法商研究 Studies in Law and Business
Vol. 39 No. 5(2022)

网络与信息法

数据隐私规制模式及其贸易法表达

彭 岳*

摘 要:数字经济时代,数字贸易越来越倚重于数据跨境自由流动。同时,为保护个人信息,各国采取措施对个人数据处理行为进行相应的规制。基于不同的隐私保护理念、立法政策和司法实践,美国、欧盟和中国分别形成了数据隐私一元规制、数据隐私二元规制和数据隐私分离规制3种模式。为缓和数据隐私规制不同模式之间的冲突,便利数据跨境自由流动,国际贸易协定主要通过贸易例外和贸易事项两种方式纳入数据隐私规制问题。不同数据隐私规制模式倾向于支持不同的纳入方式,而不同的纳入方式也会影响到不同数据隐私规制模式自主发展的空间。中国政府理应以国内法规定为基础,积极参与数字贸易规则谈判,通过国内法与国际法的良性互动,在现有的基础上细化中国方案,贡献中国智慧。

关键词:数据隐私 规制模式 数据流动 贸易例外 贸易事项

如何妥善处理好数据跨境流动与数据隐私保护之间的关系将直接影响到数字贸易的未来。在数字经济领域,美国、欧盟和中国的竞争日益激烈。就数据隐私保护而言,美国、欧盟和中国采取不同的立场和策略,形成了风格迥异的规制模式。各国和地区不同的规制模式必然增加个人数据跨境流动的合规成本,增大国际协调的难度。在此情况下,旨在寻求最佳利用世界资源的国际贸易法有必要作出制度回应,以在国际层面确立合作的框架、协调的方式和一致性的准则。

一、美国数据隐私一元规制模式

在美国法律体系下,隐私一开始就与个人信息保护问题息息相关。借助早期的司法实践、碎片化的部门立法和行业自律准则以及隐私权概念的持续理论构造,美国将数据隐私问题放置在隐私权的概念下加以处理,形成了自成一体的数据隐私一元规制模式。

* 南京大学法学院教授、博士生导师
基金项目:国家社会科学基金一般项目(18BFX211)

(一)美国法上的隐私权及其学理构造

1.美国法上的隐私权。美国司法认定的隐私权包括普通法隐私权和宪法隐私权。(1)普通法隐私权。早期美国法律对隐私的关注主要集中在保护个人免受政府的侵犯,虽然普通法长期以来一直对窃听和非法侵入进行司法限制,但是这些限制基本上没有涉及个人隐私权。随着时间的推移,技术和社会环境的变化导致了法律的转变。针对媒体泛滥和科技进步对隐私的挑战,美国学者沃伦和布兰代斯提出,应该保护个人"不受干扰的权利",在获取和传播有关个人信息方面,隐私的价值不在于有权从未经授权的披露中获利,而在于通过阻止披露该类信息,获得内心的平静和宽慰。① 在沃伦和布兰代斯提出隐私权概念后,美国大多数州逐渐开始承认所谓的"隐私侵权"。各州对隐私侵权实施司法救济的目的就是要使个人能够过上具有合理程度的隐蔽和私人的生活。② 美国学者普罗塞将各州隐私侵权总结为 4 种类型:对原告之独居、独处,或私人事务的入侵;向公众揭露使原告难堪的私人事实;将原告置于不正确的公众理解之下;被告为了自己的利益,在未获得原告同意的情况下使用其姓名或其他类似事物。③ 此后,普通法的隐私权体系基本固定。(2)宪法隐私权。在美国联邦宪法没有明确提到隐私权。在司法实践中,美国联邦最高法院承认的宪法性隐私区域较为有限,主要涉及涵盖面相对狭窄的《美国联邦宪法第四修正案》(以下简称《第四修正案》)中的隐私权、《美国联邦宪法第一修正案》(以下简称《第一修正案》)中的隐私权,以及涵盖面相对宽泛的决定隐私权和信息隐私权等。《第四修正案》中的隐私权指当政府的搜查和扣押行为侵犯了被社会认为合理的个人独处领域时,个人有不受干扰的权利。在司法实践中,美国法院主要通过是否存在对隐私的合理期望来限制《第四修正案》的适用范围。④《第一修正案》中的隐私权指当一个人的言论自由威胁到另一个人的思想自由和休息自由时,后者有不受干扰的权利。该类隐私权与《第一修正案》存在复杂的关系:当涉及自由表达权时,隐私权主张往往会得到支持;⑤当涉及出版自由权时,隐私权主张往往不会得到支持。⑥ 决定隐私权指在就事关个人根本事项,本人有权独立作出重要决定。这一隐私权通常与《美国联邦宪法第十四修正案》(以下简称《第十四修正案》)中的"自由"一词存在联系。相关司法案例的意义在于,它们成功地将隐私观念与《第十四修正案》下的"自由"案件融合在一起,创造出一种全新形式的关于"选择自由"的隐私。⑦ 信息隐私权指个人有权避免披露其个人事项。在"惠伦诉罗伊案"⑧中,纽约州的一项法律要求建立统一的州计算机文档,记录所有获得合法和非法市场上某些药物的人的姓名和地址。该案上诉人认为隐私权包括两个方面的利益,一个是避免披露个人

① See Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review 197－200 (1890).

② See Restatement (Second) of Torts § 652A (Am. Law Inst. 2018).

③ See William L. Prosser, Privacy, 48 California Law Review, 389 (1960).

④ See Olmstead v. United States, 277 U.S. 438, 478－79 (1928) (Brandeis, J., dissenting); Katz v. United, 389 U.S. 347 (1967).

⑤ See Breard v. City of Alexandria, 341 U.S. 622 (1951); Rowan v. United States Post Office, 397 U.S. 728 (1970).

⑥ See Curtiss Publishing Co. v. Butts, 388 U.S. 130 (1967); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974); McNamara v. Freedom Newspapers, Inc., 802 S.W.2d 901 (Tex. Ct. App. 1991).

⑦ See Griswold v. Connecticut 381 U.S. 479, 485－86 (1965); Roe v. Wade 410 U.S. 113, 153 (1973).

⑧ See Whalen v. Roe, 429 U.S. 589, 599－600, 605－606 (1977).

事务的个人利益,另一个是独立作出某些重要决定的利益。美国联邦最高法院最终认可了纽约州法律的合法性,该案的意义在于将信息隐私权界定为个人有权避免披露其个人事项,并被其后的案件所沿用。① 上述司法实践揭示出,每一类型隐私权的提出和接受与美国生活和技术的转变息息相关,这些转变创造出一种社会氛围,不断催生出新的受法律保护的权利。19 世纪后期,随着美国工业化和城市化的发展,人口密度增加,借助新的技术手段,人们有新的机会去窥探彼此的生活。在此种情况下,引入隐私侵权概念恰逢其时。20 世纪中期,政府收集和监视公民信息的行动日益频繁,威胁到美国个人主义理念。在此种情况下,利用《第四修正案》保护公民隐私变得日益重要。第二次世界大战之后,为了保护个人免受他人言论自由的侵扰,《第一修正案》中的隐私权得到承认。20 世纪 60 年代和 70 年代,"自由"的本质被理解为"选择",而"选择"则包括个人有权就事关个人尊严和自治的事项作出最为私密的个人决定。因此,《第十四修正案》中的隐私权获得广泛认可。②

2.美国隐私概念的学理构造。美国关于个人信息保护的司法、立法实践是围绕隐私概念而展开的。虽然就隐私本身而言,一直缺少一个有效、独特和连贯的概念,但是自隐私权概念提出以来,美国司法部门就通过不断扩张隐私权的方式来应对新技术对个人信息的挑战,美国学界也适时细化信息隐私的概念,并获得广泛赞同。面对隐私概念模糊不清的问题,学者们采取 3 种策略加以解决。还原论者认为,隐私并不构成一个独特的概念,人们完全可以通过其他概念和权利来界定隐私;集群理论者则承认,隐私不再是单一概念,而是一簇概念的集合;实用主义者认为,隐私概念的多义性决定了,应以个人事务免受某些特定行为干扰为核心构建一个可具操作性的隐私概念,并为识别、分析和赋予相关实践以某类价值提供指导。③ 美国学者索洛夫将当前社会公认的侵害隐私行为区分为以下 4 类:信息收集、信息处理、信息传播和侵入。④ 通过上述分类,信息时代个人所面临的卡夫卡式隐私困境——既然无须隐藏,为何还要关心隐私——得以彰显:隐私不仅仅是一种将个人从社会控制中解脱出来的状态,它本身就是一种社会控制形式,可以缓和或强化信息结构不平等带来的危害。索洛夫的隐私四分法得到了学界、媒体和法院的广泛关注和认同,但该方法仍无法遏制隐私概念在信息时代的继续扩张。为使隐私概念回归本义,在批判索洛夫观点的基础上,美国学者贝林提出了纯粹隐私理论,即隐私权指防止将自己信息披露给他人的能力;隐私指别人心中缺乏关于自己信息的状态。这一定义有以下 4 个特点:(1)区分自由与隐私,控制隐私权的适用范围;(2)区分隐私权与隐私,避免关于隐私的诸多争议;(3)扩大个人信息的范围,包括但不限于"敏感"或"私密"信息;(4)丰富披露的层次,以能否通过相关信息识别个人为限度。⑤ 在政策辩论中,如果相关术语模糊,那么很难取得预期效果。而理清这团乱麻的最好办法是限缩"隐私"的范围,仅关注隐私的"核心"或"本质"领域。从此种意义上讲,贝林的

① See NASA v. Nelson, 562 U.S. 134 (2011).

② See Ken Gormley, One Hundred Years of Privacy, 1992 Wisconsin Law Review, 1435 (1992).

③ See Ignacio N. Cofone & Adriana Z. Robertson, Privacy Harms, 69 Hastings Law Jounal 1044 (2018); Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stanford Law Review 1193, 1202－603 (1998); Daniel J. Solove, Conceptualizing Privacy, 90 California Law Review 1128 (2002).

④ See Daniel J. Solove, A Taxonomy of Privacy, 154 University of Pennsylvania Law Review 477, 489－491 (2006).

⑤ See Jeffrey Bellin, Pure Privacy, 116 Northwest University Law Review 505 (2021).

纯粹隐私理论有其积极价值。但是，在数字时代，美国法律实践中的隐私不再只是个人不受干扰，而是涉及个人数据处理行为中的透明、控制和安全，即“知道哪些数据正在被收集、这些数据发生了什么、如何选择收集和使用的方式，并确信这些数据是安全的”。[①] 显然，这一数据保护主题已超出隐私权传统司法实践和纯粹隐私理论所能涵盖的范围。因此，纯粹隐私理论的正本清源之举实有时代错置之憾。

（二）美国数据保护立法的体制特色

为保护个人信息处理中的个人隐私，早在计算机开始普及的 20 世纪 70 年代，美国健康、教育和福利部就将隐私标准与正当程序、消费者权利以及平等保护相结合，形成了一套相对完整的“公平信息实践”框架，以规范个人信息处理行为，并自此主导着美国的信息隐私保护实践。在美国法律体系中，作为一个立法概念，数据隐私通常与数据安全一起被纳入数据保护的立法框架之中。前者涉及个人信息的收集、使用和传播，后者涉及未经授权访问和使用个人信息。[②] 由于就数据保护方法、联邦优先范围、《第一修正案》适用限制、个人诉讼权利等重要问题迟迟不能达成共识，因此美国国会难以在联邦层面推出一部综合性的数据保护法案。受此影响，美国的数据保护法体制带有明显的“拼凑”特色，其构成既有联邦成文法、州一级立法，也包括行业自律准则。（1）联邦成文法。自 20 世纪 70 年代以来，美国国会主要利用部门法规制公共机构或私营部门收集和利用个人信息的行为，所涉领域包括消费者信用报告、电子通信、联邦机构记录、教育记录、银行记录、有线电视用户信息、视频租赁记录、机动车记录、健康信息、电信用户信息、儿童在线信息以及客户财务信息等。在上述立法不及领域，自 20 世纪 90 年代末以来，主要由美国联邦贸易委员会依据《联邦贸易委员会法》第 5（a）条——禁止不公平和欺诈行为或做法——所授予的权力来迫使公司执行其隐私政策。[③] 然而，与许多特定行业的数据保护立法相比，《联邦贸易委员会法》并不要求公司遵守特定的数据保护政策或实践。这意味着，如果某一实体未就数据隐私作出承诺，那么联邦贸易委员会将难以适用第 5（a）条。（2）州立法。美国大部分州均通过州一级立法，要求企业在数据安全遭到破坏的情况下作出回应，或要求企业承担责任。此外，许多州的消费者保护法明确禁止不公平或欺诈行为，这些条款也被越来越多地用于解决数据隐私问题。2018 年 6 月，加利福尼亚州立法机构通过一部综合性的《加利福尼亚州消费者隐私法》，创设了美国史上最为严格也最为全面的数据隐私保护制度。加利福尼亚州经济体量巨大，且众多互联网巨头和大型数字平台公司云集于此，《加利福尼亚州消费者隐私法》的影响力远超一州领域，形成了“加州效应”，直接推动了美国数据隐私法的升级。[④] （3）行业自律准则。数字隐私行业自律

① Testimony of Mr. Erich Anderson, Deputy General Counsel of Microsoft Corporation, The State of Online Consumer Privacy, Hearing Before S. Comm. on Commerce, Science, and Transportation, 112 th Cong., 2011, http://commerce.senate.gov/public/? a=Files.Serve&File_id= f8eb430d-c017-4ca1-b7e7-c2f7ec240c67, 2022-07-06.

② See Stephen P. Mulligan & Chris D. Linebaugh, Data Protection and Privacy Law: An Introduction, Congressional Research Service, IF11207, May 9, 2019, https://crsreports.congress.gov/product/pdf/IF/IF11207, 2022-07-06.

③ See Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia Law Review, 611-17 (2014).

④ See Anupam Chander, Margot E. Kaminski & William McGeveran, Catalyzing Privacy Law, 105 Minnesota Law Review, 1737 (2021).

准则的兴起与 20 世纪末美国政府提倡行业自我监管的政策息息相关。相对于政府管制,行业自我监管具有提高效率、增加灵活性、增加合规激励以及降低成本等比较优势。在自我监管的理念下,消费者信息保护通过"告知和选择"程序加以落实。即企业通常将信息隐私政策纳入服务条款合同供用户选择,除非法律明确禁止或限制,企业可以自由收集、处理和分享他们从客户那里获得的信息。然而,研究成果表明,在没有足够消费者参与的情况下,相关个人信息保护实践难言"公平",行业自我监管往往是逃避政府管制的手段而已。①

我们不难发现,虽然美国数据隐私部门立法主要围绕"公共信息实践"而展开,但是仍被放置在信息隐私权的框架下加以理解和适用,从而形成了自成一体的数据隐私一元规制模式。

二、欧盟数据隐私二元规制模式

在欧盟法的体系下,隐私和个人数据保护分别对应着私人生活受尊重的权利和个人数据受保护的权利,是典型的数据隐私二元规制模式。

(一)欧盟法隐私和数据保护基本权利的起源

1950 年《欧洲保障人权和基本自由公约》(以下简称《欧洲人权公约》)第 8 条(私人和家庭生活受到尊重的权利)就对隐私权作出了规定。1981 年欧洲委员会《关于个人数据自动化处理的个人保护公约》(以下简称《108 号公约》)序言从基本权利自身价值和工具价值的维度阐述了个人数据保护的必要性。《108 号公约》第 1 条将保护个人数据与尊重隐私权相提并论,第 2 条将个人数据界定为"与一个已识别或可识别的自然人(数据主体)有关的任何信息"。由此,《108 号公约》首次在条约层面确立了一个有别于隐私权但又与之密切关联的个人数据保护的权利。相对于隐私保护,个人数据保护的范围更广(不仅涉及其他基本权利和自由,还涵盖与隐私无关的各种数据)。同时,数据保护的范围更窄,它仅指向个人信息的处理行为,隐私保护的其他方面则被忽视。严格说来,个人数据保护并不是《欧洲人权公约》各项权利和自由中的一项自主权利。但是,自 1997 年起,欧洲人权法院就认定,个人数据保护对一个人享受《欧洲人权公约》第 8 条所保障的尊重私人和家庭生活权利具有根本重要性。对集中收集、处理和传播数据的行为,当事人可依据第 8 条赋予的信息自主权而享有隐私权。如果某一机构以超出通常可预见的方式或程度汇编某一特定个人的数据、处理或使用个人数据或出版有关材料,那么会引发相关个人对私人生活方面的权利关切,在此种情况下,国内法必须提供适当的保障,以防止对任何此类个人数据的使用违反第 8 条的规定。② 尽管如此,欧洲人权法院并没有在判决中无条件承认所有个人数据处理行为均受《欧洲人权公约》第 8 条的管辖。此外,对水平关系中的个人数据保护问题,欧洲人权法院也没有给缔约方施加积极保护义务。因此,《108 号公约》的规定只是欧洲人权法院作出相关判决时参考的补充标准而已。

(二)欧盟数据隐私二元规制模式的形成与发展

---

① See Siona Listokin, Does Industry Self-regulation of Consumer Data Privacy Work?, 15 IEEE Security. & Privacy, 94 (2017).

② See Z v. Finland, GC, 1997, § 95; Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, GC, 2017, §§ 133-134, 137.

1995 年,在《欧洲人权公约》第 8 条和《108 号公约》的基础上,欧盟通过了欧洲议会和理事会《第 95/46/EC 号指令》(以下简称 1995 年《指令》)。1995 年《指令》与《108 号公约》之间的关系较为简单。前者借鉴了后者的诸多规定,更具针对性和可操作性。而 1995 年《指令》与《欧洲人权公约》第 8 条的关系则较为微妙。欧洲法院指出,为了适用 1995 年《指令》,欧州法院应首先确定相关涉及个人数据处理的国内立法是否侵犯了个人的基本权利和自由,特别是隐私权。如果是,那么欧洲法院应参照《欧洲人权公约》第 8 条项下的基本权利解释相关条文。① 在判决书中,欧州法院将这一分析方法的合法性建立在两个基础之上:(1)根据既有案例,上述基本权利属于欧洲法院应当遵守的一般法律原则的组成部分;②(2)根据《欧洲联盟条约》第 6(2)条之规定,欧盟应尊重《欧洲人权公约》所保障的基本权利。与欧洲人权法院关于《108 号公约》法律地位的判决不同,在欧盟法项下,《欧洲人权公约》第 8 条的相关规定已经成为解释 1995 年《指令》相关条款的重要法源之一。

事实上,《108 号公约》的影响力不限于此。2000 年《欧盟基本权利宪章》(以下简称《宪章》)将“个人数据保护”(第 8 条)与“尊重私人和家庭生活”(第 7 条)并列,共同归属于“自由”名目(第 2 章)之下。通过《宪章》第 7 条和第 8 条,欧盟法确立了数据隐私二元规制模式。无论是在含义、范围还是行使方式上,《宪章》第 8 条项下的权利均与《宪章》第 7 条项下的权利有别。具体而言,《108 号公约》试图建立的并不是一项不容侵犯的个人数据权利,而是一种“制约平衡”机制。1995 年《指令》以《108 号公约》的规定为起点,强化了该“制约平衡”机制。在制定《宪章》时,起草者曾考虑将信息自决的权利纳入第 8 条,但最终仍代之以个人数据保护的权利,因此《宪章》第 8 条基本延续了 1995 年《指令》的风格。③ 例如,《宪章》在第 8(1)条明确“人人有权保护有关他或她的个人数据”后,又在第 8(2)条规定,“这些数据必须为特定的目的,并在有关人员同意或法律规定的其他合法基础上公平地加以处理。每个人都有权查阅收集到的有关他或她的数据,并有权要求改正”,紧接着在第 8(3)条规定,“对这些规则的遵守应受独立机关的控制”。从“制约平衡”的角度看,第 8(2)条、第 8(3)条属于行使第 8(1)条项下权利应满足的要件。与之不同,真正构成《宪章》第 8(1)条例外的是《宪章》第 52 条。《宪章》第 52(1)条规定:“对本宪章所承认权利和自由之行使的任何限制,必须由法律规定,并尊重这些权利和自由的实质。根据相称性原则,只有在必要和真正符合本联盟承认的普遍利益目标或保护他人权利和自由的需要时,才可作出限制。”

2018 年 5 月,替代 1995 年《指令》的《欧盟一般数据保护条例》(以下简称《条例》)正式实施。《条例》更为关注数据保护而非隐私。从形式上看,《条例》的正文通篇未提及“隐私”一词,这与 1995 年《指令》形成鲜明的对比。从理念上看,《条例》的规定直接承接《宪章》第 8 条和《欧盟运行条约》第 16 条,引入数据保护的权利是为了向个人提供结构性的法律保护,使其个人信息免受不适当处理,而不管这种处理是否落入《宪章》第 7 条关于尊重私人生活权利的范围。随着《条

① See Joined Cases C－465/00, C－138/01 and C－139/01, Österreichischer Rundfunk, [2003] ECR I－04989.

② See Case C－274/99 P Connolly v. Commission [2001]ECR I－1611.

③ See Explanations Relating to the Charter of Fundamental Rights of the European Union, Document CONVENT 49 of 11.10.2000, Explanation on Article 8.

例》的实施,《条例》关于数据保护独立于隐私的二元规制模式也将渗透到欧盟各成员国法律体系之内,而这最终会加深欧盟模式与美国模式的隔阂。

(三)欧盟数据隐私二元规制模式的司法实践

随着 2009 年《里斯本条约》的生效,《宪章》所列的个人数据受保护的权利取得了欧盟基本权利的法律地位,欧盟成员的相关法律规定必须达到《宪章》规定的保护水准。因此,在审理涉及个人数据保护的案件时,欧洲法院应首先考虑《宪章》第 8 条的有关规定。同时,由于《宪章》第 7 条与个人数据保护存在千丝万缕的关系,因此欧洲法院还要处理好《宪章》第 7 条与第 8 条之间的复杂关系。现有判决表明,除非存在明确指向,法院并不试图明确区分两个条款之间的功能,而是倾向于一并适用。从判决结果和分析过程看,欧洲法院一并适用《宪章》第 7 条和第 8 条虽然没有引起大的法律争议,但是该法律适用方法极有可能忽视两者之间的本质区别,并妨碍第 8 条功能的发挥。① 例如,在"迈克尔·施瓦辛格诉波鸿市案"②中,德国人迈克尔·施瓦辛格拒绝德国政府相关机构采集其指纹并储存在护照上,并认为该规定侵犯了其在《宪章》第 7 条和第 8 条项下的权利。欧洲法院将之区分为两个层面的问题加以分析:(1)涉案措施"是否存在相关威胁"? 通过"并读"《宪章》第 7 条和第 8 条,欧洲法院认定,政府相关机构采集和储存指纹,构成对尊重私人生活和保护个人数据权利的双重威胁。(2)该类措施是否有"正当性"? 就此,欧洲法院先考察了《宪章》第 8(2)条。对该条项下的当事人"同意"问题,欧洲法院认定,因人们不能自由反对处理其指纹,故申请护照的人不能被视为同意处理指纹。而后,法院转而详细分析本案所涉立法是否符合《宪章》第 52(1)条,并得出肯定的答案。从法律分析方法的角度看,欧洲法院"并读"《宪章》第 7 条和第 8 条并将第 8(2)条与第 52(1)条共同放置在"正当性"下分析均有值得商榷之余地。正是由于没有将《宪章》第 7 条和第 8 条项下的权利作出区分,因此欧洲法院才会就相关措施"是否存在相关威胁"得出一个涵盖过宽的"一般规则"。而欧洲法院将《宪章》第 8(2)条置于"正当性"层面加以讨论更是误读了该条的功能:《宪章》第 8(2)条的功能是为数据处理行为定制立规,以促进第 8(1)条项下权利的实现;而第 52(1)条的功能是为限制第 8(1)条项下权利提供正当性依据。两者不在同一个逻辑层面。上述案件说明,欧洲法院仍在纠结于《宪章》第 8 条的适当定位。虽然在大多数情况下,最终审判结果不会因此而改变,但是这一架空第 8(2)条的思路必然会影响到《宪章》第 8 条权利的独立性和可扩展性。

三、中国数据隐私分离规制模式

(一)数据隐私规制法律框架的确立

中国个人信息保护制度最初也是依托于隐私概念得以存在和发展的。1982 年《中华人民共和国宪法》(以下简称《宪法》)第 38~40 条分别规定了公民人格尊严不受侵犯、住宅不受侵犯以及通信自由和通信秘密受法律保护等,隐含了公民隐私不受侵犯或受法律保护。但因《宪法》之

① See H. Kranenborg, Commentary on Article 8, in S. Peers et al. (ed.), The EU Charter of Fundamental Rights: A Commentary, Hart Publishing, 2014, pp.229-262.

② See Case C-291/12, Michael Schwarz v. Stadt Bochum, [2013].

规定不能作为裁判之依据，[①]故就大大降低了此类规定的实际意义。1986年《中华人民共和国民法通则》规定了若干具体人格权，没有直接提及隐私权。2002年《中华人民共和国民法典草案》(第一稿)第4编(人格权法)第25条规定："隐私的范围包括私人信息、私人活动和私人空间"，引发诸多理论争议。[②] 2009年《中华人民共和国侵权责任法》第2条从救济法的维度将之列为受侵权法保护的民事权益之一。2016年《中华人民共和国网络安全法》(以下简称《网络安全法》)第12条提及，任何个人和组织不得利用网络从事侵害他人名誉、隐私、知识产权和其他合法权益等的活动，但未明确隐私的权利属性。直至2017年《中华人民共和国民法总则》(以下简称《民法总则》)第110条才将隐私权列为自然人享有的具体人格权之一。2020年《中华人民共和国民法典》(以下简称《民法典》)第110条、第990条、第994条、第1032～1034条、第1126条明确提及隐私权或隐私，私法意义上的隐私权由此完整确立。

在隐私权逐步被认可、确立和澄清的过程中，个人信息保护的法律框架也逐渐成形。2020年《民法典》通过之前，与个人信息保护相关的法律规定大致针对3类事项：(1)互联网信息保护。2012年《全国人民代表大会常务委员会关于加强网络信息保护的决定》(以下简称2012年《网络信息保护决定》)明确了网络服务提供者、公民个人和主管部门的义务、权利和职责。2013年工业和信息化部《电信和互联网用户个人信息保护规定》细化了上述决定的内容。2016年《网络安全法》第四章则从法律层面和网络信息安全的维度认可了上述规定，从而将个人信息保护规定上升到法律层面。(2)消费者信息保护。2013年修订的《中华人民共和国消费者权益保护法》第29条、2014年国家工商行政管理总局《网络交易管理办法》第18条分别针对经营者和网络服务提供者收集、使用消费者个人信息，作出相应的规定。其具体要求与2012年《网络信息保护决定》相关规定保持一致。2018年《中华人民共和国电子商务法》第23条规定："电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。"(3)特定信息保护。特定信息大致分为两类：一类是特定人群的信息，如人才信息、金融信息、患者信息、儿童信息等；[③]另一类是不特定人群信息，如居民身份信息、人口普查信息、社会保险信息、统计资料等。[④] 法律就第一类个人信息保护施加特别规定，与个人在特定关系中处于弱势地位有关系。而第二类个人信息保护的必要性主要建立在相关信息具有普遍社会影响力和公信力的基础之上。2021年8月，中国个人信息保护领域第一部专门性、综合性、基础性法律——《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)——出台，中国数据隐私规制法律框架基本确立。

(二)数据隐私规制的中国特色

① 参见《最高人民法院关于裁判文书引用法律、法规等规范性法律文件的规定》(法释〔2009〕14号)。

② 参见王利明：《隐私权概念的再界定》，《法学家》2012年第1期。

③ 例如，1995年《中华人民共和国商业银行法》(2003年修正、2015年修正)第29条，2002年《深圳经济特区人才市场条例》(2019年修正)第9条、第10条，2009年《中华人民共和国侵权责任法》第62条，2019年《儿童个人信息网络保护规定》第7条。

④ 例如，2003年《中华人民共和国居民身份证法》(2011年修订)第19条，1989年国务院《第四次全国人口普查办法》第13条、2000年国务院《第五次全国人口普查办法》第24条、2010年国务院《全国人口普查条例》第4条，2010年《中华人民共和国社会保险法》(2018年修正)第81条，1983年《中华人民共和国统计法》第14条、1996年修正的《中华人民共和国统计法》第15条、2009年修订的《中华人民共和国统计法》第29条。

在《个人信息保护法》中,隐私权并未能取得基本权利的地位,而是成为一种具有特殊地位的公法权利。在这一公法权利体系下,就其实质要素而言,个人信息保护与隐私保护存在较为明显的区别;就其形式要素而言,个人信息与个人数据之间的关系仍有待澄清。

首先,对于个人信息受保护的权利属性存在较大的理论争议。其大致可分为两个层面 4 个组别:即私法层面的"民事权利说"和"行为规制说"与公法层面的"公法权利说"和"宪法权利说"。(1)私法层面的"民事权利说"和"行为规制说"均主张个人信息保护的私法属性,均承认民法是保护人之主体地位的重要手段和基础规范,能够为个人信息保护提供体系支持。而两者的区别在于,持"民事权利说"者认为,自然人对个人信息有控制和支配的权利,其他人均负有一般性的不作为义务,相比于其他部门法,民法权利保护模式更适合中国的立法及司法现实。个人信息权可以嵌入既有人格权规范体系中,实现法律体系的内在和谐。① 持"行为规制说"者认为,个人信息利益尚未达到权利的分配密度,因而不宜采用权利化模式,而应采用行为规制模式对个人信息主体提供一定程度的保护。民法行为规制模式可以在法益保护与行为自由之间确定一个妥当的平衡点,既可确保法益免受特定行为之侵害,亦可为行为人提供明确的行为指引,避免过度钳制其行为自由空间。② (2)公法层面的"公法权利说"和"宪法权利说"并不否认民法体系在保护个人信息权益方面所发挥的作用,其所要强调的是,只有将个人信息保护放置在公法体系下,才能全面规范不对称权力结构下的个人信息处理关系。持"公法权利说"者认为,个人信息保护法实际是个人信息处理规制法,其主要功能在于赋予信息主体新型公法权利,以对抗信息控制者的信息处理行为。③ 持"宪法权利说"者则指出,个人信息保护法体系建构的规范基础是国家在宪法上所负有的保护义务,应以"个人信息受保护权－国家保护义务"框架建构个人信息的权力保护模式。④ 从表面看,"宪法权利说"有助于将中国个人信息受保护的权利拔高到类似于欧盟基本权利的层面,但在司法实践中,宪法权利实效性欠缺是一个不争的事实。"民事权利说"和"行为规制说"的优点在于可利用成熟的侵权责任体制为信息主体提供私法救济,但此类强化个人信息赋权并给予事后司法救济的模式未必符合个人信息保护的基本原理,也很难实现保护个人数据利益的政策目标。因此,在个人信息受保护的权利属性争议中,主张社会控制而非个人控制的"公法权利说"逐渐获得认同。⑤

其次,对于隐私与个人信息保护之间的关系相关法律有着较为明确的区分。例如,2016 年《网络安全法》第 45 条将隐私和个人数据并列;2017 年《民法总则》第 110 条规定自然人享有隐私权,第 111 条规定自然人的个人信息受法律保护;2020 年《民法典》第 110 条和第 111 条延续这种二元保护模式并在人格权编第 6 章对之作出更为具体的规定,第 1034 条规定了个人信息与隐私之间的关系,即"个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定"。对于如何处理个人信息,《民法典》第 1035～1039 条就自然人权利和信息处理者的义务作出了较为详细的规定,从内容看,这与《网络安全法》第 4 章(网络信息安全)的规定

① 参见杨立新:《个人信息:法益抑或民事权利》,《法学论坛》2018 年第 1 期。

② 参见叶金强:《〈民法总则〉"民事权利章"的得与失》,《中外法学》2017 年第 3 期。

③ 参见周汉华:《个人信息保护的法律定位》,《法商研究》2020 年第 3 期。

④ 参见王锡锌:《个人信息国家保护义务及展开》,《中国法学》2021 年第 1 期。

⑤ 参见高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

有相似之处，但在义务主体方面存在差别。2021年《个人信息保护法》则专注于个人信息保护，通篇未提及隐私问题。

最后，对于个人信息与个人数据之间的关系相关法律规定有所提及，但具体含义仍须澄清。美国信息隐私法倾向于将这一关系放置在网络环境下加以讨论，由此“网上个人信息的隐私保护”自然被界定为“数据隐私”，并与“数据安全”共同构成“数据保护”概念的一部分。欧盟1995年《指令》和《条例》均强调，指令或条例“适用于全部或部分以自动化方法处理个人数据，以及适用于以非自动化方法处理构成存档系统一部分或拟构成存档系统一部分的个人数据”。由此，通过对处理方式的限定，个人信息被限缩在特定情景之下。与欧美不同，中国关于个人信息保护的若干重要立法，未能就如何协调个人信息与个人数据的关系作出系统性安排。例如，2016年《网络安全法》关于个人信息保护的规定被放置于网络信息安全的语境下，个人信息尚可与个人数据保持对应关系。然而，2020年《民法典》在将《网络安全法》有关个人信息保护的内容基本复制到人格权编时，仅试图通过限定义务主体的方式来调整个人信息的保护范围，并未限制其具体适用场景，由此导致个人信息保护涵盖面过宽。① 2021年《中华人民共和国数据安全法》（以下简称《数据安全法》）和《个人信息保护法》分别对数据和个人信息加以界定，前者将数据界定为“任何以电子或者其他方式对信息的记录”，后者将个人信息界定为“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，不包括匿名化处理后的信息”。两相结合，个人信息与个人数据又恢复到一一对应关系。但是，这两个定义同样缺乏场景限制。由于未能将信息或数据限定在网络空间或自动处理的情景之下，因此《个人信息保护法》同样面临涵盖面过宽的问题，并引发诸多法律适用难题。鉴此，越来越多的学者建议在法律概念上严格区分信息与数据，通过限定个人信息的形式要素——信息的可获取性——来限定个人信息保护法律的适用范围。②

中国经由《民法典》和《个人信息保护法》构建的数据隐私法律框架有其自身的特色。虽然《个人信息保护法》第1条明确提及“依据宪法，制定本法”，但是只能说明该法具有作为个人信息基本法律的宪法地位，而不能就此认为个人信息保护的权利是一种宪法权利。③ 2020年《民法典》第110条、第111条和第127条区分了隐私、个人信息和数据，初步确立了分别保护的体制。2021年《数据安全法》和《个人信息保护法》可以说是这一思路的产物。问题是，在界定个人信息和数据的形式要素时，两部法律并未采取通行的“自动化处理＋存档系统”标准，而是沿用了2016年《网络安全法》采取的“记录”标准，由此导致《个人信息保护法》未能将其适用范围限定在特定的信息关系之中，进而引发《网络安全法》《民法典》《数据安全法》《个人信息保护法》间复杂的关系之争。因此，对中国数据隐私分离规制模式仍有进一步澄清的必要。

四、贸易法纳入数据隐私规制的方式

美国、欧盟和中国分别形成的数据隐私一元规制、数据隐私二元规制和数据隐私分离规制模

① 参见蔡一博：《〈民法典〉实施下个人信息的条款理解与司法应对》，《法律适用》2021年第3期。

② 参见朱扬勇、熊赞：《论数据与信息的差别——从计算机的视角》，《数据法学》2021年第1期。

③ 参见林来梵：《民法典编纂的宪法学透析》，《法学研究》2016年第4期。

式虽然均认可“公平信息实践”,但是难以形成深度共识。为在数据规制与数据流动之间达成平衡,国际贸易协定主要通过贸易例外和贸易事项两种方式纳入数据隐私规制事项。不同的纳入方式直接影响到未来数字贸易的发展方向。

(一)作为贸易例外的数据隐私规制

贸易例外模式主要出现在世界贸易组织(以下简称世贸组织)的《服务贸易总协定》之中。在“乌拉圭回合”谈判期间,数字贸易仍处于萌芽时期,各国对是否以及如何纳入与之相关的数据隐私规制问题,持极为谨慎的态度。但在“乌拉圭回合”谈判之前,在经济合作与发展组织(以下简称经合组织)的推动下,国际社会曾一度就如何协调隐私保护与个人数据跨境流动之间的关系达成共识。例如,1980 年经合组织《保护隐私和个人数据跨境流动指南》(以下简称《隐私指南》)确立了收集限制、数据质量、目的特定性、使用限制等“公平信息实践”原则,为各国协调相互间的数据隐私规制冲突提供了国际标准。① 然而,一旦数据隐私规制与贸易规制扯上关系,问题就变得格外复杂。究其原因,这一方面涉及数字产品的贸易定性问题,另一方面与国际贸易法的硬法特征息息相关。因此,当美国政府试图利用国际贸易体制限制数据隐私保护问题时,并未得到其他国家的积极回应。1985 年,经合组织《跨境数据流动宣言》明确提及,在国际贸易中的数据流动问题仍须进一步研究。就此,在经合组织框架下协调数据隐私保护与数据自由流动的努力告一段落。在此背景下,《服务贸易总协定》关于数据隐私保护的处理方式特别值得关注,它基本上代表了主要国家就数据隐私问题进行贸易规制所能取得的最大共识。根据《服务贸易总协定》第 16(c)(ii)条的规定,如果相关法律或法规涉及“保护与个人数据处理和传播有关的个人隐私,以及保护个人记录和账户的机密性”,那么构成与《服务贸易总协定》不相抵触的法律或法规,《服务贸易总协定》的任何规定不得解释为阻止任何成员采取或执行确保此类法律或法规得到遵守所必需的措施,只要该措施的实施不在情形类似的国家之间构成任意或不合理歧视的手段或构成对服务贸易的变相限制。可见,作为一项政策目标,个人数据隐私保护的重要性已获得世贸组织成员的承认。基于数据隐私保护之目的,成员方有权选择某一数据隐私保护制度和标准,而只是要求采取相关数据隐私保护措施应符合相应的关系要件,措施的实施应符合最低贸易限制要求等。显然,这一模式不能确保所有世贸组织成员都采用适当和稳健的数据隐私规制法律。②

(二)作为贸易事项的数据隐私规制

与传统货物和服务贸易不同,以数据跨境流动为核心的数字贸易自一开始就与个人数据隐私保护存在关联。就数据隐私规制而言,美国与其主要贸易伙伴之间存在视角和规制方法上的重大差别,在美国法项下,数据隐私规制的首要目标是防止政府侵害,然后再扩展至消费者隐私保护领域,数据隐私保护与数据跨境自由流动可以并行不悖。而在欧盟法项下,数据隐私所涉的隐私权和个人数据保护的权利为欧盟基本权利,它们约束国家行为,成员国据此承担保护私人利益的首要义务。为解决数据隐私规制冲突,美国和欧盟所采取的贸易谈判策略各有不同。自 2012 年起,美国在一系列区域贸易协定中不断植入数据跨境自由流动规则。例如,2012 年《美国和韩国自由贸易协定》电子商务章节第 15.8 条首次规定“各方应努力避免对跨境电子信息流动设置或维持不必要的障碍”。2014 年美国与亚太地区 11 个国家达成的《跨太平洋伙伴关系协

① 参见敖海静:《数据保护的软法之道》,《法商研究》2021 年第 6 期。

② 参见彭岳:《跨境数据隐私保护的贸易法维度》,《法律适用》2022 年第 6 期。

定》第14.11.2条首次明确“每一缔约方应允许通过电子方式跨境传输信息,包括个人信息,如这一活动用于涵盖的人开展业务”。2018年《美国、墨西哥和加拿大协定》(以下简称《美墨加协定》)还对《跨太平洋伙伴关系协定》的数字贸易规则进行了一系列升级,不仅剔除了“跨境数据自由流动”条款中的“考虑各方监管需求”的规定,而且要求缔约方在制定其个人信息保护的法律框架时,应考虑亚太经合组织《隐私框架》和经合组织《隐私指南》(2013年修订)等国际机构的原则和指南等。① 从原则上讲,欧盟并不反对数据跨境流动,1995年《指令》和2016年《条例》均将促进欧盟内部数据自由流动作为立法宗旨之一,并明确规定,不得以保护与个人数据处理相关的自然人为由,限制或禁止欧盟内部个人数据流动。但是,对将个人数据转移到第三国或国际组织的,数据控制者和处理者必须满足欧盟指令或条例规定的要件,否则禁止个人数据流出欧盟。为维护其基本权利属性,欧盟强调,“欧盟数据保护规则不能成为自由贸易协定谈判的主题”。② 相应地,欧盟很少在国际贸易协定中就数据自由流动作出承诺。例如,2012年《欧盟和韩国自由贸易协定》电子商务章节就缺乏关于数据自由流动的条款;2016年《欧盟和加拿大全面经济贸易协定》电子商务章节则强调,“本章并未规定一方有义务允许通过电子方式进行交付,但根据本协议另一条款规定的该方义务除外”。无论是美式的个人数据跨境自由流动优先方案,还是欧式的个人数据保护权利优先方案,均有其深厚的国内数据隐私规制法律制度作为支撑,并且与美国和欧盟在全球数字经济中的地位相匹配。因此,在短期内美欧之间很难就数字贸易规则,特别是在数据跨境流动中的数据隐私规则达成一致意见。这直接影响到在国际层面达成多边贸易协定的可行性。③ 尽管如此,通过《跨太平洋伙伴关系协定》和《美墨加协定》,美国将个人信息保护问题作为贸易规制事项纳入国际贸易协定,并施加条约限制,已经对欧盟数据保护规则不可谈判的立场造成沉重打击。在此情况下,作为数字经济大国之一,中国的立场和选择很有可能左右数字贸易法的发展方向。

(三)中国数据隐私规制的贸易法维度

1.国内法关于个人数据出境的规定。中国国内法从3个维度对个人数据出境问题作出了规定。这些规定重叠适用,构成限制个人数据跨境流动的严密法网。(1)网络安全维度。2016年《网络安全法》第12条提及“国家……保障网络信息依法有序自由流动”。对关键信息基础设施的运营者,该法第37条规定了数据本地化义务,“因业务需要,确需向境外提供的,应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估;法律、行政法规另有规定的,依照其规定”。2020年《信息安全技术个人信息安全规范》第3.9条规定了安全评估的内容,其涵盖范围超出了个人信息安全的范畴,扩展至个人信息处理的全过程。(2)数据安全维度。2021年《数据安全法》第11条规定:“国家……促进数据跨境安全、自由流动。”该法第31条将重要数据分为两类:关键信息基础设施的运营者在中国境内运营中收集和产生的重要数据的出境安全管理,适用

① 参见周念利、陈寰琦:《基于〈美墨加协定〉分析数字贸易规则“美式模板”的深化及扩展》,《国际贸易问题》2019年第9期。

② European Commission, Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World, Brussels, 10.1.2017 COM(2017) 7 Final.

③ See Susan Aaronson, Why Trade Agreements Are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-border Data Flows, Human Rights, and National Security, 14 World Trade Review 695 (2015).

《网络安全法》的规定;其他数据处理者在中国境内运营中收集和产生的重要数据的出境安全管理办法,由国家网信部门会同国务院有关部门制定。2022 年 7 月,《数据出境安全评估办法》公布,由此我国的数据安全评估制度基本成熟。(3)个人信息保护维度。根据 2021 年《个人信息保护法》第 38 条的规定,“个人信息处理者因业务等需要,确需向境外提供个人信息的”,应当具备以下条件之一:1)通过国家网信部门组织的安全评估;2)经专业机构进行个人信息保护认证;3)与境外接收方订立合同,约定双方的权利和义务;以及 4)法律、行政法规或者国家网信部门规定的其他条件。该法第 40 条则规定了必须进行安全评估的情况,即“关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者……确需向境外提供的,应当通过国家网信部门组织的安全评估”。2022 年《数据出境安全评估办法》第 4 条确立了 4 类需要申报数据安全评估的情形,细化了该条的规定。就整体而言,尽管《数据安全法》和《数据出境安全评估办法》均提及促进数据自由流动,但是基于网络主权之理念,《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》所构建的个人信息出境安全评估制度决定了在中国法项下,数据跨境自由流动是例外而非原则。

2.国际法关于个人数据跨境流动和数据隐私的规定。目前,除世贸组织协定之外,中国已经签署 20 个双边和诸边自由贸易协定,涉及 30 个国家和地区。相关自由贸易协定主要关注货物贸易和服务贸易,即使涉及数字贸易或电子商务,大多提出倡导性要求,甚少施加有拘束力的义务,更没有提及数据跨境自由流动事项。2020 年 11 月,中国主导签署的《全面经济伙伴关系协定》在数据跨境流动方面实现了两点质的突破:一是禁止数据当地化,二是确立数据跨境自由流动原则。与此同时,在每一条规定之下,均设置了例外条款,即上述规定不得阻止一缔约方采取或维持该缔约方认为是实现其合法的公共政策目标或保护其基本安全利益所必要的措施。从形式上看,《美墨加协定》的“原则+例外”结构与《服务贸易总协定》第 16(c)(ii)条的一般例外规定有类似之处。由此,一项限制数据跨境流动或要求数据本地化的措施,无论其是网络安全措施、数据安全措施还是个人信息保护措施,均可被纳入贸易例外的框架下加以理解。然而,这一解读有混淆关于贸易事项和贸易例外之嫌。如果结合《全面经济伙伴关系协定》第 12.8 条的规定,那么可以发现,一国如采取数据隐私规制措施,还须符合《全面经济伙伴关系协定》第 12.8 条项下的特别规定。即每一缔约方:(1)应采取或维持保证电子商务用户个人信息受到保护的法律框架;(2)在制定保护个人信息的法律框架时,应考虑相关国际组织或机构的国际标准、原则、指南和准则;(3)应公布其向电子商务用户提供个人信息保护的相关信息;(4)应鼓励法人通过互联网等方式公布其与个人信息保护相关的政策和程序;以及(5)应在可能的范围内合作,以保护从一缔约方转移来的个人信息。由于《全面经济伙伴关系协定》第 12.8 条本身没有例外规定,因此不管缔约国是否限制数据跨境自由流动,只要其采取数据隐私规制措施,就应符合协定的要求。这意味着,即使中国决定利用《全面经济伙伴关系协定》第 12.14 条和第 12.15 条项下的较为宽松的例外规定,就个人信息出境提出数据本地化要求或禁止数据跨境流动,但作为缔约方仍负有国际法义务,按照《全面经济伙伴关系协定》第 12.8 条的具体要求来建构本国的个人信息保护法律框架。

值得注意的是,在签署《全面经济伙伴关系协定》之后,中国又于 2021 年下半年相继申请加入《全面与进步跨太平洋伙伴关系协定》和《数字经济伙伴关系协定》。与《全面经济伙伴关系协定》不同,《全面与进步跨太平洋伙伴关系协定》和《数字经济伙伴关系协定》关于数字贸易的规定

深受美国方案的影响。就数据跨境自由流动而言,《全面与进步跨太平洋伙伴关系协定》第14.11.3条和《数字经济伙伴关系协定》第4.3条虽然允许存在例外但是条件更为严格,如在判断是否对信息传输施加“超出实现目标所需限度的限制”时,不再由实施的缔约方自我认定,而是采取更为客观的评估方法。就数据隐私规制而言,《全面与进步跨太平洋伙伴关系协定》第14.8.5条和《数字经济伙伴关系协定》第4.2.6条更强调效果等同原则,如在参照国际标准制定个人信息保护的法律方面,缔约方可采取多种方式履行该义务,包括“全面保护隐私、个人信息或个人数据的法律、涵盖隐私的特定部门法律或规定执行由企业作出与隐私相关的自愿承诺的法律”。对不同形式的个人信息保护法律,《全面与进步跨太平洋伙伴关系协定》第14.8条和《数字经济伙伴关系协定》第4.2条要求每一缔约方应鼓励建立促进不同个人信息保护体制之间兼容性的机制,“这些机制可包括对监管结果的承认,无论是自主给予还是通过共同安排,或通过更广泛的国际框架”。

《全面经济伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》的上述规定为中国个人信息保护法律制度的存续和发展设置了较为明晰的国际法限度。就数据隐私规制而言,《网络安全法》《数据安全法》和《个人信息保护法》规定的处理个人信息原则基本符合《全面经济伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》的要求,这就为实施《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》所建议的替代合规打下了良好的基础。就数据跨境流动而言,中国国内法规定与亚太经合组织《隐私框架》和经合组织《隐私指南》的数据自由流动宗旨存在较为明显的冲突。虽然《个人信息保护法》第38条第2款提及,中国缔结或者参加的国际条约、协定对向中国境外提供个人信息的条件等有规定的,可以按照其规定执行,但是此类规定意在授权而非施加义务。因此,如果不能成功寻求例外,那么《网络安全法》《数据安全法》《个人信息保护法》中的限制个人数据出境的规定将承受较大的国际法合法性压力。从此种意义上讲,例外条件更为严格的《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》将会对中国数据规制法律产生更具限制性的影响。

尽管如此,基于《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》自身的特殊性,在短期内,中国申请加入《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》的行为仍不会从根本上动摇中国关于数字贸易的基本立场。根据《数字经济伙伴关系协定》第14.3条和第14－A.1条的规定,其关于数据跨境流动和数据本地化的相关规定不在缔约方之间创设权利和义务,也不能提请争端解决。《全面与进步跨太平洋伙伴关系协定》的两大成员——加拿大和墨西哥——均为《美墨加协定》的缔约国,而《美墨加协定》的“毒丸条款”会从缔约体制层面遏制中国与加拿大、墨西哥缔结自由贸易协定。因此,最有可能对中国个人信息保护法律制度施加国际法限制的《全面与进步跨太平洋伙伴关系协定》反而会因为美国的干涉而难以发挥作用。

可以认为,无论是作为贸易例外事项还是作为贸易规制事项,当前国际贸易法并不会实质性地限制中国数据隐私规制体制的独立性和自主性。但是,《全面经济伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》均指向了国际组织或机构的标准、原则、指南,并将之作为评判缔约方国内个人信息保护法律是否符合条约要求的标准之一。在此种情况下,中国规制主权将受制于国际标准的变动。鉴于美国和欧盟主导着亚太经合组织《隐私框架》和经合组织《隐私指南》,对已经加入《全面经济伙伴关系协定》且正在寻求加入《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》的中国而言,必须密切关注《隐私框架》《隐私指南》提及

的国际软法标准及其发展趋势,[①]并利用现有国际机制,积极参与国际软法塑造过程。

五、代结语:中国数据隐私规制贸易法表达的展望

各国不同的数据隐私规制模式直接影响到个人数据跨境自由流动:在美国数据隐私一元规制模式下,数据跨境流动只有在涉及个人可识别信息且侵害到个人隐私的情况下才会受到限制。在欧盟数据隐私二元规制模式下,符合《条例》规定条件的控制者或处理者方可将个人数据传输到第三国或国家组织。中国数据隐私分离规制模式在概念上严格区分隐私和个人信息保护,对于后者,只有因业务等需要,确需向境外提供个人信息的,才能进行数据跨境流动。对于特定情形,只有通过国家网信部门组织的安全评估方可允许出境。

为平衡数据跨境自由流动与数据隐私规制之间的关系,世贸组织以贸易例外的方式允许成员采用数据隐私措施,只要该措施的实施符合相关要件。《全面经济伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》《美墨加协定》以贸易事项的方式不仅要求缔约方国内建立数据隐私规制法律框架,而且要求相关法律框架应当考虑国际机构和组织的标准、原则、指南和准则。不仅如此,《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》和《美墨加协定》均提及,每一缔约方应鼓励建立促进不同个人信息保护体制之间兼容性的机制。对欧盟而言,贸易例外方式可使欧盟继续域外适用《条例》且不会威胁到个人数据保护权利的基本权利属性。对美国而言,通过贸易事项方式可限制其他缔约方利用严格的个人信息保护规定阻碍数据跨境流动。对中国而言,贸易例外方式有助于维护网络主权和数据主权,发展具有中国特色的个人信息保护法。但是,这一方式很难保证数据跨境自由流动,进而会影响到中国贸易的壮大和数字经济的发展。相反,贸易事项方式可在一定程度上便利数据跨境自由流动,但是中国个人信息保护法的发展将可能被限定在国际机构和组织认定的基准和方向之上。

从理论上讲,如果将个人信息保护权视为一种民事权利或权益,那么可利用侵权法对相关侵害行为实施事后救济,在此种情况下,中国数据隐私规制法律可能走上类似于美国普通法的隐私侵权法道路。反之,如果将个人信息保护权视为一种宪法性权利,那么可借助《个人信息保护法》对个人信息处理行为实施监管,并利用民事、行政和刑事救济手段强化监管效力,在此种情况下,中国数据隐私规制法律可能走上类似于欧盟基本权利的道路。然而,随着《全面经济伙伴关系协定》生效以及寻求加入《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》,中国国内数据隐私法基本被锁定在第三条路径——隐私和个人信息保护严格分离的规制模式——之上。这一模式给中国带来的体制优势是,没有宪法权利或基本权利不可谈判的困扰,中国可将数据隐私保护问题作为贸易规制事项纳入数字贸易谈判,从而限制他国借数据隐私规制之名行数字贸易保护之实。但随之而来的问题是,《网络安全法》《数据安全法》《个人信息保护法》所构建的个人数据出境安全评估制度的具体实施可能会受到贸易协定相关条款的实质性限制。就如何平衡其间的利害关系而言,《个人信息保护法》第 38 条第 2 款将之留给了实践,即若协定对向中国境外提供个人信息的条件等有规定的,则“可以按照其规定执行”。就条约适用的国内法法理而言,这一授权性规定无可厚非,但就“有约必守”的国际法原则而言,当主管机关选择不按其规定执行

① 参见敖海静:《数据保护的国际软法之道》,《法商研究》2022 年第 2 期。

时，有必要在相关贸易协定中寻找例外依据。因此，中国主管机关愈是倾向于不按照协定规定执行，愈有必要关注贸易协定中的条件条款和例外规定。而相关实践也会促进国内法与国际法的良性互动，有助于数据隐私治理体系的发展和成熟。

总而言之，数字时代的数据隐私规制关系到政治层面政治体制的维系、社会文化层面个人行为社会正当性的获得，以及个体层面个人自我发展的实现等重大价值。① 欧盟将个人数据保护的权利抬升到基本权利层面，并通过《条例》的域外适用机制加以推行，虽然有助于实现其政策目标，但是该数据隐私二元规制模式也因此丧失了可复制性。美国利用普通法隐私体制救济私人侵权、利用宪法隐私体制限制政府侵权以及利用部门立法和州立法规制特定个人信息处理行为，并不能有效应对数字时代信息不对称造成的“卡夫卡困境”，如果在全球推广，那么反而会造成更大的数字鸿沟。在《民法典》严格区分隐私与个人信息的基础上，《个人信息保护法》旨在“保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用”，较好地回应了数字经济发展的要求。而《网络安全法》《数据保护法》“维护网络空间主权和国家安全”“维护国家主权、安全和发展利益”等宗旨更是反映了绝大多数发展中国家的心声。在数字贸易国际规则逐渐成形的关键时期，中国政府理应以国内法规定为基础，积极参与数字贸易规则谈判，通过国内法与国际法的良性互动，在现有的基础上细化中国方案，贡献中国智慧。

Abstract: In the era of digital economy, digital trade increasingly relies on cross-border free flow of data. At the same time, in order to protect personal information, countries take measures to regulate the behavior of personal data processing. Based on different privacy concepts, legislative policies and judicial practices, the United States, the European Union and China have formed three types of data privacy regulation: unitary regulation, dual regulation and separation regulation respectively. In order to ease the conflicts between different data privacy regulation modes and facilitate the free flow of data across borders, international trade agreements mainly include data privacy regulation issues through trade exceptions mechanism and trade matters mechanism. Different data privacy regulation modes tend to support different inclusion modes, and different inclusion modes will also affect the space for independent development of different data privacy regulation modes. The Chinese government should take an active part in the negotiations on digital trade rules based on domestic laws and regulations, refine China's proposals on the existing basis and contribute Chinese wisdom through the positive interaction between domestic and international laws.

Key Words: data privacy, regulation mode, data flow, trade exceptions, trade matters

责任编辑　　何　艳

① See Alan F. Westin, Social and Political Dimensions of Privacy, 59 The Journal of Social Issues, 432-434 (2003).