欧盟个人数据权的演进及其启示

张　金　平*

摘要：因数据处理市场长期被美国企业主导，欧共体及欧盟自1970年起实施数据处理方面的统一政策，目的是限制美国企业，重点是协助消费者转向本土企业。欧盟个人数据权经历了4个阶段的演进：欧共体早期明确上述政策并提出以访问权为核心的个人数据权雏形；欧共体后期将个人数据权塑造成限制数据跨境转移的合法依据；欧盟早期通过《95指令》实现个人数据权的体系化并构建起以行政救济为主的救济机制；欧盟近期通过《通用数据保护条例》，不仅为消费者从他国企业转向本土企业提供携带权，而且还赋予个人数据权人权地位和行政监管机制的域外效力。在本土企业主导国内市场的情况下，我国不能照搬欧盟的个人数据权机制来限制本土企业的发展。

关键词：个人数据　　产业发展　　数据跨境　　国家安全　　域外效力

2018年9月公布的十三届全国人大常委会立法规划，将个人信息保护法和数据安全法列为第一类立法项目，由此我国个人信息方面的系统性立法正式进入议程。与此同时，欧盟《通用数据保护条例》以人权高度和天价罚款树立起保护个人数据权利（以下简称个人数据权）的最高标准。不过，面对如此高的标准，日本、印度和巴西等国的个人数据立法或修法仍基本照搬《通用数据保护条例》，连美国加州也把《通用数据保护条例》规定的各项个人数据权尽数引入。① 2016年《中华人民共和国网络安全法》也参照《通用数据保护条例》规定个人有权同意他人是否可以收集其个人信息、有权要求更正和删除其个人信息，并且后续的国家标准《信息安全技术 个人信息安全规范》亦参考《通用数据保护条例》为这些权利的行使提供推荐性指南。因此，我国未来立法不能再像《中华人民共和国民法总则》那样，回避是否设置个人信息权或者个人数据权，以及是否借鉴《通用数据保护条例》等争议。有鉴于此，本文旨在从历史角度系统剖析欧盟创设个人数据权的背景、目的、内部构造、后续权能扩展以及性质升级等演变，②为我国立法提供清晰的参考系，避免盲目移植《通用数据保护条例》的个人数据权规定作茧自缚，继而从比较法方面探讨我国未来个人数据立法的目的和所需的制度设计。

一、欧共体内部萌芽期：确定个人数据权的创设初衷与内部结构

1951年成立的欧洲煤钢共同体（以下简称欧共体），经由1993年《马斯特里赫特条约》发展为欧洲经济货币联盟和欧洲政治联盟（以下简称欧盟）。1960年以来的计算机自动化数据处理技术的发展，③几乎与欧共体的发展同步，但这一产业却由美国主导，深刻影响了欧共体及欧盟的经济、政治和法律政策。本

*　中央财经大学法学院讲师

基金项目：国家社会科学基金重大项目（18ZDA136）

①　《2018加州消费者隐私保护》不仅引入了《通用数据保护条例》的被通知权、访问权、修改权、反对权，而且还引入了携带权和被遗忘权。

②　我国学者对欧盟个人信息权的初步介绍成果比较多。参见蒋舸：《个人信息保护立法模式的选择——以德国经验为视角》，《法律适用》2011年第2期；杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，《比较法研究》2015年第6期；等等。

③　See U.S. Department of Health, Education & Welfare, Records, Computers and the Rights of Citizens, July 1973, No. (OS) 73—94, p.8.

文将欧共体和欧盟在个人数据权保护方面统一政策的历史演进分成4个时期:确定政策目的、形成个人数据权雏形的欧共体内部萌芽期,塑造个人数据保护国际规则的欧共体国际突破期,以指令形式统一立法的欧盟发展期和以条例替代指令的欧盟改革期。其中,从1972年到1980年期间,欧共体认清了当时数据处理产业的国际局势,进而明确了个人数据权的创设初衷、雏形及其内部结构。

1.个人数据权创设初衷:协助欧洲消费者转向本土企业

欧共体委员会1973年调查显示,"欧洲市场上超过90%的计算机都是依靠美国的技术,其中IBM一家公司就独占60%"。[①] 对于数据处理产业的重要性,欧共体委员会不仅将其定性为继医药和汽车产业之后的全球第三大产业,而且指出未来社会的架构很大程度上取决于使用数据处理系统的方式,更直指美国企业独霸该产业的弊端,"允许其决定产品价格、技术标准、未来商业创新的节奏和市场发展的模式。"[②]

为此,欧共体委员会产业与技术部在1973年建议采取统一措施,旨在从美国企业手中夺回欧洲数据处理市场,关键是让欧洲的个人、企业、政府等消费者转向欧共体本土企业,首先要突破的障碍是消费者的价格偏好——消费者更愿意使用IBM等美国企业更先进的产品和服务——因此所提议措施包括进行企业重组、加大产业扶持力度、政府仅采购本土企业的产品和服务,以及"为消费者转向欧共体本土企业提供协助"。[③] 欧共体委员会于是确定了整体战略,"将时刻谨防IBM公司滥用其市场支配地位,但最有效的方法是在本土培育强有力的竞争对手",因而建议欧共体理事会形成两大决议:一是加大产业扶持,二是采取协同的政府采购合同。此外,欧共体委员会还对欧洲公民个人信息的保护政策首次提出,"最重要的是各成员国达成政治上的一致,而不是等到各自立法后再进行冲突协调"。[④]

2.个人数据权的雏形和内部结构:以访问权为核心的三权雏形

欧共体理事会的决策机构部长委员会在1973年和1974年先后对私营部门和公共部门处理个人数据出台两项决议,明确个人数据处理的初步规则。[⑤] 为此,德国、法国、卢森堡、英国、比利时等国纷纷通过或者起草个人数据保护法,但除德国外的其他国家并未区分私营部门与公共部门的个人数据处理规则。[⑥]为协调各成员国立法,欧共体理事会在1977年指定欧共体委员会进行数据安全与保密专项研究。[⑦]

欧共体委员会在1980年汇报了最终研究成果,[⑧]其中第5个子报告《访问权的技术面向》详细阐述了欧共体个人数据权的雏形及其内部结构。在内容上,该报告并未使用"隐私权"概念,而是开门见山地指出个人数据保护法所要保护的两大类个人利益,"一类是防止个人数据的过多披露,所保障的权利可称为'保密权';另一类则相反,旨在让数据主体能够自由访问或者获取他人存储的有关其个人的信息,所保障的权利可称为'知情权'",并强调前者已可以通过当时的技术得到很好保护,但后者并未获得相应的发展。[⑨]

对于知情权的内部构造,欧共体委员会作了非常精妙的总结:"知情权包括四个子权利:(1)公众有权意识到这些文档的存在,即公众有权知道或者有机会知道所有有关自然人信息的文档的存在,不论是由公共部门还是私营部门持有。(2)个人有权被告知其个人信息存在于特定的文档。该权利区别于第一个子权利在于它是个人权利而非公众的权利。同时,该权利也独立于第一个子权利,例如向个人发送通知能够

---

① The Commission of the European Communities (CEC), Communication Concerning a Community Policy for Data Processing, SEC (73)4300 Final, 1973, p.1.

② CEC, Communication Concerning a Community Policy for Data Processing, SEC (73)4300 Final, 1973, p.1.

③ Directorate-general for Industrial and Technological Affairs of CEC, Towards a European Policy on the EDP Industry, III/1005/73-E, 1973, pp.18-19.

④ CEC, Communication Concerning a Community Policy for Data Processing, SEC (73)4300 Final, 1973, pp.1-13.

⑤ See Committee of Ministers of Council of Europe, Resolution (73)22 on the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Private Sector, Sep. 1973; Committee of Ministers of Council of Europe, Resolution (74)29 on the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Public Sector, Sep. 1974.

⑥ See CEC, Final Report Volume 2: Study on Data Security and Confidentiality-Organization and Method of Operation of the Data Protection Authorities, 1980, pp.45-160.

⑦ See Council Decision of 27 September 1977 Adopting a Series of Studies in Support of the Use of Informatics, 77/616/EEC.

⑧ See CEC, Summary Report: Study on Data Security and Confidentiality, 1980, pp.5-7.

⑨ See CEC, Final Report Volume 5: Study on Data Security and Confidentiality-Technical Aspects of the Right of Access, 1980, p.1.

满足第二个子权利的需求,但并不满足第一个子权利的需求。相反,通过'公众可获取清单'的方式可以满足第一个子权利,但无法满足第二个子权利的需求。(3)个人有权知道在特定系统中个人信息的具体内容。很显然,该权利是知情权的核心部分,也促成了本研究的主要内容。该权利预设了第二个子权利的存在,但并未预设第一个子权利的存在。(4)个人有权在知道个人信息存在错误的情况下请求修改该信息。从严格意义上讲,该权利并不是知情权的组成部分,但却是访问权的自然延伸,我们认为缺少该权利本报告就不再完整。我们也应当研究作为该子权利的补充性权利'转告权',即要求修改者将修改后的信息发送给之前已经从修改者处接收过该个人信息的主体。对于这 4 个子权利,我们应当考虑不同的适用方法和不同结果,以及不同的技术要求"。[①]由此可见,知情权分为公众知情权与个人知情权。其中,个人知情权是个人数据权的雏形,其内部构造是以"访问权"为核心的,被通知权为行使访问权的前提,修改权为访问权的自然结果。

3.欧共体及其成员国的立法逻辑:个人数据权并非立法的真正核心

仅从《访问权的技术面向》而言,知情权的第一个子权利"公众知情权"似乎与个人数据保护无关。然而,欧共体委员会在《数据安全与保密总报告》中却强调:"正是公众对于个人数据使用的关心导致了个人数据保护法的诞生,也正当化了个人数据监管部门实质、有效而透明的监管"。[②]换言之,欧共体早期的个人数据立法的核心是为了提供行政监管部门主动执法的正当性和法律依据,从而实现打压美国企业、引导消费者转向本土企业的战略目标,而个人知情权作为私权传统上仍以事后的司法救济为主,无法在理论上为行政监管部门提供事前主动执法的正当性。因此,欧共体委员会不仅指出欧共体及其成员国的数据监管当局必须教育公众使用外国产品和服务的危害、引导其转向本土企业,而且坦承欧共体成员国监管当局至少在早期是以一种事先防御性而不是提供事后救济的方式运作。[③]

二、欧共体国际突破期:确立以个人数据权限制数据跨境转移的合法性

数据处理产业为美国企业主导,且欧洲大量数据被转移到美国,引发欧洲各国的恐慌。例如,曾任法国最高法院总法律顾问的儒瓦内先生在 1977 年指出:"信息是一种权力,而经济信息就代表着经济权力。信息拥有经济价值,而存储和处理特定类型的数据能够赋予一国在政治和技术上的优势。反过来,通过数据跨境转移就可能导致一国国家主权的丧失"。[④]欧共体委员会在 1980 年也承认"国家经济和国家主权与最初的数据保护问题越来越融合在一起"。[⑤]不仅如此,加拿大在 1979 年的克莱因报告中也对美国企业独霸加拿大国内数据处理市场有类似的担心。[⑥] 因此,欧共体这一时期致力于联合其他国家塑造以个人数据保护限制数据跨境转移的国际法依据。

1.《经济合作与发展组织指南》:隐私与个人数据保护成为限制数据跨境的理由之一

欧共体及其成员国、美国、加拿大、日本和澳大利亚等国对于数据跨境转移问题专门在 1978 年组成了隐私保护与个人数据跨境转移专家组。不过,作为全球数据处理市场的主导者,美国对个人数据保护的态度与欧共体成员国、加拿大等国都相去甚远:主张个人数据的保护要考虑数据控制者的利益,个人仅有一定的参与权而非控制权;在国际层面,基于国内的宪法第一修正案(言论自由)和数据处理产业的优势主张

① CEC, Final Report Volume 5: Study on Data Security and Confidentiality—Technical Aspects of the Right of Access, 1980, pp.2—3.

② CEC, Summary Report: Study on Data Security and Confidentiality, 1980, p.49.

③ See CEC, Summary Report: Study on Data Security and Confidentiality, 1980, p.19.

④ Speech at OECD Symposium on Transboder Data Flows and the Protection of Privacy, Venna, 1977, Cited in Vincent Mosco and Janet Wasko, The Political Economy of Information, The University of Wisconsin Press, 1988, p.306.

⑤ CEC, Summary Report: Study on Data Security and Confidentiality, 1980, pp.20—21.

⑥ See Clyne Report, 1979, Cited in William L. Fishman, Introduction to Transborder Data Flows, 16 Stanford Journal of International Law, 9 (1980).

数据跨境自由流动。[①] 因此，经过两年谈判，经济合作与发展组织专家组也无法在个人数据的隐私或隐私权概念上达成一致，只能同时使用“隐私与个人自由”术语来指代所要保护的个人利益。尽管如此，专家组在个人数据处理的基本原则上还是达成初步共识（如第 13 条规定的个人参与原则），并允许成员国以保护隐私和个人自由、公共利益、国家安全和国家主权为由限制数据跨境转移，由此形成无强制力的《关于隐私保护和个人数据跨境转移的经济合作与发展组织指南》（以下简称《经济合作与发展组织指南》）。

2.《108 号公约》：统一成员国以个人数据保护限制数据跨境流动的立场

为弥补《经济合作与发展组织指南》无强制力的缺陷，欧共体理事会在该指南出台不到半年就颁布了《关于个人数据自动处理过程中的个人保护公约》（以下简称《108 号公约》）。[②] 《108 号公约》在内容上与《经济合作与发展组织指南》相比具有很多相同点，同样以个人数据处理基本原则为主要内容，但同时实现了 3 个方面的突破。其一，该公约具有法律约束力，成员国应当采取措施执行。其二，该公约是一个开放性公约，不仅欧共体成员国可以加入，非成员国也可以参加，如毛里求斯、摩洛哥、塞内加尔和俄罗斯都先后加入了该公约。[③] 其三，该公约通过立法技巧将限制数据跨境流动的合法理由进行了扩张，如该公约第三章第 12 条（数据跨境流动与国内法）容易让人误认为成员国仅能按照该条款以个人数据保护为由限制数据跨境流动，实际上该公约第二章第 9 条还赋予了成员国基于国家安全、公共安全、国家金融政策或者打击犯罪等理由对特殊类型数据的跨境流动加以限制的权力。

3.《服务贸易总协定》突破：在世界贸易组织规则中成功加入个人数据与隐私保护例外

第二次世界大战后，美国在计算机、旅游、金融等跨境服务产业方面得到空前的发展，急迫改变国际贸易规则，于是在 1989 年提出《服务贸易总协定》草案，限定成员国仅可以“为保护公共道德、秩序或安全，人类、动植物的生命或健康；为确保本协定执行，包括涉及知识产权保护和防止欺诈或不公平行为；为征收或执行间接税”目的限制跨境服务贸易。[④] 为反制美国，[⑤]欧共体委员会在 1990 年提出了自己的服务贸易总协定草案，在美国草案例外条款的基础上明确增加两个限制跨境服务贸易的新依据：“为保护个人数据和个人隐私”和“为保护消费者”。[⑥] 因原加入《经济合作与发展组织指南》的发达国家，以及希望保留更多限制跨境服务贸易合法理由的发展中国家的支持，[⑦]欧共体上述建议草案在 1994 年最终获得通过（《服务贸易总协定》第 14 条）。由此，欧共体成功将个人数据和隐私保护作为限制服务贸易的合法事由纳入世界贸易组织规则之中，为下一步采取更强势的统一个人数据立法奠定了扎实的国际法基础。[⑧]

三、欧盟发展期：打造体系化的个人数据权与行政执法为主的救济机制

《108 号公约》虽对成员国具有约束力，但真正执行该公约的国家并不多，并且该公约允许成员国自行

① See William L. Fishman, Introduction to Transborder Data Flows, 16 Stanford Journal of International Law, 5 (1980); U.S. Department of Health, Education & Welfare, Records, Computers and the Rights of Citizens, July 1973, No. (OS) 73—94, pp.40—41; The Privacy Protection Study Commission Created by the U.S. Privacy Act of 1974, Personal Privacy in an Information Society, 1977, pp.17—22.

② See Explanatory Report on Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, para. 17.

③ See United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, 2016, p.25.

④ See Group of Negotiations on Services, Communication from the United States: Agreement on Trade in Services, MTN.GNS/W/75, 1989, p.12.

⑤ See Juan A. Marchetti and Petros C. Mavroidis, The Genesis of the GATS, 22 The European Journal of International Law 689, 695 (2011).

⑥ See Group of Negotiations on Services, Proposal by the European Community: Draft General Agreement on Trade in Services, MTN.GNS/W/105, 1990, p.13.

⑦ See Juan A. Marchetti and Petros C. Mavroidis, The Genesis of the GATS, 22 The European Journal of International Law, 697—698 (2011).

⑧ 参见张金平：《跨境数据转移的国际规制及中国法律的应对》，《政治与法律》2016 年第 12 期。

决定执行的方式,因此实施效果也参差不齐。[①] 该公约的上述局限对内构成统一欧共体内部市场的障碍,对外难以统一主张本地区因提供了个人数据高水平保护而可以限制数据向其他低水平国家(尤其是美国)的转移。于是,欧共体委员会在 1990 年就开始起草欧盟层面的统一立法《关于个人数据处理中的个人保护的指令(草案)》(以下简称《90 草案》)。[②] 两年后,欧共体委员会根据欧共体理事会和欧共体议会的意见进行修改,包括将草案标题修改为《关于个人数据处理中的个人保护与这些数据自由流动的指令》(以下简称《92 修订稿》),明确保护个人利益和规制个人数据跨境流动系指令的双重目的。服务贸易总协定通过后不久,《92 修订稿》经微调后即获通过,史称《95 指令》。

1.发展个人数据权:实现权利的体系化和法定化

《90 草案》希望以个人数据权为核心构建个人数据保护规则,因而在第三章专门以"数据主体的权利"为标题将个人数据权法定化。其中,第 14 条以欧共体委员会 1980 年个人数据权雏形为基础构建个人数据权体系:(1)反对权;(2)针对个人画像进行自动决策的反对权;(3)被通知权;(4)访问权;(5)修改、删除或者屏蔽权;(6)针对市场营销或广告目的的数据处理者提出的删除权;(7)转告权;(8)司法救济权,即本条上述权利受侵害时获得司法救济的权利。相对于 1980 年的雏形,《90 草案》解释备忘录指出个人数据权体系增加的反对权源自隐私权,即个人有权反对他人对其个人数据的处理,维持其个人信息的保密性、维系个人生活的安宁,但该反对必须有合法理由,即数据控制者"缺乏处理个人数据的法律正当性";而增加的针对自动决策的反对权,则是为了避免"处于强势地位的公共或私营机构,剥夺个人影响这些机构对使用个人数据或人格画像作出决策的能力"。[③] 针对广告营销增加的删除权,其实更类似于反对权,目的是"保护数据主体不受垃圾广告邮件的骚扰"。对于被通知权、访问权、修改、删除、屏蔽、转告权之间的逻辑关系,《90 草案》则沿袭了 1980 年个人数据权雏形的内部逻辑关系。[④]

不过,数据主体要行使反对权,仍同行使访问权一样,须以被通知权为前提;而司法救济权是通过司法途径保护这些权利的必然要求。因此,《92 修订稿》整合了个人数据权的具体权利并调整了其次序:先规定被通知权,后规定访问权、修改、删除、屏蔽和转告权,继而规定反对权,同时限制转告权的行使,即被证明不可能或者不符合比例的不得行使。至于司法救济权,则统一放在"责任与制裁"一章,并且司法救济的范围不限于《90 草案》第 14 条规定的 7 项权利,还包括本指令其他条款规定或保障的权利(如同意权)。上述修改最终成为《95 指令》正式文本。

2.知情同意:仅是处理个人数据的合法依据之一

《90 草案》希望能突破性地创设以个人数据权为基础的知情同意规则,在第 12 条直接以"知情同意"为标题,并明确数据主体作出同意的生效条件。对此,草案解释备忘录专门强调了知情同意的功能:"为了确保数据主体能够权衡将要发生的有关个人数据处理风险和收益,并能够行使本指令第 14 条赋予的权利(修改、删除、屏蔽),数据控制者必须向数据主体提供与数据主体决策有关的信息,例如数据控制者的名称与地址、数据处理的目的、所存储的数据内容等"。[⑤]

然而,在《90 草案》的讨论阶段,草案第 12 条的知情同意规则造成了误解,一些利益相关方得出这样的结论——所有的个人数据处理都要求事先获得数据主体的同意——但事实上同意只是数据处理的合法依据之一。因此,更符合逻辑的做法是将同意的规则放在第 2 条,稍做修改之后作为同意的概念。尽管如

① See CEC, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) 314 Final—SYN 287, 1990, pp.14—15.

② See European Commission (EC), Report on Europe and the Global Information Society, Office for Official Publications of the European Communities, 1994, pp.4—22.

③ CEC, Amended Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of such Data, COM (92) 422 Final—SYN 287, 1992, p.29.

④ See CEC, Amended Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of such Data, COM (92) 422 Final—SYN 287, 1992, pp.29—31.

⑤ CEC, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) 314 Final—SYN 287, 1990, pp.26—27.

此,在同意作为数据处理的合法依据之一的情况下,《92 修订稿》的草案解释备忘录仍坚持《90 草案》所解释的知情同意的功能。[①] 类似地,《网络安全法》第 41 条第 1 款"网络运营者收集、使用个人信息……并经被收集者同意"的规定,也容易让人误认为知情同意是处理个人数据的唯一合法依据。[②]

3.权利救济体系:以行政救济为主

《90 草案》沿袭传统的私权救济体系,除了在第三章"个人数据权"第 14 条中专门规定司法救济权外,还在第六章"责任与制裁"第一个条款(即第 21 条)中明确了数据控制者的损害赔偿责任。此外,第六章第 23 条规定成员国应当采取刑事处罚等有威慑力的处罚,[③]但并未专门强调要提供行政救济。

然而,这样的救济机制与各成员国已有的以行政救济为主的机制,以及《联合国关于个人数据文档计算机化的规制指南》(以下简称《联合国指南》)都不相符。首先,德国和法国此前的个人数据保护法仅规定侵害个人数据权或者违反该法其他义务的刑事责任和行政责任,并未规定民事责任。例如,德国 1977 年《联邦数据保护法》第 41 条规定了非法收集、传输、修改个人数据的刑事责任,第 42 条规定了数据处理者违反各项义务的行政责任。对此,欧共体委员会信息社会法律顾问委员会主席赫伯特·布尔克特指出,这体现了德国当时流行的法哲学:"如果立法者希望通过立法来规范行为,立法者不能依赖诉讼来实现。诉讼涉及各种负担,针对国家(公共部门)的诉讼更是如此。立法者需要的是设立专门的行政机构来保障公民的利益,即使这个机构的基本架构仍然与其他国家机构的设置很接近"。[④]其次,法国信息与自由委员会主导者儒瓦内在 1990 年力主通过的《联合国指南》,在"监督与制裁原则"部分明确建议成员国成立独立的行政机构来监督指南个人数据处理原则的实施。[⑤]

因此,最后通过的指令对《90 草案》做出了非常大的调整,要求成员国构建以行政救济为主、民事救济和刑事救济为辅的救济体系。[⑥] 其中,第 22 条规定数据主体提起损害赔偿之诉前可以先寻求行政救济;[⑦]第 28 条第 4 款还专门强调成员国数据监管机构享有审理个人申诉的权力。对此安排,《95 指令》前言第 62、63 目强调:"成员国设立具有完全独立权限的监管机构是保护个人利益的核心组成部分。这些机构在履行职责尤其是处理数据主体提起的申诉时,必须有必要的手段,包括调查权、干预权和参与诉讼的权力"。此外,依据服务贸易总协定个人数据与隐私保护例外,指令创设第三国适当性评估机制来限制数据向非成员国转移。不言而喻,指令强调行政执法更是为了实现创设个人数据权的目的,即以保护该权利为名事前审查和限制个人数据的跨境转移。

四、欧盟改革期:赋予个人数据权人权属性与救济机制的域外效力

由于《95 指令》实施后出现各成员国执法机制和执法力度不一致 、公民几乎未提起侵权之诉等问题,[⑧]导致欧盟在个人数据保护方面并未形成真正的统一体,也无法保证个人数据转移到第三国之后仍能够获得与欧盟一致的同等保护水平,[⑨]因此,欧盟委员会从 2010 年就开始呼吁采用成员国可直接实施的条例替代《95 指令》,[⑩]并在 2012 年正式提出《通用数据保护条例》草案,以期"所有企业将以统一的个人数

① See CEC, Amended Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of such Data, COM (92) 422 Final—SYN 287, 1992, p.11.

② 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。

③ See CEC, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) 314 Final—SYN 287, 1990, p.40.

④ Herbert Burkert, Privacy Data Protection——A German/European Perspective, in Christoph Engel and Kenneth H. Keller, Governance of Global Networks in the Light of Differing Local Values, Baden—Baden: Nomos Verlagsgesellschaft, 2000, p.46.

⑤ See United Nations General Assembly, Resolution 44/132 of 15 December 1989, Resolution 45/95 of 14 December 1990.

⑥ See Article 22—23, Article 28 of Directive 95/46/EC.

⑦ 该条个人数据权侵权使用的术语是"breach of rights"而不是传统私权侵权的"tort"。

⑧ See The RAND Corporation, Review of the European Data Protection Directive, 2009, pp.7—11.

⑨ See EC, Strategy to Strengthen EU Data Protection Rules, IP/10/1462, 2010.

⑩ See EC, Europeans' Privacy Will Be Big Challenge in Next Decade, Says EU Commissioner, IP/10/63, 2010.

据保护规则向 5 亿欧盟人销售产品和提供服务……将欧盟个人数据保护标准塑造成全球标准”。[①] 最终,借着 2013 年的“斯诺登事件”、2014 年“谷歌西班牙案”、[②]2015 年废除安全港协议的“施姆雷斯案”[③]的东风,欧盟以执行《里斯本条约》和《欧盟基本权利宪章》为名,在 2016 年通过了史上最严的《通用数据保护条例》。

1.个人数据权的人权化:提供宽泛的行政执法权与司法解释权

在《108 号公约》通过后,欧共体议会法律委员会就强调,只有将个人数据权上升为基本权利才能合法有效限制数据向美国等第三国流动,“我们现有的筹码是基本权利……由于有关保护个人数据的权利将被作为一项人权来进行保护,成员国数据保护立法应当尽可能一致,也就有必要考虑将其纳入《欧洲人权公约》”。[④]在 1997 年的《欧盟基本权利宪章》中,[⑤]这一目标终于实现。该宪章将个人数据权独立于隐私权,即宪章第 7 条在规定隐私权的同时,第 8 条第 1 款规定个人数据权是一项基本权利,第 2 款规定个人的同意权、访问权和修改权,第 3 款要求成员国设立独立监管机构来保障个人数据权。据此,欧盟委员会及其成员国的数据监管机构不用再依靠公众知情权而可获得充分的执法权——任何个人数据的保护水平只要没达到基本权利的高度,监管机构都可以进行执法——法院也可以据此审查和修正行政机关的行为。例如,欧盟法院在 2015 年的“施姆雷斯案”中直接适用宪章第 8 条,认定欧盟委员会无法通过与美国商务部签订安全港协议的形式就担保美国提供了“等同于《欧盟基本权利宪章》要求的保护水平”,从而判定安全港协议无效。[⑥]

2.新增携带权:回归个人数据权协助消费者转向本土企业的本质

虽然欧共体委员会产业与技术部早在 1973 年就强调要为欧洲消费者从美国企业转向本土企业提供协助,但是在 43 年之后才得到最为直接的立法执行,即《通用数据保护条例》第 20 条规定的数据携带权。对于此条的立法目的,《通用数据保护条例》前言第 68 目还打着“继续强化数据主体对其个人数据控制”的幌子,但第 29 条工作组在其《数据携带权指南》中就直言不讳地指出:“数据携带权的主要目的就是协助数据主体从一个服务提供者转移到另外一个服务提供者,由此促进服务提供商之间的竞争”。对于数据携带权的性质,第 29 条工作组指出,数据携带权是访问权的升级版和补充性权利,原因在于数据主体依据《95 指令》行使访问权可能受制于数据控制者选择提供给数据主体的数据格式,而“新增的数据携带权旨在对数据主体就其个人数据进行赋权,以便于协助数据主体便利地将其个人数据从一个 IT 服务环境中转移到新的环境中”。[⑦]

3.加大个人数据权的行政救济力度:天价行政处罚与域外效力

为弥补《95 指令》执法力度的有限性,防止企业出现类似脸书公司参与棱镜门计划、将个人数据分享给美国政府等“阳奉阴违”做法,欧盟有意加大了包括跨境执法在内的行政执法力度。其一,对于侵害个人数据权的行政处罚力度,2012 年《通用数据保护条例》草案还区分了反对权和其他权利的罚则,但最终文本(《通用数据保护条例》第 83 条)则统一按照反对权违规处罚这一更为严格的处罚力度,即 1 000 万欧元或企业上一年度全球营业额的 2%中较高的罚款。[⑧] 其二,对于欧盟境外数据控制者涉及向欧盟境内数据

① Viviane Reding, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, SPEECH/12/26, Munich, 2012.

② See Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

③ See Case C-362/14 Maximillian Schrems v. Data Protection Commissioner.

④ European Parliament, 1981-1982 Session Report of Proceedings of 8 March 1982, Protection of the Rights of the Individual with Regard to Data Processing, Doc. 1-548/81, p.13.

⑤ See European Parliament, Annex: The Convention Responsible for Drafting the Charter of Fundamental Rights, http://www.europarl.europa.eu/charter/composition_en.htm, 2018-09-31.

⑥ See Case C-362/14 Maximillian Schrems v. Data Protection Commissioner, para. 73.

⑦ Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, WP 242, 2016, p.4.

⑧ See EC, Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, COM (2012) 11 Final, pp.92-93.

主体提供产品或服务或者监视这些数据主体的行为的,《通用数据保护条例》(第3条)都赋权各成员国监管当局进行监管,并要求这些数据控制者必须在欧盟境内指派一名代表作为联系人,代为处理与是否遵守《通用数据保护条例》有关的行为(第27条)。

值得注意的是,对于个人数据被跨境转移到第三国,即数据接收者与数据提供者之间是合同相对方,数据接收者所在国是该合同的第三方)之后的个人数据权保障,《通用数据保护条例》将第三国是否有独立监管机构监管数据处理作为第三国个人数据保护水平适当性评估机制中的一个条件;如果第三国未能通过适当性评估但企业仍有需要进行数据跨境转移的,那么要求通过双边谈判等方式确保欧盟人在司法救济上享有国民待遇。[①] 例如,"斯诺登事件"之后,美国国会在欧盟委员会及欧盟法院的步步紧逼之下,[②]于2016年初快速通过了《司法救济法案》,允许欧盟及其25个成员国的公民以美国公民的同等身份、依据美国1974年《隐私法》对美国联邦政府使用其个人数据的行为在美国直接提起侵权诉讼。[③]

五、对我国的启示

正如美国学者詹姆斯·惠特曼对个人数据保护法的定位,"它不是逻辑的产物,不是经验的产物,也不是现代社会共同的感情需要,而是当地社会的焦虑和理想主义的产物"。[④]因此,在目前尚缺乏个人数据保护最低国际标准的情况下,我们需要从比较法的视角检视我国未来个人数据立法的目的,所需要的制度设计、功能和实施机制。

1.制度目的:旨在构建公平竞争秩序

欧共体及欧盟4个阶段的个人数据权历史演进历程清晰地表明:欧盟有关个人数据权立法的一切努力最终都是为了保护、扶持和发展欧盟本土数据处理产业,扭转欧洲数据处理市场被美国垄断的局面,维护经济安全乃至国家主权的独立,并希望在全球数据处理市场中分得一杯羹。欧盟实施这一政策的筹码是人权、5亿优质欧盟消费者和对国际规则形成规律的准确把握。因此,在《服务贸易总协定》中成功加入个人数据权可作为限制数据跨境的合法理由后,欧盟在《95指令》和《通用数据保护条例》的立法目的中都毫不掩饰地表明其保护个人数据权和规制数据跨境流动的双重立法目的。[⑤] 事实也证明,欧盟通过其精心的制度设计,一方面迫使美国在2001年和2016年先后签订妥协性的安全港协议和隐私盾协议,[⑥]另一方面赋权欧盟监管当局对谷歌、脸书等美国企业频繁开展个人数据执法调查。[⑦]

然而,我国个人数据保护立法的"焦虑"并不是他国企业主导了我国数据处理市场,我国未来的社会治理也不需要取决于外国企业的参与程度,因而在整体战略上并不需要通过个人数据保护制度尤其是个人数据权来协助我国消费者从他国企业的产品和服务中转向本土企业。相反,主导我国数据处理市场的主体恰恰是我国本土企业(如我国互联网市场的前10大企业皆为中国企业),并且部分本土企业已经在国际市场中崭露头角,其中,腾讯、阿里巴巴和百度还稳居世界互联公司市值前10强。[⑧] 因此,从根本上而言,我国在个人数据处理产业的政策上重点是谨防本土企业实施不正当竞争或者滥用市场支配地位,相应措施的关键在于构建数据处理行业的公平竞争秩序、防止最终损害消费者利益,同时还要为我国企业开拓海

① See Recital 108 of GDPR.

② See EC, Calls on the U.S. to Restore Trust in EU-U.S. Data Flows, IP/13/1166; Case C-362/14 Maximillian Schrems v. Data Protection Commissioner.

③ 不包括丹麦和英国。See H. Rept. 114-294, Part I, 2015, p.2; Public Law 114-126; Judicial Redress Act of 2015; Office of the Attorney General of the United States Department of Justice, Judicial Redress Act of 2015, 82 FR 7860, 2017.

④ James Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal, 1220 (2004).

⑤ See Article 1 of Directive 95/46/EC and Article 1 of GDPR.

⑥ 参见张平、张金平:《欧美跨境数据转移法律博弈之考察》,载中国互联网协会编著:《互联网法律》,中国工信出版社与电子工业出版社2016年版,第414~449页。

⑦ 例如,英国在剑桥分析案后对脸书公司的处罚、法国2019年对谷歌隐私政策的调查和处罚。

⑧ 参见中国互联网协会、工业和信息化部信息中心:《2018年中国互联网企业100强发展报告》,第12~14页,https://max.book118.com/html/2018/0809/8055025072001117.shtm,2019-09-03。

外市场塑造有利的国际环境。①

具体而言,在国内层面,我国最近几年发生的华为与腾讯、顺丰与菜鸟、新浪与脉脉、淘宝与美景等本土企业间的个人数据之争,不断冲击我国的竞争秩序,市场呼吁构建的是公平竞争秩序,乃至个人数据的归属及其经济利益的分配机制。② 在"新浪诉脉脉案"和"淘宝诉美景案"③中,我国法院虽限于财产权法定原则未直接认定企业对其收集或加工的个人数据享有财产权,但倾向于通过适用《反不正当竞争法》第 2 条的原则性规定来保护企业所事实掌握的个人数据及其加工而成的数据产品,以此解释公平的竞争秩序。值得注意的是,美国法院在同样是利用技术获取他人平台个人数据的"hiQ 诉领英案"④中提供了公平竞争的另一种解读:基于 hiQ 公司完全依靠抓取和分析领英公司所公开的用户个人信息而生存、领英公司推出与 hiQ 公司具有直接竞争关系的业务并继续允许其他第三方获取涉案个人信息等因素,判决领英公司不得禁止 hiQ 公司抓取用户公开的个人信息。因此,面对未来我国越来越普遍的数据竞争方面的纠纷,我国法院在解释公平竞争秩序时还需要更全面的考虑,在行为定性上应当更加谨慎。⑤

在国际层面,公平竞争秩序的构建也要考虑到中国企业的海外市场扩展,因此我国立法需要为中国企业主动提供制度支持。数据产业的竞争并不仅仅在于国内市场的争夺,还延伸到海外市场的争夺,而且其中往往涉及数据处理科技的竞争问题,当地政府可能以各种理由阻止中国企业的进入。例如,蚂蚁金服和华为手机进入美国市场时,美国政府都以这两家企业可能将在美国收集的个人数据跨境转移到中国后分享给中国政府为由加以阻挠。美国这种做法与欧盟通过个人数据保护法限制美国企业在目的上是一致的,只是在策略上更直接罢了。⑥ 面对这样的阻力,我国政府需要为本土企业进入海外市场提供良好的国际环境,关键是加强执法的透明度建设。例如,《网络安全法》第 28 条规定网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助(如提供涉案个人信息),但目前尚未在制度文本上提供更为详细的执法协助程序,因而在透明度建设上尚有提升的空间。⑦ 在此问题上,美国《通讯执法协助法》第 103 条也有类似的执法协助规定,并在文本上规定通过法院命令或者其他合法授权途径才能要求企业提供执法协助。⑧ 即便如此,在欧美隐私盾协议谈判中,美国面对欧盟的压力仍然不得不在执法协助透明度上加码,同意增设隐私监察使、与欧盟共同设立隐私保护小组等机制。⑨ 因此,在未来的个人数据保护法或者数据安全法的立法当中,还需要增加企业执法协助方面的透明度机制。

2.制度设计:个人数据权定性为参与原则下的知情权

为实现对美国企业的限制,欧盟巧妙地选取了个人数据权这个"小权利",通过 30 多年的努力,将其从知情权雏形发展到囊括携带权和被遗忘权的完整体系,并将其性质从普通私权上升为一项美国无法质疑的基本权利。即便如此,欧盟在《95 指令》《欧盟基本权利宪章》和《通用数据保护条例》等立法及其立法草案中都从未指出个人数据权源自信息自决权,因为德国联邦宪法法院创设的信息自决权仅适用于个人对抗公权力。⑩ 例如,欧共体委员会在 1990 年针对公共部门处理个人数据提议的《关于公共数字通信网络

① 参见王晓晔:《竞争政策为什么应成为国家基本经济政策》,《中国价格监管与反垄断》2016 年第 3 期。

② 参见龙卫球:《数据新型财产权构建及其体系研究》,《政法论坛》2017 年第 7 期;程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018 年第 3 期。

③ 参见北京市海淀区人民法院(2015)海民(知)初字第 12602 号民事判决书,北京知识产权法院(2016)京 73 民终 588 号民事判决书;杭州互联网法院(2017)浙 8601 民初 4034 号民事判决书。

④ See hiQ Labs, Inc. v. Linkedin Corporation, Order Granting Plaintiff's Motion for Preliminary Injunction, Docket No. 23, Aug. 14, 2017.

⑤ 参见陈兵:《大数据的竞争法属性及规制意义》,《法学》2018 年第 8 期。

⑥ See S. 3361—Fair Trade with China Enforcement Act, 115th Congress (2017—2018).

⑦ See US—China Business Council, Letter on PRCG Cybersecurity Regulations, Aug. 10, 2016.

⑧ See Section 103 of Communications Assistance for Law Enforcement Act of 1994.

⑨ See European Commission, On the Adequacy of the Protection Provided by the EU—U.S. Privacy Shield, C (2016)4176, paras. 64—90.

⑩ 该案创设的信息自决权可以解释为民主政治中公众对政府行为的知情权,即公众监督政府行使权利的前置性权利。参见何生根:《知情权之属性之学理研究》,《法律科学》2005 年第 5 期。

下保护个人数据的指令(草案)》建议稿中,曾指出个人数据保护的目的之一是"确保公共数字通信网络用户的信息自决权",但该指令并未获得通过。①

相反,在不同的制度目的下,我国未来所要构建的个人数据权或者个人数据权益并不是人权意义上的权利,更不应当以信息自决权为基础。个人数据处理之所以会成为当今社会的关注点,在很大程度上是因为计算机技术的发展让我们进入到信息社会和数字社会,数据处理成为人们生活、社会经济发展的重要内容。并且,个人数据在事实上由收集者所掌握和控制,个人无从知道和控制其个人数据是否被收集、处理和向第三方披露,也不知道其个人数据被用于何种目的。② 因此,世界各国都无法回避个人数据的保护问题,但规制的办法并非仅有欧盟以个人控制为核心创设个人数据权的唯一出路。例如,美国以产业利益为主导的个人数据公平处理原则,并不强调通过统一立法创设个人数据权,仅仅要求企业在处理个人数据的实践中保障个人一定的参与权或者知情权,即允许个人参与决定哪些个人数据可以被收集、如何使用和披露。③ 质言之,各国的法律及政策并不必然以个人数据权为核心来构建相关的数据保护与利用规则,而是根据本国的个人、企业和国家的实际以及传统提供相应的制度安排。因此,只要本土企业主导了国内相关市场,我国就没有必要将个人数据自动化处理当作洪水猛兽,复制欧盟的做法、处处以保护个人数据权为名作茧自缚,而要侧重于培育市场的公平竞争,以及对处于相对弱势地位的消费者提供适当保护。

具体而言,目前《民法总则》第111条和《网络安全法》第4章都没有明确个人对其个人数据的合法利益是否以权利形式存在。对此,在构建公平竞争秩序、发展我国数字经济的宗旨下,我国在未来立法中有必要进一步明确,将个人数据权塑造成性质为综合性的知情权,在功能上仅保护个人对其个人数据一定的积极参与权,不延及消极属性的隐私权,且在内部构造上以访问权为核心,以被通知权为前提,以修改权为延伸。其中,在权利定性上,知情权兼具私权和公权的综合性质:④一方面,个人数据权具有私权属性,提供个人参与决定企业收集和使用其个人数据是否合法公平的机会;另一方面,个人数据权具有公权属性,旨在监督政府的个人数据处理行为。这一点从《网络安全法》第41条至第43条以及第76条有关网络经营者(并不区分公私主体)的规定中可以得到佐证。在功能上,知情权保护个人参与有关其个人数据处理中的合法利益,确保相关数据处理是公平合理、不被滥用的,因而并不保障个人能够单方面控制其个人数据的披露和使用。这与个人在数字经济时代参与正常经济社会交往的事实不符合,也不符合我国数字经济的发展需求。这一点早已为1980年《经济合作与发展组织指南》的个人参与原则所承认。此外,欧共体委员会早在1980年的《访问权的技术面向》中指出了知情权与隐私权的差异,后者是防止个人数据的过多披露,要求数据处理者做好安全保障措施。对此,我国民法典人格权编应当明确独立出个人数据权,同时强调个人数据权是参与原则下的知情权,并非绝对权。⑤ 在权利内部构造中,知情权的核心权利是访问权,即个人有权知道其被收集和处理的个人数据的具体内容;而行使访问权的前提是被通知权,即个人获得通知、确认其个人数据被收集;知情后的必然结果是请求修改或者删除不正确的个人数据,以免对个人造成不利后果。⑥ 至于超越参与原则、容易增加企业不符合比例原则的执行成本的反对权、被遗忘权和携带权,则尚不适宜引入我国。目前,《网络安全法》第43条仅规定个人在一定条件下的请求网络运营者删除或更正其个人信息的权利,但并未关注到该两项权利的前置性权利(即访问权),也未能提供个人行使这两项权利的实施细则。就整体而言,在我国未来的个人数据立法中,参与原则下个人知情权体系的构建仍

① See CEC, Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network and Public Digital Mobile Networks, COM (90) 314 Final—SYN 288, 1990, p.85.

② 参见郑成思主编:《知识产权——应用法学与基本理论》,人民出版社2005年版,第84页。

③ See U.S. Department of Health, Education & Welfare, Records, Computers and the Rights of Citizens, July 1973, No. (OS) 73—94, pp.41—42.

④ 参见何生根:《知情权之属性之学理研究》,《法律科学》2005年第5期;刘艺:《知情权的权利属性探讨》,《现代法学》2004年第4期;曹艳春:《知情权的私法保护》,《政治与法律》2005年第4期;肖玉英:《试论隐私权与知情权》,《法学杂志》2001年第4期。

⑤ 有关知情权在民法下可以构成具体人格权的论述,可参见曹艳春:《知情权的私法保护》,《政治与法律》2005年第4期。

⑥ See Explanatory Memorandum of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para. 13.

然有充分的制度空间。

3.实施机制:更为灵活和宽松

为了构建公平竞争秩序、保护参与原则下的个人数据权,我国未来立法所需要的法律实施机制不应当代替企业直接设置各项具有很强主观性的实践指标,也不宜采取天价行政处罚的政策,而应尽可能采用企业可以根据市场发展不断自行调整的个人数据处理注意义务,以及未履行这些义务的法律责任。不论是欧盟以个人数据权为核心构建的个人数据保护体系还是美国以行业自律为基础的机制,其最终的实施机制都是对企业设置特定的法律义务,若违反该义务则承担相应的责任。因此,企业处理个人数据的法律义务及其责任的设定,将直接涉及企业的执行成本以及整个个人数据保护机制的实施效果。如果仅从保护个人利益的角度看,那么对企业设置越高、越具体的法律义务能够越好地保障个人利益,但企业的执行成本也就相应增高。另外,如果违反该义务的责任非常严格和僵硬,那么就无法为我国企业在全球激烈的数据产业领域的竞争提供相对的制度优势。在这一方面,欧盟为了反制美国企业,在《通用数据保护条例》中增设企业的各项义务和采用可以媲美反垄断处罚力度的罚则,但欧盟忽视了这种法律实施机制也适用于本土企业,更何况美国企业的创新是源自美国本土,因而最终难以实现在本土"培育强有力的竞争对手"的初衷。相反,美国联邦政府对于个人就其个人数据享有的权益以及企业处理个人数据的义务都极力保持克制,至今未通过联邦立法直接加以明确,而是留给行业自律,并主要通过联邦贸易委会监督企业是否自律。[①] 如此一来,美国企业可以根据自身发展情况做出适当的保护消费者的承诺、构建和维护自己的良好商业信誉。相比之下,目前《网络安全法》仍然主要以法律直接设定企业处理个人数据的义务为主,而未引入"隐私权设计"的义务体系和反对权、被遗忘权和携带权,在违反义务的责任设置上则兼顾了民事、行政和刑事法律责任。[②] 其中,在行政责任方面,《网络安全法》提供了多种灵活的制裁措施,包括责令改正、警告、没收违法所得、罚款、责令暂停业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。因此,就目前而言,我国在个人数据保护上构建了比较灵活和相对宽松的执法机制,与我国现有的产业发展和个人利益保护需求比较协调,但具体的实施效果还有待进一步观察。

此外,在数据跨境规则和域外效力问题上,我国应当保有与本土企业实力相匹配的大国风范,并为我国企业拓展"一带一路"等海外市场创设和维系良好的国际环境。目前,《网络安全法》已经通过第 37 条建立起针对关键信息基础设施经营者转移个人数据和重要数据的安全评估机制,并未对一般网络经营者的个人数据跨境加以限制,但由于我国数据处理市场主要以本土企业为主,数据跨境更多地由本土企业发起,因此具体的数据跨境安全评估标准不宜过严,以免限制我国企业的海外市场发展。[③] 与此同时,未来立法也无须急于增设具有类似于欧盟域外效力的相关规则。欧盟《通用数据保护条例》第 3 条赋予该法域外效力旨在防止非欧盟境内企业处理个人数据时降低欧盟人的个人数据保护水平,但得结合第 27 条(要求境外企业在欧盟境内指派代理人)才能进行行政执法。然而,《通用数据保护条例》并未规定违反第 27 条的法律责任,并且这种行政执法管辖权的扩张会直接涉及他国的国家主权,因此其本身的合法性还值得商榷。[④] 相反,我国应当考虑规定类似于美国《澄清合法使用境外数据法》创设的企业执法协助机制。因为该法要求在美国设立的企业有义务在接到法院传票后提供其控制的电子通讯信息(即使该信息存储在美国境外也不例外)。[⑤] 如果这些企业不遵守该法,那么美国可以直接对其进行相应处罚。

责任编辑 张家勇

① See Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, 2012, p.11, p. 73.

② 参见《中华人民共和国网络安全法》第 64 条、第 66 条、第 74 条。

③ 参见张新宝:《我国个人信息保护法立法主要矛盾研讨》,《吉林大学社会科学学报》2018 年第 5 期。

④ See United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, 2016, pp.18—19.

⑤ See Clarifying Lawful Overseas Use of Data Act (18 U.S.C. § 2713).