》（以下简称《隐私准则》）[⑥]和亚太经济合作组织（以下简称亚太经合组织）制定的《隐私框架》[⑦]就构成当前国际数据保护软法实践的基础框架。

（一）《隐私准则》

经合组织在1980年发布的《隐私准则》是信息隐私保护领域第一部通过协商达成的国际准则。[⑧] 经合组织希望通过该准则消除以隐私保护为名对数据跨境流动设置的不当障碍，从而确

---

① See The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, p.5.

② 参见冉从敬、陈贵容、王欢：《欧美跨境数据流动管辖冲突表现形式及主要解决途径研究》，《图书与情报》2020年第3期。

③ 参见个人信息保护课题组：《个人信息保护国际比较研究》，中国金融出版社2017年版，第166～167页。

④ See The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, p.5.

⑤ 参见冯硕：《网络个人信息保护国际合作的障碍与选择：以软法为路径》，载张平主编：《网络法律评论》（第20卷），北京大学出版社2018年版，第131～132页。

⑥ See OECD, Guidelines Governing the Protection of Privacy and Transorder Flows of Personal Data, in OECD, the OECD Privacy Framework, OECD Publishing, 2013, pp.9－126.

⑦ See APEC, APEC Privacy Framework (2015), APEC Secretariat 2017.

⑧ See ICCP, WPISP, 30 Years After: The Impact of the OECD Privacy Guidelines, OECD Conference Centre, 2010, p.4.

立数据自由流动与合法限制原则。[①] 2013 年修订后的《隐私准则》由 6 个部分组成:第一部分包括必要的定义,指定了准则适用的范围,并且声明该准则仅为隐私保护和个人数据跨境流动规则的最低标准;第二部分是准则的核心内容,提出了在国家层面保护个人自由和隐私的 8 项原则,即限制收集原则、数据质量原则、目的明确原则、限制使用原则、安全保障原则、公开原则、个人参与原则以及问责原则;第三部分主要是对问责原则的细化,对数据控制者提出了一些要求;第四部分阐述了主要涉及成员方之间关系的国际适用原则;第五部分概述了实施准则的各种方法,并强调了适用时的非歧视性;第六部分讨论了成员方间的互助事项,主要是通过信息沟通来避免不兼容的保护个人数据的国家程序。《隐私准则》最后还提到了当个人数据流动涉及多个国家时可能出现的法律问题。作为软法,虽然《隐私准则》对成员方并无法律约束力,但是其所附的经合组织理事会建议指出,成员方在制定有关隐私和数据保护的国内法时应考虑准则的要求。

(二)《隐私框架》

在亚太经合组织内部,各成员方的隐私法差异较大,立法承认隐私权的程度也各不相同。这使得亚太经合组织认为制定有关最低隐私标准的区域协议是促进成员方之间数据自由流动的理想机制,同时也有助于发展电子商务。[②] 为此,亚太经合组织电子商务指导小组起草了《隐私框架》,并在 2004 年获得采纳。除了简短的前言,《隐私框架》的主体由 4 个部分构成:序言、范围、亚太经合组织信息隐私原则以及执行。在第一部分即序言中,《隐私框架》声称其符合《隐私准则》的核心价值,并且力图使隐私保护与社会需求、商业利益相协调,也适当承认成员方内部的文化多样性。第二部分澄清了亚太经合组织信息隐私原则涵盖的范围,并对某些重要概念提供了较准确的定义。例如,其将“个人信息”界定为关于某个已识别或可识别的个人的任何信息,同时通过评注的方式将单独看不符合这一定义但与其他信息结合时可以确定个人身份的信息也纳入进来。通过对这些适用对象尽可能地精确界定,《隐私框架》基本厘清了自身的适用范围。第三部分规定了 9 项核心的信息隐私原则,分别是预防损害、通知、收集限制、使用限制、保障选择权、个人信息的完整性、安全保障、访问和更正的权利以及可问责性。第四部分涉及《隐私框架》的实施问题,既建议成员方在境内实施该框架时应考虑的措施,也规定了实施《隐私框架》的制度安排。与《隐私准则》一样,《隐私框架》也缺乏强制实施的法律效力,只是咨询性的,[③]但不管是在理论上还是在实践中,国际软法并非都完全得不到实施。《隐私框架》本身就旨在以可适应各种实施机制的灵活方式来实施,因为它本身就预设了亚太经合组织成员方在法律和文化上的多样性。

(三)评价

虽然以《隐私准则》和《隐私框架》为核心的国际数据保护软法框架已经成为大多数国家制定国内数据保护法律的基石,但是这并不意味着它们就是完美的。考虑到《隐私框架》声称它符合《隐私准则》的核心价值的说明并非某种修辞,其信息隐私原则也与《隐私准则》的 8 项基本原则

① 参见张继红:《个人数据跨境传输限制及其解决方案》,《东方法学》2018 年第 6 期。

② See Catherine Valerio Barrad, Alan Charles Raul, APEC Overview, in Alan Charles Raul ed., The Privacy, Data Protection and Cybersecurity Law Review, Law Business Research Ltd., 2014, p.20.

③ See Catherine Valerio Barrad, Alan Charles Raul, APEC Overview, in Alan Charles Raul ed., The Privacy, Data Protection and Cybersecurity Law Review, Law Business Research Ltd., 2014, p.20.

存在许多相似之处，[①]因此两者的不足也有高度的同质性。从总体看，经合组织专家组在2013年修订《隐私准则》时虽然提出了对同意、目的特定化和使用限制等原则的疑虑，但是并没有提出任何明确的指导以及在这个时代需要作出怎样的改变。[②] 换言之，尽管经合组织对数据利用和挖掘产业如火如荼的发展状况十分清楚，坚持原先的基本原则可能会阻碍数据的自由流动和进一步挖掘应用，但是基于各方面的考虑，它还是选择了一种稳健的方式来更新《隐私准则》。

具体来说，这些不足表现为以下几点：(1)事前同意只能作为保障机制的一种手段而不是数据行为合法性的所有依据。《隐私准则》和《隐私框架》对弱化数据收集、事先告知和同意原则的时代要求回应不足，对数据使用中的效益和风险的实践评估也关注不够。(2)《隐私准则》和《隐私框架》既然仍固守以数据主体的同意为基础的收集限制原则，就必然要求数据处理者要受特定数据处理目的的严格限制。但正如同意原则作为一种实质的事先判断既缺乏真实性又不符合经济考量一样，[③]数据使用行为受目的特定原则的严格限制既阻碍了数据的自由流通、妨碍了创新，也对数据处理者设置了超出合理限度的认知要求。(3)虽然《隐私框架》的制定受到《隐私准则》的深刻影响，但是两者在数据跨境流动议题上的立场仍存在分歧。经合组织曾在一份报告中坦承成员方对保护个人数据的共识难掩各方围绕个人数据保护和促进数据流动间的矛盾。[④] 而就亚太经合组织的数据跨境流动实践看，因其规则是以美国为主导制定的，故鲜明地表达了美国通过市场的自问责机制而非设立数据流动的高门槛限制来保护个人数据的政策主张。[⑤] 这种价值分歧在很大程度上是以欧盟为主导的基于地理位置的数据转移政策与以美国为主导的基于对数据控制者问责的数据转移政策间发生冲突的体现。这种冲突甚至渗透到亚太经合组织内部，使得成员方可以基于本国法规定和安全需求拒绝某些执法合作。虽然这是主权原则和软法的基本性质附带产品，但是它加剧了以《隐私框架》等为代表的国际数据保护软法的内部矛盾，弱化了这些规则的实践效果，因此未来有必要通过这套软法规则内嵌于市场结构中的某些实施机制来缓和这种矛盾，尽可能实现数据跨境流动规则的统一。

---

① 参见施佳倩：《OECD个人数据保护原则的形成、影响和现代化》，载高富平主编：《个人数据保护和利用国际规则：源流与趋势》，法律出版社2016年版，第16页。

② 参见《21世纪的数据保护原则——OECD1980年〈指南〉的修正》，施佳倩译，载高富平主编：《个人数据保护和利用国际规则：源流与趋势》，法律出版社2016年版，第43页。

③ 同意的真实性是同意成为个人数据处理正当性基础的关键。根据《欧盟个人数据保护指令》设立的工作组和后来的欧洲数据保护委员会都规定了同意合法有效的标准，即同意必须是清楚而不含糊的意思表示，必须自由作出，必须明确，必须在获得充分告知的情况下作出。See EDPB, Guidelines 05/2020 on Consent Under Regulation 2016/679, Version 11, Adopted on 4 May 2020. 其中最关键的两个标准是自由作出和事前充分告知。但在实践中，数据主体基本上缺乏对个人数据的决定自由和控制能力，难以作出自由的同意。事前充分告知在现实中更难以获得保证。在数字经济时代，个人数据有重大的经济价值。同意原则在很多场合不合理地增加了个人数据处理的成本。在个人数据的处理方式和目的日益多样化的过程中，数据处理者将面临无休止的告知并须取得数据主体同意的情况，不仅束缚了经济创新，而且在数据处理者缺乏告知并征求数据主体同意途径的情况下，同意原则不仅带来高昂成本，而且事实上也不可能。此外，僵化地坚持同意原则还会给数据主体自身带来成本上升和不必要的骚扰等弊端。因此，有必要对同意原则进行反思。参见任龙龙：《论同意不是个人信息处理的正当性基础》，《政治与法律》2016年第1期。

④ See OECD, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, OECD Digital Economy Papers, No. 176, OECD Publishing, 2011.

⑤ 参见王融：《大数据时代数据保护与流动规则》，人民邮电出版社2017年版，第266～267页。

三、国际数据保护软法的模式约束和建构原则

国际学术界对软法谱系的追溯,存在两种不同的观点,形成了两种不同目标主导下的规制模式——侧重效率的软法规制与侧重安全的软法规制。全球税收治理与全球食品安全领域的软法实践分别是这两种模式的典型代表。作为国际软法家族的后来者,国际数据保护软法的建构不可能脱离这些成熟的国际软法实践模式而独立自在地生成,而是必然要根据自身的问题背景和实际需求选择合理的模式作为建构的蓝本。同时,在这一过程中,真正塑造国际秩序的主权国家也必然会出于本国主体性原则对建构模式的选择和生成施加不同的影响。中国也不例外。

(一)两种软法谱系及其目标侧重:当代国际软法的成熟实践

第一种谱系将软法的起源追溯至中世纪的法律多元和商法实践;第二种谱系则视软法为晚近时代的产物,将其与社会法的概念以及由欧洲反形式主义法学家在 19 世纪末及其后发展起来的法律多元主义相联系。① 在实践效果上,前者侧重效率,后者侧重安全。

1.侧重效率目标的新中世纪谱系。据这一谱系学者的描述,类似中世纪的法律多元化,当代软法的自发和源于事实的本性使得全球性法律多元主义也被认为是自由和效率的来源,具有深度组织性且能提供最终的保护。② 软法强烈的事实性就是灵活和效率的保证。由于经济软法依据全球贸易和组织的需要发展和演变,在回应全球经济活动者利益时具有可塑性,因此软法可以高效地适应快速变化的经济需求。这种将软法的起源追溯至中世纪的法律多元并且在规制目标上侧重效率的模式较为典型地体现在软法在全球税收治理领域发挥的作用中。这是因为该领域软法工具的首要目标是追求效率——有效打击各种逃避税行为,确保合理税收——而非保护纳税人的权利。如今,全球治理正在向一种由 20 国集团(G20)、国际组织和联合国组成的"耦合三角"的新兴治理结构转型。③ 这种新兴治理结构在全球税收治理领域替代性地发挥了推动多元主体参与的作用,使那些游离于由条约、协定等硬法构成的全球税收治理体系之外的国家始终难以脱离全球税收治理的软法治理进程。正是在这个层面上,"软法治理将主要依赖由多元主体所形成的网络治理结构及其功能运作,这些治理结构及其功能为全球税收治理中的软法治理提供了一种重要的'功能约束力'",④使软法治理有了实质效果,趋于高效率的"硬法化"。由此观之,也正是由于这套软法机制对效率的强调符合大多数国家对反逃避税行为的实践需求,税收透明度和信息交换的国际标准才得以迅速在全球适用,从而使国际税收软法具备了逐步转化为条约、国际习惯和国内法等硬法的可能性。

2.侧重安全目标的社会谱系。社会谱系的学者是从工具论的维度来理解软法的,将其视为实施一项新社会政策的有效手段。从该观点产生的背景看,社会谱系源于人们认识到欧洲一体化在促进市场效率与着力于社会保护两个方面的不对称性,⑤认为软法是对过度经济自由化的

① See Anna di Robilant, Genealogies of Soft Law, 58 Scandinavian Studies in Law, 219 (2017).

② See Anna di Robilant, Genealogies of Soft Law, 58 Scandinavian Studies in Law, 231 (2017).

③ 参见刘衡:《国际法之治:从国际法治到全球治理》,武汉大学出版社 2014 年版,第 65 页。

④ 崔晓静:《全球税收治理中的软法治理》,《中外法学》2015 年第 5 期。

⑤ See Fritz W. Scharpf, The European Social Model, 40 Journal of Common Market Studies, 645－665 (2002).

社会矫正机制。因此,以社会安全为目标的社会法领域是软法社会谱系实践的重要场域,其中食品安全监管中的国际软法实践最典型地体现了作为社会矫正机制和政策工具的软法的社会安全指向。20世纪中叶以前,食品安全监管仍是各国国内法的规制领域,随着第二次世界大战之后跨国食品贸易的迅速增长,食品安全风险的国际化趋势才愈发明显。迄今为止,通过相关国际组织决策、国际判例、执法的国际协调和市场竞争等途径,国际社会已经围绕食品生命周期建构起覆盖种养殖、加工、流通和消费等食品安全全链条的系统性软法规制体系。其中最典型的莫过于国际食品法典委员会制定的国际标准。这些标准虽然具有较强的技术性,但是在这一特征背后深藏着消弭安全风险、追求社会安全的价值目标,而该目标正是通过作为食品安全国际软法体系理论前提的食物权的保障得以体现的。在国际人权法中,食物权最早是作为"相当生活水准"和生命权的构成要素,《经济、社会及文化权利国际公约》第11条首次将其作为一项独立、自成一体的基本权利进行明确规定。[①] 食物权在数量和质量上都有最低限度的要求,前者表现为粮食安全,后者表现为食品安全,食物权也就相应转化为确保粮食和食品的安全。[②] 食品安全国际软法体系的社会政策目标和人权指向不仅是学理主张,而且也得到国际软法实践的贯彻实施。联合国粮农组织于1992年通过的《世界营养问题宣言》就明确提出每个个体均享有充足、安全和营养的食物的权利,尔后该权利在《关于世界粮食安全的罗马宣言》《2002年世界粮食峰会宣言》《2007年食品安全北京宣言》中得到重申,并形成人权保护进入食品安全监管国际软法领域的趋势。在此意义上,技术性绝非食品安全国际软法体系的本质特征,其在根本上是作为一种通过确保人人对食物权的享有来追求社会安全的政策工具,而其技术性的面向只是用以实现这一目标的有效途径。

(二)前提性的建构原则:本国主体性原则

理论建构和实践操作不可能脱离既有的学术积累和社会结构。作为国际软法家族中的年轻一员,国际软法实践中的两种谱系是国际数据保护软法产生发展过程中难以规避的前提环境和结构约束。从某种意义上讲,效率与安全间的矛盾在数据保护领域就体现为数据的自由流动与本地化存储以及隐私保护间的矛盾。但谱系的提炼只是韦伯意义上的"理想类型"而非实践的客观再现。各国对逃避税行为的合作打击不可能完全忽视对纳税人财产和迁徙自由的保护,粮食的自由贸易也在很大程度上更有利于解决食品的短缺和安全问题。因此,从数据自由流动到严格的本地化存储是一个渐变的光谱,两者之间存在无数种可能性。例如,在数据出入境问题上,非洲集团、俄罗斯、土耳其等注重安全管控,加拿大、日本、韩国和拉丁美洲一些国家则偏爱自由流动。[③] 因此,各国在数据保护和流动问题上的政策选择以及由此塑造出的国际数据保护软法框架,也必定处于一种自由与安全之间的动态平衡关系之中。但这种动态平衡关系在根本上受制于各国在国际数字经贸格局中的现实地位、发展潜力和利益追求。欧盟长期坚持高标准的隐私保护政策,在数据跨境流动议题上对第三国设置严苛、充分的保护条件,正是源自其数字经济

① 参见陈亚芸:《〈经济、社会及文化权利国际公约〉食物权法律解析》,《北方法学》2010年第6期。

② See Kerstin Mechlem, Food Security and the Right to Food in the Discourse of the United Nations, 10 European Law Journal, 642 (2004).

③ See Nivedita Sen, Understanding the Role of the WTO in International Data Flows, 21 Journal of International Economic Law, 341 (2018).

竞争力落后于中美两国。[①] 因此,在讨论国际数据保护软法及其实施机制的建构问题时,首先必须坚持本国主体性原则,即基于我国数字经济现状和发展趋势来参与和推动国际数据保护软法及其实施机制的塑造。考虑到信息技术的突飞猛进给全球数字经济带来的极大不确定性,认真对待本国主体性原则显得更为必要。

坚持本国主体性原则,既是历史唯物主义方法论的必然要求,也是基于数据的本质属性和我国数字经济国情的现实选择。从本质上看,数据既不稀缺,也是非竞争和高度差异化的,随着时间的推移,新数据的价值也明显超越老数据。因此,视数据为类似于石油、土地这样的资产并加以严格管控的做法背离了其作为"流动性财产"的性质。[②] 如今,数据已成为重要的生产要素。不论是个人、企业还是国家,如果仅仅是静态地占有数据而不是创造允许数据自由流动组合的环境,那么不可能创造出巨大的经济效益,只有自由流动和汇聚的数据资源才能形成潜在的数据智能。21 世纪的竞争优势必然是由重视使用数据资源并以前所未有的方式创造价值的数字战略决定的。[③] 因此,符合数据本质的未来数字战略应是更重视数据的自由流动和充分利用,而非过多关注数据的静态权属状态。

从我国的现实国情看,我国不仅在互联网数字技术领域抢得先机,而且数字经济规模已达 39.2 万亿元,仅次于美国位居全球第二,其他相关项指标也居世界前列。[④] 但中美两国的相对优势地位未能掩盖我国数字经济规模只有美国 1/3 的绝对差距。对此,不论是出于深化开放的考量,还是出于发挥数字经济潜能的考量,鼓励数据流动和利用而不是通过数据本地化存储来限制数据外流都应成为我国的基本立场和战略选择。[⑤] 从现实选择看,我国事实上已承认数据自由流动原则的基础性地位,网络主权并不否定网络空间的互联互通性、信息的自由流动性和创新性。[⑥]《中华人民共和国数据安全法》(以下简称《数据安全法》)第 11 条也将"促进数据跨境安全、自由流动"作为立法目的,比《中华人民共和国网络安全法》(以下简称《网络安全法》)第 12 条规定的"网络信息依法有序自由流动"更注重数据自由流动对经济社会发展的重大意义。上海市、海南省等地纷纷探索数据跨境流动的便利化措施,贵州省甚至提出了建设"数字丝路跨境数

① 参见田晓萍:《贸易壁垒视角下的欧盟〈一般数据保护条例〉》,《政法论丛》2019 年第 4 期。

② 参见许可:《自由与安全:数据跨境流动的中国方案》,《环球法律评论》2021 年第 1 期。

③ See Geoffrey A. Manne, R. Ben Sperry, The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework, 5 CPI Antitrust Chronicle, 8－9 (2015).

④ 参见中国网络空间研究院:《中国互联网发展报告(2021)》,https://www.isc.org.cn/article/40203.html,2021－09－12;中国信息通信研究院:《全球数字经济白皮书——疫情冲击下的复苏新曙光》,http://www.caict.ac.cn/kxyj/qwfb/bps/202108/P020210913403798893557.pdf,2021－09－12。

⑤ 参见许可:《自由与安全:数据跨境流动的中国方案》,《环球法律评论》2021 年第 1 期。也有国家采用限制数据跨境自由流动的政策打击美国网络巨头的竞争优势,扶持国内产业。参见洪延青:《在发展与安全的平衡中构建数据跨境流动安全评估框架》,《信息安全与通信保密》2017 年第 2 期。但欧洲国际政治经济研究中心研究发现,采用限制数据跨境流动的管控措施会对一国实际国民生产总值造成损失,欧盟、印度和中国分别损失国民生产总值的 0.48%、0.25%和 0.55%。参见洪延青:《构建〈网络安全法〉数据跨境安全评估的总体框架》,载李林、支振锋主编:《中国网络法治发展报告(2019)》,社会科学文献出版社 2020 年版,第 59～60 页。

⑥ 参见武汉大学、中国现代国际关系研究院、上海社会科学院等:《网络主权:理论与实践(2.0 版)》,http://www.cac.gov.cn/2020－11/25/c_1607869924931855.htm,2021－01－14。

据自由港”的目标。[①] 基于这一时代背景和发展逻辑，一个自由开放的全球数据市场对我国显得至关重要；而作为全球第二大数字经济体和重要的数据利用和生产国，我国既有对数据自由流动的主观需求，也有吸引大量高价值数据流入的实际能力。当然，数据自由流动也会产生某些风险和外部效应。首先，从《数据安全法》第 11 条的语义看，将“安全”理解为对自由流动的限制条件也不无道理，但这种理解也蕴含了数据自由流动本身所应当具有的基础性地位。其次，不论是《数据安全法》第 3 条“有效保护和合法利用”的规定，还是《中华人民共和国国家安全法》第 25 条“网络和信息安全”的规定，抑或《网络安全法》第 12 条对“宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息”的禁止性规定，都表明“安全”只有实现了类型化才能成为数据自由流动的限制条件。从此种意义上讲，数据自由流动是原则，以安全为条件的管制则是例外。最后，在经济全球化时代，数据可信早已成为数据安全的关键内容，但仅单方面赋予个人数据权利并不能有效重塑信任关系。只有引入“信义规则”，同时承认用户和企业的利益，既将企业从“动辄得咎”的境地中解放出来使其能最大化数据价值，又能通过信义义务使其勤勉忠实地善待用户，[②]才能有效实现对数据自由流动的软约束。从此种意义上讲，正如下文所要强调的那样，通过对市场机制的挖掘和利用，数据的高效自由流动恰恰实现了数据的安全保障。

因此，基于我国现阶段的客观需求和未来的发展趋势，当前我国应在选择侧重效率的同时兼顾安全的软法谱系，努力发掘既有规则中有利于数字经济自由开放的因素，推动建构促进数据自由流动的国际数据保护软法框架。

四、国际数据保护软法的建构：一种“外部－内部”双层实施机制的提炼

目前，以《隐私准则》和《隐私框架》为核心的国际数据保护软法框架正逐步形成多层次、立体化的实施机制。这些实施机制要么是国际数据保护软法自身确立的，要么是借助了成员方的制度和力量。从这种意义上讲，本文将其提炼为一种“外部－内部”双层实施机制。不可否认，两者间并非泾渭分明，而是存在或明或暗、或强或弱的关联性。例如，经合组织理事会关于隐私执法的跨国合作建议本身虽然不具有强制执行的法律效力，但往往会借助成员方对内部框架的审查而得到执行，从而使《隐私准则》获得实施。前文已述，中国对国际数据保护软法建构的参与应以在兼顾安全的同时更侧重效率的软法谱系为蓝本，推动以《隐私准则》和《隐私框架》为主体的国际数据保护软法框架朝着有利于数据在全球市场自由高效流动的方向发展。因此，在这种“外部－内部”双层实施机制之下，中国除了为促进数据跨境流动而加入亚太经合组织《跨境隐私规则》之外，还应关注内嵌于市场结构中的实施机制，从而有效地发挥这套软法框架促进效率并兼顾安全的功能。

（一）外部层面的实施机制：以隐私执法机构为核心

外部层面的实施机制是指《隐私准则》和《隐私框架》自身确立的实施机制，具体是指经合组织的跨境合作建议和亚太经合组织的《跨境隐私规则》。这两项机制都是以各成员方的隐私执法

① 参见谌贻琴：《贵州省政府工作报告——2020 年 1 月 15 日在贵州省第十三届人民代表大会第三次会议上》，《贵州日报》2020 年 3 月 2 日。

② 参见许可：《自由与安全：数据跨境流动的中国方案》，《环球法律评论》2021 年第 1 期。

机构为核心建构起来的实施网络,而这种以成员方隐私执法机构作为实施机制核心的建构原则实际上是一种典型的“搭便车”实践,从长远看,其沟通了国际软法与成员方内部硬法,从短期看,其强化了这一机制本身的效率指向。

根据 2006 年执行报告的调查结果,经合组织理事会于 2007 年通过了关于就隐私执法开展跨境执法合作的框架的建议。为落实该建议,经合组织建立了一个全球隐私执法网络,旨在回应隐私问题跨境执法中面临的挑战,加强跨境隐私保护联合执法合作。① 经合组织全球隐私执法网络是一个包容各方的合作网络,任何负责执行具有保护个人数据作用的法律法规,以及有权展开调查或启动执法程序的成员方隐私执法机构都能加入该网络。与此类似,为促进《隐私框架》的统一执行,亚太经合组织电子商务指导组下设的数据隐私分组在 2012 年构建了《跨境隐私规则》,并引入隐私执法机构和问责代理机构,从而对加入的企业形成了实际的约束力。②《跨境隐私规则》是一个基于自愿问责的以涉及个人数据跨境流动的企业为规制对象的规则体系。它要求企业根据符合或高于《隐私框架》的标准制定其内部的隐私规则,管理个人数据的跨境流动。为保证加入《跨境隐私规则》的成员方能够按照《隐私框架》的要求监管本国企业,亚太经合组织还在 2010 年构建了颇具特色的跨境隐私执法安排。作为《跨境隐私规则》设定的准入条件,申请加入的成员方至少要有一个隐私执法机构加入跨境隐私执法安排,且该隐私执法机构还必须是在成员方境内切实拥有针对框架 9 项信息隐私原则的执法权的公共机构。作为多边机制,各成员方的隐私执法机构可以通过跨境隐私执法安排共享信息,协商开展平行或联合调查执法。但由于《隐私框架》和《跨境隐私规则》本身缺乏法律强制力,只有成员方执法机构有权处罚违反框架的本成员方企业,因此跨境隐私执法安排更突出的功能实际上是提供了一个跨境执法的监督和协作机制,“既然一成员方在申请加入《跨境隐私规则》体系前派出了执法代表机构,并且承诺对违反该规则的认证企业进行法律制裁,那么在其他成员方隐私执法机构发出协助要求时就不好偏袒本成员方企业”,③否则不仅变相鼓励了其他成员方今后不与自己合作,置自身执法机构于孤立的尴尬境地,而且还使得自身的问责代理机构及其认证的企业失去信誉,被排除在数据流动市场之外。

由于加入《跨境隐私规则》的前提是成员方至少要有一个拥有充分执法权的隐私执法机构加入跨境隐私执法安排,因此就使《跨境隐私规则》实际上强化了还没有制定数据保护法律的成员方参与企业提供的数据隐私保护;而对于已制定此类法律的成员方,由于企业必须遵守这些法律,因此《跨境隐私规则》也没有弱化对数据隐私的保护。换言之,那些与经《跨境隐私规则》认证的企业进行交易的人不仅获得了对方遵守一套国际公认的数据保护规则的承诺,而且在事实上还获得了在对方违规时要求强制执行的权利。同样的道理,虽然国际软法没有法律强制力,不是严格意义上的法律,不遵守不算违背,但是遵守软法显然会使相应的行为更具正当性。④ 因此,那些希望从已制定严格数据保护法律的国家获取数据的企业,如果参与《跨境隐私规则》,那么就

① 参见何波、石月:《跨境数据流动管理实践及对策建议研究》,《互联网天地》2016 年第 12 期。

② 参见黄宁、李杨:《“三难选择”下跨境数据流动规制的演进与成因》,《清华大学学报》(哲学社会科学版)2017 年第 5 期。

③ 弓永钦、王健:《APEC 与欧盟个人数据跨境流动规则的研究》,《亚太经济》2015 年第 5 期。

④ 参见何志鹏、孙璐:《国际软法何以可能:一个以环境为视角的展开》,《当代法学》2012 年第 1 期。

更可能成为有吸引力的数据接收者。如此,“《跨境隐私规则》通过提供一套可扩展的隐私底线标准,不仅有力促进了全球贸易和经济增长”,①而且在寻求个人数据的隐私保护与自由流动的平衡方面提供了有益经验。因此,以经合组织的跨境合作建议和亚太经合组织的《跨境隐私规则》为代表的国际数据保护软法的国际实施机制虽然是围绕各成员方的隐私执法机构进行建构的,但是在机制设计上却较好地实现了“外部—内部”两个规制层面的激励相融,从而借助成员方隐私执法机构的力量提高了自身的实施效率。

(二)内部层面的实施机制:以市场为进路

除通过自身确立的机制在外部层面加以实施之外,作为国际数据保护软法的《隐私准则》和《隐私框架》还通过审查成员方内部框架、促进立法、建立隐私执法机构、推动行业自律和建立隐私管理程序等成员方内部措施得到实施。审查成员方内部框架是指成员方“根据需要审查并酌情调整其国内框架,以确保在执行保护隐私的法律方面进行跨境合作的有效性”,②是典型的通过成员方自身的制度和能力实施《隐私准则》的成员方内部机制。与此类似,促进成员方立法和建立隐私执法机构也在很大程度上依赖成员方的主动配合。这既是由“外部—内部”两个层面的实施机制本身具有的内在关联性决定的,又是由软法的基本性质决定的。但在以《隐私准则》和《隐私框架》为核心的国际数据保护软法框架的一系列成员方内部实施机制中,仍然存在诸如激励行业自律和建立隐私管理程序这样的对本成员方法律及其强制力依赖较低的内部实施机制。激励行业自律和建立隐私管理程序之所以是国际数据保护软法的内部实施机制,是因为它们的实施要借助成员方的内部力量;而它们之所以对成员方的依赖又较低则是因为它们更多地刺激了成员方内部市场结构而非官方强制力量对数据保护的回应性机制,在较大程度上实现了对数字经济企业和产业的内部激励相融,从而有效地促进了数据的跨境流动和自由贸易。

1.激励行业自律。经合组织理事会建议通过鼓励行业自律的方式实施隐私准则。《隐私准则》第19(d)段关于自律的建议主要针对普通法系成员方。在这些成员方中,准则的非立法性实施将对成员方内部的立法起到补充作用。事实上,《隐私准则》已成为诸多私营部门隐私政策、自律政策和示范守则的基础,一些公司和贸易协会也赞同该准则。从概念的内涵看,自律是指“行业层面的组织(如行业协会),而不是政府或公司,制定和实施与该行业内企业行为有关的规则和标准的监管过程”,③以应对政府的监管缺位或监管过度。

行业自律具备特定的优势。规则制定、监督、执行和救济的整个过程可以通过自律而非政府监管得到更快的运转,这也意味着消费者利益能更快地得到保护。不仅如此,也有学者指出,自律组织在规则制定方面比政府更高效,因为当企业聚集在一起制定规则时,其间的参与方可能比外部的监管机构拥有更专业的技术和行业知识。④ 众所周知,包括立法和执法程序在内的政府

① See Annelies Boens, Malcolm Crompton, Preliminary Assessment: Potential Benefits for APEC Economies and Businesses Joining the CBPR System, 2016, APEC Secretariat, p.7.

② See OECD, Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protection Privacy, http://www.oecd..org/sti/ieconomy/38770483.pdf. 2021-04-14.

③ See Anil K. Gupta, Lawrence J. Lad, Industry Self-regulation: An Economic, Organizational, and Political Analysis, 8 Academy of Management Review, 417 (1983).

④ See Daniel Castro, Benefits and Limitations of Industry Self-regulation for Online Behavioral Advertising, The Information Technology&Innovation Foundation, December 2011, p.6.

监管是成本和资源密集型事业,而将这些职能让渡于行业自律组织则意味着能以更低的成本更快地调查和治理违规行为。这不仅培育了市场自治,而且"有利于减少政府的监管负担,使其将有限的精力集中于更有成效的事务上,如对拒绝遵守规则的不良行为人采取行动"。① 通过营造通常比政府监管更灵活的监管环境,行业自律也有助于经济发展。自律要求行业专家审查当前的活动,确定最佳的实践,并将其发展为行业准则。这种更灵活的监管环境能使企业更有效地运营,并将合规成本最小化。事实上,政府机构也承认,"行业自律可以用比直接监管更灵活、更具成本效益的方式保护隐私安全,同时也不妨碍互联网产业的快速创新"。②

但通过行业自律来实施国际数据保护软法也面临以下批评:(1)出于对行业私利的追求,自律机制比传统规则的透明度更低,公共利益难以被充分代表;(2)自律机制缺乏制裁违规行为的必要权限,致使其外部威慑不足;(3)行业内集体行动的困境会带来"搭便车"的难题。③ 从此种意义上讲,行业自律不应当取代适当的立法措施,或者说,一个更有效的解决方案是采取共同监管,即"政府和行业共同起草并执行监管标准"。这是一种政府规制与非政府规制相结合,介于自我监管与政府规制之间的合作规制。④ 这种意义上的行业自律完全能够与政府的数据保护立法共存。根据《隐私框架》的建议,亚太经合组织的成员方可以制定全面的数据保护法律,但考虑到将受此类法律影响的各个部门和行业,可以预见此类法律无法涵盖所有行业,特别是高度专业化行业所必需的数据保护规则。由于各行业处理信息类型的敏感程度不同,因此除了使某一部门的数据处理业务不同于其他部门的其他因素外,还需要对特定类型的实体制定专门规则。在这一方面,行业自律恰好可弥补政府立法的不足。这也正是《隐私框架》额外强调通过行业自律和立法、行政途径相结合的方式使自身获得实施的意义之所在。此外,执法也可由此意义上的行业自律而获得进一步的改善。除了前述减少了政府机构的监管负担的收益之外,由于政府严厉惩罚违规者的概率增大,因此遵守数据保护规则的强制力将更强。事实上,行业自律与某种政府干预相结合的共同监管是对实现内部治理和外部威慑激励相容的积极探索,带有典型的合作治理色彩,⑤要比单纯的自律更有效率。这种意义上的行业自律除了体现在《欧盟条例》有关数据跨境传输机制的创新上,事实上在国际软法层面就通过《隐私框架》的影响在菲律宾催生出积极的成果。作为亚太经合组织的成员方,菲律宾在 2012 年制定了《数据隐私法》,并于 2016 年设立了国家隐私委员会作为隐私执法机构。⑥ 根据该法,鉴于监管医疗卫生行业数据处理活动的复杂性,该委员会目前正在努力召集政府和行业代表,以便合作起草用以规制该行业的数据处理活动的专门规则,而这些规则也旨在对综合性的数据隐私法律作出有益的补充。

---

① See Daniel Castro, Benefits and Limitations of Industry Self－regulation for Online Behavioral Advertising, The Information Technology&Innovation Foundation, December 2011, p.7.

② Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, 6 I/S: A Journal of Law and Policy for the Information Society, 356 (2011).

③ See Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self－regulation, or Co－regulation?, 34 Seattle University Law Review, 458－459 (2011).

④ 参见匡文波、杨春华:《走向合作规制:网络空间规制的进路》,《现代传播》2016 年第 2 期。

⑤ 参见周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018 年第 2 期。

⑥ See Michelle Renee D. Ching, Bernie S. Fabito, Nelson J. Celis, Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance, 24 Advanced Science Letters, 7042 (2018).

2.建立隐私管理程序。随着《隐私准则》的制订,问责制作为促进和确定组织对隐私保护的责任的手段越来越受到关注。在这一经验的基础上,2013 年修订的《隐私准则》在有关“实施问责制”的第三部分引入了隐私管理程序的概念,并阐述了其基本要素。同样地,《隐私框架》也将隐私管理程序与对数据控制者的问责相联系,并将其作为该框架的内部实施机制之一。隐私管理程序的概念主要是针对数据控制者面临的数据泄漏等安全风险日益增大的现实提出的。一般来说,它包括各类组织为确保个人数据得到适当保护、风险得到管控、隐私立法得到遵守而采用的政策、程序和制度。这意味着 20 世纪 90 年代发展起来的隐私影响评估也被纳入组织的风险管理当中,帮助组织分析数据的生命周期,从而在引入新技术或计划之前就考虑到隐私问题,并通过报告、审计、教育和绩效评估促进问责制。事实上,这也恰是这些软法规则多将隐私管理程序与问责原则相联系的重要原因。具体而言,综合《隐私准则》和《隐私框架》的规定,隐私管理程序的最基本要素主要包括:(1)针对数据控制者的结构、规模及其控制的数据数量和敏感程度进行定制,(2)提供基于风险评估的适当保障措施,(3)建立内部监督机制,(4)程序本身应当定期监测和评估更新。全面的隐私管理程序为数据控制者与监管机构和数据主体进行良好沟通提供了有效方式,也是数据控制者判断自身是否合规的工具,使其有机会查漏补缺,从而在整个组织内部培育一种隐私文化。这就使“拥有强大隐私管理程序的组织可能享有更高声誉,从而具有市场竞争优势”。[①] 换言之,从长远看,成功向外界传达出稳健的隐私管理程序对其运营至关重要的组织更容易强化利益相关者的信任,也更容易展现出良好的商业前景。

基于《隐私准则》和《隐私框架》的建议和影响,加拿大、法国和澳大利亚等国发布了“问责指南”或“隐私治理框架”,旨在协助私营部门(在某些情况下也包括公共部门)建立确保隐私合规的程序。[②] 如果这些“指南”“框架”得到广泛传播,那么不仅有助于向数据控制者灌输有关隐私管理程序的知识,而且更重要的是,由于它们都是免费资源,因此对数据控制者来说就是建立定制化的隐私管理程序的无成本方法。加拿大的指南认可隐私管理程序作为确保隐私合规的工具。根据这些指南,全面隐私管理程序的两个关键要素是组织承诺和程序控制。这些指南在具体内容上大多都借鉴了《隐私准则》和《隐私框架》关于隐私管理程序基本要素的规定,勾勒了这一程序的重要特征(如任命数据官员、建立内部报告机制等)以及为使程序发挥作用而采取的步骤(如进行个人数据清查、制定保护警示政策、定期进行风险评估以及采用隐私设计[③])等。

---

① See Office of the Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Alberta and British Columbia, Getting Accountability Right with a Privacy Management Program, http://iapp.org/media/pdf/knowledg_center/canada-Getting-Accountability-Right(April 2012)pdf, 2021-01-14.

② See Anna von Dietze, Privacy Accountability: National Regulators' Accountability Guidance (Part 1), https://www.lexology.com/library/detail.aspx? g=c0de3d1c-2e8e-402c-a1cd-07677527ac9a, 2019-12-13; Theo C. Ling, National Regulator Accountability Guidance (Part 2): The Australian and French Accountability Guides, https://www.lexology.com/library/detail.aspx? g=9dfbd348-0391-4c90-9d3f-ca3004081270, 2019-12-13.

③ 隐私设计,也称从设计着手保护隐私,是与隐私影响评估相对应的另一种隐私保护理念。隐私影响评估原是评估特定制度或技术的隐私后果的系统过程,而隐私设计比隐私影响评估更全面,是“将公平信息实践原则纳入信息技术、业务实践,以及物理设计和基础架构”的过程。换言之,它是系统工程的一种方法,要求在整个工程过程中都要考虑隐私保护。See Yoel Raban, Privacy Accountability Model and Policy for Security Organizations, 4 iBusiness, 169 (2012). 然而如今,隐私影响评估的发展逐渐有涵盖隐私设计的趋势,逐步推动相关组织在引入新的技术和规划之前将隐私问题纳入考量。

相比之下,澳大利亚和法国的指南没有明确提及或促进隐私管理程序的实施,但在实质内容方面,法国指南和加拿大的实践大体相似,也包括建议制定充分的内外部隐私政策、任命经过培训的数据保护官员、开展隐私问题培训、进行隐私风险评估等,而其中值得关注的一项创新做法是证明符合指南中 25 项要求的公司将获得合规性责任印章。① 这种印章与前述《跨境隐私规则》体系中问责代理机构对企业进行认证后授予的隐私保护信赖标章具有异曲同工之妙,实际都是面向市场的信号,强化了公众对其在提供产品或服务过程中保障用户数据隐私的信心。除了激励数据控制者遵守问责指南的要求外,获得隐私印章的过程还为数据控制者提供了道德和法律框架,证明了他们负责任地创新和处理个人数据的意愿,并通过引入问责制的概念帮助他们遵守区域数据控制保护软法框架。这实际上是一种基于市场声誉机制的隐私认证制度,能更充分地调动数据控制者主动参与的积极性。

事实上,通过问责制对隐私管理程序的嵌入,这种认证制度已经逐渐演变成一种相对独立和广泛的国际数据保护软法实施机制。由于隐私专业人员在实施隐私管理程序中的作用越来越重要,因此界定专业人员的能力就成为认证制度最初关注的焦点,德国、加拿大、新西兰以及欧盟等国家或地区已开始推行数据保护和隐私领域的认证项目,并开展这方面的专业教育和职业发展服务。这本身也可看作是成员方对《隐私准则》第 19(g)段的落实,该段要求成员方考虑隐私保护所必要的技能发展。在这方面,值得注意的是加拿大的访问及隐私协会专业标准和认证项目。该项目通过制定专业标准、建立认证模型和认可有能力实施隐私管理程序的治理团队来实现“将信息访问和隐私保护专家确立为加拿大的公认职业”的目标。在各成员方的实践基础上,成立于 2000 年的国际隐私专业人员协会也提供了 3 种类型的认证计划以及职业教育和发展服务,旨在定义、促进和改善全球隐私职业和隐私保护状况。基于《隐私准则》第 19(g)段的桥梁作用,认证制度的声誉机制和信号功能促进了隐私管理程序对隐私增强技术的需求,迫使技术的生产者和使用者将设备的能力和设备的合法性视为不可分割的整体,从而激励他们将强化隐私保护作为技术的积极方面。换言之,通过将内置隐私增强技术作为各种设备和技术的法律要求,生产商“将被迫面对这些问题,并与潜在客户进行谈判”。② 如此一来,随着时间的推移,这些价值观不仅被内化为产品的成本,也被内化为消费者的决策,从而内生出一种尊重和保护数据安全、促进数据流动的市场结构。

五、结 语

效率和安全永远是法律要加以协调平衡、不可偏废的基础价值。在数据保护问题上,国际社会也始终面临数据的隐私保障、本地化存储和自由流动的价值抉择。从根本上讲,这种基础价值的立场倾向受制于行为主体的物质基础和利益追求。从这一立场出发,便可理解数据保护议题

① See Johanna Carvais－Palut, The French Privacy Seal Scheme: A Successful Test, in Rowena Rodrigues, Vagelis Papakonstantinou eds., Privacy and Data Protection Seals, Springer, 2018, pp.49－58.

② See Benjamin J. Goold, Building It in: The Role of Privacy－enhancing Technologies in the Regulation of Surveillance and Data Collection, in Benjamin J. Goold, Daniel Neyland eds., New Directions in Surveillance and Privacy, Willan Publishing, 2013, p.29.

背后实质上隐藏的是抢占新一代全球经济和技术革命先机和话语权这一国家间生存竞争的重大问题，这使得国际社会在诸如此类新兴全球性治理问题上很难形成各方普遍接受的硬法规则。不仅如此，即便是经历数年艰难谈判而来却仍只作为满足现阶段紧迫需求的权宜之法的美欧《隐私盾协议》也难逃被欧盟法院以不具同等数据保护水准为由推翻的命运，[①]现阶段也更不具备直接通过国际组织平台形成有约束力的数据跨境流动规则的客观条件。[②] 在此背景下，通过某些非机构性多边协调机制形成一些区域性软法规则便成为一种次优的选择。

通过对当前国际软法谱系的学理归纳，可大致提炼出两种韦伯意义上的“理想类型”——侧重效率目标的新中世纪谱系和侧重安全目标的社会谱系，它们各自在全球税收治理和全球食品安全规制领域发展出相对成熟的实践。这也构成建构国际数据保护软法框架时不可回避的约束性结构。但这种“约束”不意味着非此即彼的选择，而是某种程度的此中有彼、彼中有此。从此种意义上说，以何种谱系作为主导而非绝对的模型来建构某阶段的国际数据保护软法框架从根本上说受制于本国数字经济的发展现状和未来趋势。我国现阶段应积极主动地以侧重效率同时兼顾安全的软法规制模式为蓝本对既有国际数据软法规则加以型塑和建构，努力发掘其中有利于数据自由流动和数字贸易自由化的因素，以便为我国数字经济的发展创造自由、开放的数据市场环境。具体到数据保护议题方面，《隐私准则》和《隐私框架》就是典型的国际软法规则。虽然软法规则缺乏法律强制力，但是却可以集中资源将其吸引力聚焦于规制对象的内在逻辑和规则的内在理性，尽可能地将其实施机制内嵌于全球数字贸易的市场结构之中。不论是作为这些软法规则的国际实施机制的亚太经合组织《跨境隐私规则》，还是作为内部实施机制的行业自律、隐私管理程序等措施，都不同程度地内含这种事理逻辑。借助颇具特色的“外部－内部”双层实施机制，以《隐私准则》和《隐私框架》为代表的国际软法在为寻求数据安全保护和自由流动在实践中的平衡作了有益探索的同时，更为该领域的规则生成奠定了基础。

作为新兴数字经济大国，我国在互联网数字技术上已抢占先机，是重要的数据生产国。《网络安全法》第41条和《个人信息保护法》第13条等法律虽然都规定了同意原则，但是作为该领域的框架性和基础性法律，这些法律有关个人数据保护和流动的规范仍显简单。其中有关数据跨境流动的规则也仅限于《网络安全法》第37条关于进行安全评估的原则性规定和《数据安全法》第31条的准用和授权条款，而作为重要配套规则的《数据出境安全评估办法》仍处在征求意见阶段。基于此，我国有必要通过“软硬兼施”的办法加快数据保护规则体系的构建，在加快制定相关基础法律和完善我国司法机构域外管辖权[③]的同时，鼓励企业和行业组织借鉴国际软法规则完善自身隐私政策和规则体系。其实，可视为软法规则的推荐性国家标准《信息安全技术－个人信

① See Data Protection Commissioner v. Facebook Ireland Ltd., Maximillian Schrems, Case C－311/18, Judgment of the Court (Grand Chamber), 16 July 2020, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=645986, 2021－01－14.

② 参见张舵：《略论个人数据跨境流动的法律标准》，《中国政法大学学报》2018年第3期。上述引文中所说的“国际组织”并非一种广义概念，更多的是指联合国、欧盟等类型的国际组织，而不包括诸如亚太经合组织、经合组织等所说的“非机构性多边协调机制”。

③ 参见邵怿：《网络数据长臂管辖权——从“最低限度联系”标准到“全球共管”模式》，《法商研究》2021年第6期。

息安全规范》就具有较强的规范意义,对执法部门、司法机构和企业有重要的参照价值。[①] 作为亚太经合组织的重要成员方,我国也应当利用已相对成熟的《隐私框架》来补充和完善自身的数据保护法律体系,“指定或设立具体的数据保护机构,并授予该机构必要的执法权力,尽快申请加入亚太经合组织《跨境隐私规则》体系”。[②] 与此同时,随着我国国力的不断增强,也有必要在“一带一路”倡议、上海合作组织以及亚州基础设施投资银行等由我国倡议和参与构建的多边协调与合作机制中展开数据保护议题的对话与合作,促进机制内各国同我国数据业务的对接和发展,并在此基础上从构建多元兼容的软法规则入手,逐步提升我国在有关数据保护规则议题方面的国际话语权。

Abstract: Data protection is a common governance problem faced by international community, and the flexibility of law is the inherent demand to solve this problem in the digital era. Based on the objective reality of conflicting data protection laws in various countries, international soft law has become a sub-optimal option for strengthening data protection at the international level. Based on the analysis of the neo-medieval genealogy focusing on efficiency and the social genealogy focusing on social security, combined with the principle of national subjectivity, China should choose a soft law model that focuses on efficiency while taking into account safety as the blueprint, and actively participate in the international data protection soft law framework represented by OECD Privacy Guidelines and APEC Privacy Framework and its construction of external-internal two -layer implementation mechanism. China should consider joining CBPR system, improve the legal system of data protection through the combination of soft law and hard law, and promote the formation of diverse and compatible international soft law in the field of data protection in other multilateral coordination and cooperation mechanisms.

Key Words: data protection, privacy protection, international soft law

责任编辑 **何 艳**

① 参见冯洋:《从隐私政策披露看网站个人信息保护——以访问量前 500 的中文网站为样本》,《当代法学》2019 年第 6 期。

② 黄宁、李杨:《“三难选择”下跨境数据流动规制的演进与成因》,《清华大学学报》(哲学社会科学版)2017 年第 5 期。