

论数据携带权的属性、影响与中国应用

丁 晓 东*

摘 要: 欧盟颁布的《一般数据保护条例》首次在立法中确立了数据携带权,赋予个体无障碍地获取与转移个人数据的权利。但数据携带权并不具有成为一种基本权利的条件,而且可能带来诸多负面影响,不利于数字市场的良性竞争。应当将数据的可携带性视为一种努力目标,并且应当根据不同的情形对数据控制者施加不同的责任。对于中国而言,首先要避免在立法层面照搬照抄欧盟的数据携带权。其次,在涉及数据获取与转移的场合,需要在不同的场景中赋予个体不同程度的数据携带权。在不影响隐私期待及相关主体合法权益的前提下,企业应当为个体提供获取数据的便利,并且不应应对普通用户设置数据转移的技术障碍。此外,还可以利用数据携带权倒逼政府实行数据共享。

关键词: 数据携带权 个人信息保护 竞争法 政府数据共享

DOI:10.16390/j.cnki.issn1672-0393.2020.01.007

2018年5月25日,欧盟颁布的《一般数据保护条例》正式生效。这一法律史无前例地引入数据携带权,赋予数据主体以获取和传输个人数据的权利。根据《一般数据保护条例》第20条的规定,数据主体有权获取“经过整理的、普遍使用的和机器可读的”个人数据,有权“无障碍地将此类数据从收集其数据的控制者那里传输给其他控制者”。^①

无疑,数据携带权将对用户的数据权利产生重要的影响。数据携带权使用户能够在不同的网站和设备上自由地转移个人数据,用户对个人数据的控制能力将达到前所未有的高度。因此,这一权利的支持者指出,数据携带权将促进用户福利,打破数据壁垒与数据垄断,促进数据共享与数据流通。但与此同时,数据携带权的反对者也指出这一权利可能带来的种种问题。例如,这一权利可能带来技术性难题,为企业附加过多的责任;又如,数据携带权未必能够促进用户福利,未必有利于市场的良性竞争。

围绕数据携带权问题之所以产生争议,是因为理论研究未能澄清数据携带权的权利属性问题,未

* 中国人民大学法学院、中国人民大学未来法治研究院副教授、博士生导师
基金项目:国家社会科学基金项目(18BFX198)

① 本文所引用的《一般数据保护条例》的中文版本为作者所译,参见《欧洲一般数据保护条例》,丁晓东译, <http://www.calaw.cn/article/default.asp?id=12864>, 2018-09-05。下文引用均为此译本,部分译文做了修改。

能充分认知该权利对市场竞争秩序的影响。^①那么,究竟该如何认识数据携带权这一新型权利的权利属性?其对市场竞争秩序有何影响?本文拟对此进行深入剖析,并在此基础上对数据携带权的中国应用问题进行讨论,探讨我国正在制定的个人信息保护法是否应当移植或借鉴欧盟的数据携带权,^②以及如何在争议案件与具体场景中运用这一权利。

一、数据携带权的起源、要素与争议

(一) 数据携带权的起源

数据携带权的起源可以追溯到2007年。随着网络平台的支配力越来越大,其对用户权益的影响也越来越大,一些专家学者在2007年提出“社交网络用户权利法案”的宣言,要求强化网络社会中的个人数据权利。^③伴随着这一理念和运动,一些社会活动者创立了“数据可携带项目”,提出数据携带权的概念。该项目认为,数据携带权意味着个人可以“获取个人的数据并将其移植到一个平台上或者替换平台上之前的数据”,数据携带权将帮助网络用户实现“人们在互操作的应用程序中重新使用数据的能力”。^④

在“数据可携带项目”提出后不久,一些社会组织、政府和企业也加入倡导数据携带权的动议。2010年,隐私权组织“电子隐私基金会”建议,数据可携带权应该是“社交网络用户隐私权法案”的一个组成部分。^⑤同年,美国白宫发起“我的数据”(My Data)倡议,强调便捷化数据访问,同时提高数据的可移植性。^⑥2011年,谷歌和脸谱加入“数据可携带项目”。^⑦谷歌创建“谷歌外带”(Google Takeout)工具,允许用户从27个谷歌产品中下载数据。^⑧在脸谱平台上,用户不仅可以下载其个人资料中共享的信息,还可以下载脸谱所保存的其他不可见信息,如用户点击的广告、用于登录的IP地址等信息。^⑨

经过众多专家学者、社会组织和政府机构的倡议,欧盟委员会在起草《一般数据保护条例(草案)》时,正式将数据携带权列入数据主体所享有的一系列数据权利中。根据欧盟委员会的意见,数据携带

^① 目前关于数据携带权的研究较少,相关文献参见曹亚廷:《数据可携带权及其对征信业影响初探》,《征信》2016年第9期;李蕾:《数据可携带权:结构、归类与属性》,《中国科技论坛》2018年第6期。

^② 全国人大常委会法工委发言人岳仲明表示,2020年将制定个人信息保护法、数据安全法等。参见《2020年将制定个人信息保护法、数据安全法》,http://www.sohu.com/a/361947598_612075,2019-12-23。

^③ See Joseph Smarr, Marc Canter, Robert Scoble, Michael Arrington and others, A Bill of Rights for Users of the Social Web, http://www.template.org/?page_id=599, 2018-09-09。

^④ Data Portability Project, http://dataportability.org, 2018-09-10。

^⑤ See Kurt Opsahl, A Bill of Privacy Rights for Social Network Users, https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users, 2018-09-12。

^⑥ See Kristen Honey, Phaedra Chrousos & Tom Black, My Data: Empowering All Americans with Personal Data Access, https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access, 2018-09-12。

^⑦ See Duncan Riley, Facebook, Google and Plaxo Join the Data Portability Workgroup, http://techcrunch.com/2008/01/08/this-day-will-be-remembered-facebook-google-and-plaxo-join-the-dataportability-workgroup, 2018-09-13。

^⑧ See Download Your Data, https://takeout.google.com/settings/takeout, 2018-09-14。

^⑨ See What Categories of My Facebook Data are Available to Me? https://www.facebook.com/help/405183566203254, 2018-09-14。

权可以提升用户对于个人数据的控制程度,促进网络空间中网络服务商与用户之间的信任。此后,数据携带权面临种种怀疑和指控,并且一度在草案中被取消。但在2016年通过的最终版本中,这一新生的数据权利还是被保留了下来,作为与数据访问权、更正权、被遗忘权、限制处理权等权利相并列的数据权利。^①

(二)数据携带权的要素

对于数据携带权,《一般数据保护条例》的“重述”以及第29工作组对其作出了进一步的阐释。^②根据“重述”特别是第29工作组发布的指南,数据携带权包含如下基本要素:

第一,就权利属性而言,数据携带权首先意味着,数据主体有权下载关于个人数据的集合。就这一点而言,数据携带权可以说是数据访问权的进一步扩张,它不仅赋予数据主体以访问个人数据的权利,^③而且为数据主体管理和重新使用个人数据提供了更为方便的途径。数据携带权赋予个体以一种“经过整理的、普遍使用的和机器可读的”方式来获取和下载个人数据。例如,数据主体如果有兴趣获取其在某个音乐网站所选择的音乐列表,或者听歌的历史记录,或者想获得网页电子邮件里的联系人列表,就都有权要求网站提供此类下载链接。^④数据携带权还赋予数据主体以自由迁徙数据的权利。《一般数据保护条例》第20条第1、2款不仅禁止数据控制者人为设置传输障碍,妨碍数据主体传输个人数据,而且要求其在技术允许的情形下必须为数据主体传输个人数据提供便利。如果技术可行,那么数据控制者有义务使个人能够在数据控制者之间传输个人数据。^⑤

第二,就数据携带权所涉及的数据范围而言,《一般数据保护条例》第20条第1款将其范围限定在“数据主体提供与数据主体有关的个人数据”。这一范围首先排除了匿名化的数据或与数据主体无关的数据。^⑥但第29工作组发布的指南也指出,不应对此进行过于严格的解释。在不会对第三方的权利和自由产生不良影响的情况下,可被移植的数据也应当包括涉及多人的数据,如电话、人际互动或网络通讯记录等可能涉及他人的数据,当个人请求对这些数据行使数据携带权时,此类数据也应当被包括在数据携带权的范围之内。^⑦

第三,就下载的格式而言,数据携带权要求下载的格式是“经过整理的、普遍使用的和机器可读

^① 参见丁晓东:《什么是数据权利?——从欧洲〈一般数据保护条例〉看数据隐私的保护》,《华东政法大学学报》2018年第4期。

^② “重述”不具有法律效力,但为《一般数据保护条例》提供补充信息,帮助相关主体理解和适用条例;第29工作组(29 Working Party)是一个根据1995年《欧盟数据保护指令》第29条成立的咨询机构,由欧盟成员国数据保护机构、欧洲数据保护监督员和欧洲委员会组成的代表组成,意为为欧盟各国的数据保护提供专业指引。2018年5月25日以后,这个工作小组由欧洲数据保护委员会(European Data Protection Board)替代。

^③ 参见《一般数据保护条例》第15条。

^④ See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-09-18.

^⑤ 正如第29工作组发布的指南所指出的:“数据可携带性可促进用户在不同机构之间控制和有限地分享个人数据,从而丰富服务和改善用户体验。数据可携带性可促进用户在他们感兴趣的各服务之间传输和重用与他们有关的个人数据。”See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-10-20.

^⑥ 能够关联到个体的假名化的数据(pseudonymous data)将被视为个人数据。

^⑦ See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-09-18.

的”。第29工作组发布的指南指出,对于什么是“普遍使用的”,要视具体场景和技术共识而定,在没有约定和共识的情况下,应当使用通用的开放格式的数据,以使数据的重新利用成为可能。数据控制者不得以非通用格式为个人提供数据,因为这会使得用户无法便捷地重新使用数据。^①而对于“机器可读的”格式,欧盟的相关法律则将其定义为“使软件应用程序能够轻易地识别、认知和提取特定数据的格式”,而那些限制自动处理的文件格式编码的文档将被排除在外,因为从这些文档中很难提取相应数据。^②

第29工作组发布的指南还指出,下载格式应当符合互操作性的要求。这一要求“强烈鼓励行业利益相关者与行业协会之间进行合作,共同制定一套通用的可互操作的标准和格式,以实现数据可移植性的要求”。^③但另外,第29工作组发布的指南也指出,这种互操作性的要求并不一定要达到兼容性要求的程度。^④互操作性与兼容性的区别在于,互操作性要求在用户不知道或不太清楚功能单元性能的情况下仍然可以在不同功能单元之间进行交流、运行程序或传输数据,而兼容性则要求不同的系统可以实现兼容。^⑤

(三)数据携带权的争议

自从数据携带权被提出以来,围绕这一权利就存在很多争议。支持者与反对者分别提出了若干对立意见。具体说来:

1. 数据携带权的支持意见

第一,数据携带权可以强化用户或数据主体对个人数据的控制。数据携带权的支持者指出,信息隐私的关键在于对个人信息的控制。在这个意义上,通过赋予用户以获取和移植自身数据的权利,用户可以进一步强化对自身数据的控制,从而获得更好的服务和用户体验。^⑥

第二,数据携带权可以消除数据的“锁定效应”,促进网络与数字市场中的竞争。支持者指出,网络服务商或其他服务商在为用户提供服务时,常常会设置各种壁垒和障碍,防止用户转移到其他网站或服务器上,用户即使对网站或服务设备感到不满,也常常会因为数据难以转移等问题而放弃迁移。^⑦因此,通过赋予个人数据携带权,消除个人数据自由传输的不必要障碍,可以促进竞争,消除或

^① See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-09-18.

^② See Amending Directive 2003/98/EC on the Re-Use of Public Sector Information, <http://www.nationalarchives.gov.uk/documents/information-management/response-open-data-user-group.pdf>, 2018-09-18.

^③ See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-09-09.

^④ 如同《一般数据保护条例》“重述”第68条所指出的:“数据主体具有发送或接收有关他或她的个人数据的权利,但不应当对控制者施加采用或维护技术兼容的处理系统的责任。”

^⑤ 例如,基于互操作性的要求,用户在苹果 Mac OS X 系统上所建立的文档应当能够传输到 Windows 系统上,但 Mac OS X 系统与 Windows 系统并不兼容。

^⑥ 如同第29工作组发布的指南所指出的,数据携带权这项新权利的目的在于“赋予数据主体权利,并给予他/她对有关他或她的个人数据更多控制权”。See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-10-20.

^⑦ See Laise Bornico and Ian Walden, Ensuring Competition in the Clouds: The Role of Competition Law? 12 ERA Forum, 282(2011).

至少部分消除“锁定效应”。^①

此外,支持者还提出了一些与以上两点理由相关的论点。例如,数据携带权可以促进用户与数据控制者之间的信任,同时提升用户与数据控制者的福利。也就是说,一方面数据携带权可以改进用户的使用体验,给用户带来更多便利,另一方面,数据携带权也可以让商家或数据控制者更为方便有效地获取更多用户数据,因为很多用户在行使数据携带权的同时,常常不会删除之前所保存的记录。这样,数据携带权就可能促进数据的共享,实现用户与数据控制者的双赢。^②

2. 数据携带权的反对意见

第一,数据携带权不能成为一种权利。有学者指出,数据携带权在欧盟的实证法体系下不能成立。《欧盟基本权利宪章》规定“每个人都有权获得个人数据保护”,但对此《欧盟基本权利宪章》只规定了特定的权利,如数据被公平处理的权利,数据收集须获取个人同意或其他正当理由的权利,数据访问权与更正权,《欧盟基本权利宪章》并没有将数据携带权视为一种基本的数据权利。^③也有学者指出,对于数据权利是否包括数据携带权,还未达成共识。^④在未达成共识的情形下将数据携带权上升为一种基本权利,这并不明智。^⑤

反对者指出,数据携带权不仅不能成为数据隐私权的一种,而且也未必有利于用户的数据隐私保护。在反对者看来,个人数据访问权已经存在不少安全隐患,实践中已经出现很多他人盗用或冒充某个用户行使数据访问权从而非法获取个人数据的情形。如果用户被赋予数据携带权,那么此种风险将成倍增加,因为基于数据携带权的要求,用户将能够一次性地批量下载和转移所有个人信息,一旦他人成功盗用或冒充某个用户,就可能瞬间获取和转移这位用户的所有信息。^⑥此外,数据携带权所涉及的数据可能包含他人数据,如个人图片可能常常包含与其他人的合影、个人聊天记录可能包含他人隐私。^⑦

第二,数据携带权不一定能够促进市场竞争。对于“锁定效应”,反对者首先指出,数据携带权的确有助于消解“锁定效应”和促进数据流通,但其效果却并不一定总是促使用户将数据从大企业转移到中小企业,相反,其效果完全可能促使用户将数据从中小企业转移到大企业,从而阻碍中小企业发展。其次,数据携带权所鼓励的互操作性的难度非常大,成本也非常高,因为现实中实现不同系统与

^① See Urs Gasser & John Palfrey, *Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation*, <http://cyber.law.harvard.edu/interop/pdfs/inter-op-breaking-barriers.pdf>, 2018-10-10.

^② See Elias Bizannes, *Why Every Site should Have Data Portability Policy*, <http://techcrunch.com/2010/06/23/data-portability-policy>, 2018-10-15.

^③ See Inge Graef, Martin Husovec & Nadezhda Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, <https://ssrn.com/abstract=3071875>, 2018-10-16.

^④ See David Krebs, *Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union*, 10 *Canadian Journal of Law and Technology*, 38(2012).

^⑤ See Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare*, 72 *Maryland Law Review*, 373(2017).

^⑥ See Stefan Weiss, *Privacy Threat Model for Data Portability in Social Networks Applications*, 29 *International Journal of Information Management*, 250 (2009).

^⑦ See Barbara Van der Auwermelen, *How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations*, 1 *Computer Law & Security Review*, 60 (2017).

功能单元之间的互操作性非常困难;^①这样,数据携带权就可能会给中小企业造成更大的合规压力。最后,数据携带权的行使可能侵犯企业的知识产权,因为企业所收集的个人信息可能已经符合企业商业秘密的保护标准,或者可以获得数据库的保护。^②

二、数据携带权的权利属性之剖析

对于数据携带权,支持意见与反对意见的争议焦点首先是数据携带权的权利属性:数据携带权是否可以成为一种权利。支持者认为数据携带权是公民数据权利的自然延伸,有利于在网络与信息时代对公民进行数据赋权;反对者则认为这种权利并无共识,而且未必有利于保护公民的相关权益。

就权利理论的原理而言,支持者的理由具有一定的道理。毋庸置疑,从《欧盟基本权利宪章》中只能推导出公民的若干数据权利,如公民的个人信息访问权、个人信息被平等对待的权利,而并不能直接推出数据携带权。但《一般数据保护条例》中确立的大量数据权利本身就是对传统数据权利的拓展,“数据主体的权利”这一章规定了一系列重要权利:数据主体对个人数据的访问权、更正权、擦除权(被遗忘权)、限制处理权、数据携带权、一般反对权和反对自动化决策的权利,这些数据权利很多都不能被传统的数据权利囊括。^③

从权利理论的角度来看,权利的内涵与边界本身就是随着时代发展而变化的,现代社会在强调消极权利的同时,早已经越来越多地拥抱积极性权利。^④ 隐私权利与个人信息权利的历史演化就说明了这一点。1890年,美国学者沃伦与布兰代斯提出隐私权概念时,首先提出的是作为防御性权利的隐私权。^⑤ 其后,现代数据隐私法的权威阿兰·威斯丁又提出了积极性的信息权利或数据权利的概念,将数据权利界定为个人对自身信息的积极性控制。^⑥ 从强化用户控制的角度思考数据携带权,可以发现数据携带权正是数据个人控制权的逻辑终点,这种权利将使个人的数据权益从一种消极性的防御性权利转向一种积极性的控制性权利。^⑦

不过,反对者所提的理由也不容忽视。在纸面上将数据携带权上升为一种基本权利,这并不困

^① See Peter Swire & Yianni Lagos, Why the Right to Data Portability likely Reduces Consumer Welfare, 72 Maryland Law Review, 355-356 (2017).

^② 有的公司直接将商业秘密作为不提供用户下载数据的理由。See Emil Protalinsk, Facebook: Releasing Your Personal Data Reveals our Trade Secrets, <http://www.zdnet.com/blog/facebook/facebook-releasing-your-personal-data-reveals-our-trade-secrets/4552>, 2018-10-18.

^③ 参进程啸:《论大数据时代的个人信息权利》,《中国社会科学》2018年第3期;丁晓东:《论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析》,《现代法学》2019年第3期。

^④ See Henry Shue, Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy, Princeton University Press, 1980; Lawrence Coker, Positive Liberty: An Essay in Normative Political Philosophy, Kluwer Academic Publishers, 1980; Cass Sunstein, After the Rights Revolution: Reconceiving the Regulatory State, Harvard University Press, 1993; Stephen S. Holmes & Cass S. Sunstein, The Costs of Rights, W.W. Norton, 1999; Thomas Halper, Positive Rights in a Republic of Talk, A Survey and a Critique, Kluwer Academic Publishers, 2003.

^⑤ See Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review, 193 (1890).

^⑥ See Alan Westin, Privacy and Freedom, Atheneum, 1967, p.7.

^⑦ 这种积极数据权利也为其他很多学者所分享。Arthur R. Miller, Assault on Privacy: Computers, Data Banks and Dossiers, The University of Michigan Press, 1971, p.25; W.A. Parent, Recent Work on the Concept of Privacy, 20 American Philosophy Quarterly, 346 (1983); Jonathan Zittrain, What the Publisher can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, 52 Stanford Law Review, 1203 (2000).

难,但可携带性是否可以成为个人数据的一种属性,却值得商榷。有不少学者试图从财产权或类似权利的角度来定性个人数据权,认为可携带性应当成为数据权利的重要特征,但是不同于一般财产,数据具有许多独特性,如个人数据并非独立存在的客体,其储存完全依赖其他载体;^①并且个人数据常常与特定场景中的技术性载体密切结合,强行在法律上赋予个人数据可以携带的属性,特别是要求个人数据可以在不同的企业与操作系统之间自由转移,在操作上其实并不容易实现。《一般数据保护条例》“重述”与第 29 工作组发布的指南所设想的互操作性,在实践中其实非常难以实现。例如,有的专家曾经研究过替代微软现有文件的其他格式,^②结果发现,这些试图实现互操作性的文件格式之间存在“非常严重的互操作性问题”,其较轻的后果是格式化的问题,较重的后果是导致图片、脚注、注释、图表等内容的丢失。^③

将数据携带权上升为一种基本权利,也的确会带来相应的风险以及侵害其他权利的可能。如反对者所说,当用户被他人冒充,用户的个人数据就有可能被全部挪用,尤其是当某些黑色产业利用较为先进的技术手段时,这甚至可能会导致海量的个人数据被盗。对于这种风险,其实从第 29 工作组发布的指南中也可以部分看出。第 29 工作组发布的指南专门指出,数据控制者必须完全确认用户的身份,当数据控制者对用户的身份存疑时,其可以对用户的身份提出进一步验证的请求。^④这一规定表明,第 29 工作组其实意识到数据携带权可能给用户带来的数据泄露风险,只是第 29 工作组相信通过有关验证机制就可以确保用户身份的真实性。^⑤

此外,数据携带权的权利边界还可能面临过窄或过宽的困境,从而使数据携带权失去意义或侵犯其他合法权益。一方面,当把数据携带权界定为只是“数据主体提供的与数据主体有关的个人数据”^⑥时,很多数据将不能被纳入数据携带权的范围,如个人在云服务器上储存的与个人无关的视频文件,在电商平台上留下的用户评论。在很多情况下,其实个人更在意的是此类数据的自由下载和移植,如个人可能希望将此类视频文件从网易云传输到百度云,将对某个产品的差评从京东转移到淘

① 参见梅夏英:《数据的法律属性及其民法定位》,《中国社会科学》2016年第9期。

② 例如开放文件(OpenDocument)格式,这一格式被“促进结构化信息标准组织”(Organization for the Advancement of Structured Information Standards)认为是全球领先的文件标准,2005年被认定为国际标准。See OpenDocument Format, <http://opendocumentformat.org/>, 2018-12-08.

③ See Rajiv Shah & Jay P. Kesan, Lost in Translation: Interoperability Issues for Open Standards, https://law.depaul.edu/about/centers-and-institutes/center-for-intellectual-property-law-and-information-technology/programs/Documents/ipsc_2011/papers/KesanJ_Paper.pdf, 2018-12-08.

④ See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-09-18.

⑤ 从风险控制的角度来看,第 29 工作组的这种自信存在一定的疑问,毕竟面对海量的用户,企业或网站不可能对用户的身份进行一一的人工验证,并且即使能够进行人工验证,也很难保证用户身份的真实性。

⑥ 就“数据主体提供”这一界定而言,第 29 工作组将其限定为两类数据,一类是数据主体主动提供的数据,例如邮寄地址、用户名、年龄等;另一类是由数据对象通过使用服务或设备提供的观测数据,如个人的搜索历史、交通数据和位置数据等。但第 29 工作组也指出,此类数据不应当包括“推断数据”和“派生数据”,即通过后续分析得到的数据,如关于用户健康状况评估结果的数据、银行征信管理系统中出于风控目的创设的用户数据、网站为用户创设的用户画像数据。See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-10-22.

宝。^①第29工作组虽然认为不宜将个人数据做过窄解释,^②但仍无法涵盖此类显然不是个人数据的数据类型。另一方面,数据携带权的行使又可能过宽,从而侵害其他企业或个人的合法权益。除了像反对者所说的个人数据移植可能侵犯企业的商业秘密或数据库权益之外,个人数据的转移还可能会侵犯他人的利益。例如,在社交网络的场景中,当个人把数据成批量地从一种社交场景转移到另一种社交场景时,就可能导致个人数据所涉及的第三人数据被不恰当地获取与使用。^③我们知道,2018年发生了举世震惊脸谱数据泄露事件,^④在此事件中,剑桥分析公司通过一款应用程序收集了30万用户的信息,并通过授权获得这30万人的朋友圈,从中获得了5000万人的信息。虽然此案涉及的是剑桥分析公司对于这5000万人信息在没有获得授权情况下的非法使用,没有涉及数据携带权,但此案所隐含的数据携带权困境却非常明显。如果用户首先行使数据携带权,下载其“结构化的、普遍使用的和机器可读的”信息,然后将这些数据授权给剑桥分析公司使用,此时剑桥分析公司完全可以声称此类数据是合法获得的。但是,此种情况下很多用户的信息也可能面临不正当收集与使用的威胁。

为何数据携带权上升为一种基本权利存在问题,这需要分析基本权利的一般原理与数据携带权的特殊性。权利的赋予常常会影响其他相关主体的某些权利。借用美国法学家卫斯理·霍菲尔德的权利分析框架,当某种权利赋予主体以一种特权或自由类型的权利时,对方就无权对抗此种权利;当某种权利赋予主体以一种权利主张类型的权利时,他者就有责任履行相关义务。^⑤而在数据携带权问题上,这种权利所附加给数据控制者的义务比一般权利赋予相对方的责任更大,对其他权利造成的影响也更大。就其附加给数据控制者的义务来说,它不仅要求数据控制者提供数据获取与移植的便利,而且要求数据控制者提供高难度的技术支持。而就其他受其影响的权利来说,数据携带权不仅可能会影响数据安全,而且可能打破他人对数据隐私的合理期待。可以想见,当这种附加的义务超过了现实可能性,当受到影响的其他权利过多时,数据携带权就难以上升为一种基本权利。

总之,作为一种权利,数据携带权面临着很大的争议和问题,这种新型权利可能有利于促进用户的数据权益,也可能难以落地或带来新的风险。此外,这种新型权利还可能因为场景不同而面临过宽或过窄运用的困境。如此种种,都表明数据携带权尚未具备成为一种成熟型权利的条件。数据携带权或许更接近于一种理想或目标,并且这种权利也需要在不同的场景中加以限定,以保证这种权利的行使不会侵犯其他合法利益。

三、数据携带权之于市场竞争影响的双面性

关于数据携带权的另一争论关乎它对市场竞争的影响。数据携带权的支持者认为,数据携带权

^① 对于数据携带权与用户评论移植的讨论,See Vikas Kathuria & Jessica C. Lai, User Review Portability: Why and How? <https://ssrn.com/abstract=3203344>, 2018-10-28.

^② See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-10-28.

^③ See Stephan Weiss, Privacy Threat Model for Data Portability in Social Network Applications, 29 International Journal of Information Management, 249-254(2009).

^④ See Facebook - Cambridge Analytica Scandal, https://en.wikipedia.org/wiki/Facebook_-_Cambridge_Analytica_data_scandal, 2018-10-28.

^⑤ See Wesley Hohfeld, Some Fundamental Legal Conceptions as Applied in Legal Reasoning, 23 Yale Law Journal, 16(1913).

可以对抗“锁定效应”，促进市场竞争；而反对者则认为数据携带权虽然可能对抗“锁定效应”，但消除“锁定效应”并不一定符合竞争法原理，甚至可能促发不正当竞争。

支持意见在某些场景下可以成立，尤其是数据携带权可能会对当前的互联网竞争产生一定的促进作用。在互联网竞争中，先行者往往占据优势，网络效应会导致“赢者通吃”，领先一点即会导致大幅领先，^①互联网的这种竞争性质导致大型网络平台与超大型网络平台的出现。用户对于这些平台往往具有很强的依赖性，即使有同类平台或产品出现，用户也常常不会使用后发产品。其中重要的原因之一就在于，用户往往难以将个人数据转移到新的平台或产品上面。网络平台对于个人数据的这种锁定使得后发互联网企业常常难以进行有效的竞争。在这一背景下，如果用户对于个人数据的获取和移植成为一种权利，那么“锁定效应”就有可能被打破，个人数据就可以实现更为有效的流动。

个人数据的自由流通与共享也可能为市场提供数据这一公共基础设施。对于这一点，无论是数据携带权的支持意见还是反对意见都没有提及。但毋庸置疑的是，数据具有很强的公共性价值和流通性价值，很多学者都指出数据流通的重要意义。^②即使是对于个人数据权利最为强调的《一般数据保护条例》，也强调不能限制欧盟内部个人数据的自由流动。^③对于市场的平等竞争和良性竞争而言，如果个人数据能够实现合理地流通和共享，那么数据的公共性价值将能得到最大限度地体现，市场当中的主体都能平等地享受到数据这一公共基础设施所带来的价值。

但支持意见也只能在有限的场景下成立，反对意见所指出的许多理由都具有很强的说服力。首先，正如反对意见所指出的，数据携带权会给中小企业带来更高的合规压力，从而在一定程度上阻碍市场竞争和创新。如上文所述，企业要满足用户对于数据携带权的期待并不容易，编写能够实现数据携带权的“导出—导入”模块，是一个很高的技术要求。对于谷歌、脸谱这些大企业而言，实现此类技术要求可能并非难事。但对于中小企业而言，此类合规要求可能会带来极大的压力。面对数据携带权等新型权利所带来的合规要求，欧洲的中小企业不得不花费更多的费用。从竞争的角度来看，数据携带权所施加的普遍性责任无疑对中小企业更为不利。

其次，就“锁定效应”而言，数据携带权虽然有助于用户更为便利地将数据从大企业迁移到其他小企业或初创企业，但数据携带权也可能促进用户更为便利地将数据从小企业迁移到大企业。例如，当某家小型超市为消费者提供用户卡并通过这种卡收集用户信息而某家大型超市发现这家小型超市对自身形成挑战时，这家大型超市就可能希望吸引这家小型商店的用户，获取这些用户的各类消费信息。如果数据携带权成为一种强制性的要求，那么这家大型超市只要出台优惠政策，规定只要用户提供用户卡数据就可以获得折扣优惠，这家大型超市就可以很容易地获取这些用户的信息。^④由此我们可以发现，数据携带权尽管可能有助于打破数据垄断，但也完全可能加剧数据垄断。

从竞争法的角度进行分析，我们可以发现数据携带权所造成的这种效应与竞争法的一般原理并

^① See Mark A. Lemley & David McGowan, Legal Implications of Network Economic Effects, 86 California Law Review, 483—505 (1998).

^② 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；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；丁晓东：《数据到底属于谁？——从网络爬虫看平台数据权属与数据保护》，《华东政法大学学报》2019年第5期。

^③ 参见《一般数据保护条例》第1条第3款。

^④ See Inge Graef, Martin Husovec & Nadezhda Purtova, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, <https://ssrn.com/abstract=3071875>, 2018—10—16.

不吻合。为了鼓励创新和竞争,竞争法一般不会要求市场中的创新者共享其财产,或者帮助竞争对手轻易获取另一方的财产。^①相反,竞争法一般更为强调对创新者的财产权加以保护,以此来补偿创新者所承受的风险,激励企业进行更多的风险投资。基于此,数据携带权如果上升为一种基本权利,那么这种权利不但可能会对企业的财产性权益造成威胁,而且也可能影响企业在合同法上的权利。

当然,企业是否拥有对数据的财产性权利,这是一个复杂的问题。有研究者主张企业对于数据拥有财产性权利。^②但也有学者指出,当企业数据涉及个人数据时,个人对于自身的数据权利优先于企业,因为个人数据权利是一种人格性权利,不能被让渡于企业。^③还有的学者则指出,当个人数据在平台上对公众开放时,数据就位于公共领域,数据不属于任何人。^④我们这里不必深究企业数据权属问题的细节,只需要指出的是,如果将数据携带权上升为一种具有优先性的基本权利,那么企业不但无法通过财产权框架对其数据资产进行合理保护,而且也无法通过合同法的方式约束用户或另一企业。在数据的财产性属性越来越强的今天,这样一种制度安排至少存在一定的问题。因为即使各国对于数据库的财产性保护或对集合性的数据资产权利存在质疑,^⑤各国的法律也一般会承认双方约定合同的法律效力,通过合同法为企业数据提供保护。^⑥

如果考虑到数据携带权可能会对商业秘密产生影响,那么数据携带权对于竞争的负面影响可能更大。很多企业收集的个人数据是不公开数据,并非平台数据或公开数据。对于此类数据,当其满足一定的要件时,就受到商业秘密的保护。一般认为,商业秘密保护与不正当竞争关系密切,对商业秘密的非法获取常常被认为是一种不正当竞争,对商业秘密的保护也常常通过反不正当竞争法来实现。^⑦如果一个企业可以通过用户数据携带权而轻易获取另一个企业的商业秘密,那么就等于在法律上承认未经对方许可获取商业秘密不属于不正当竞争。这种推论显然不符合人们对商业秘密保护与反不正当竞争的一般认知。

最后,用户黏性的降低与数据流通的加快对于竞争是好是坏,也难以进行简单判断。一方面,互联网的先行者效应、赢者通吃效应、倾覆效应固然会导致数据垄断,数据流通也因此会有利于打破用户黏性,增强市场竞争活力。但另一方面,在网络与信息科技领域,市场中的竞争往往更为激烈,所谓

① 正如美国汉德法官曾指出的:“为了促进竞争,成功的竞争者不应当受到谴责”。See *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 430 (2d Cir. 1945).

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4期。

③ 参见姚佳:《企业数据的利用准则》,《清华法学》2019年第3期。

④ 例如,在“HiQ诉领英案”中,法院认为,一旦平台接入互联网,就意味着平台数据具有公共属性,不为任何私人或企业所有。作为此案HiQ公司的顾问,哈佛大学的劳伦斯·却伯(Laurence Tribe)教授指出,数据与信息的访问权是一种言论自由的权利,受到美国宪法第一修正案的保护。根据这种观点,数据的本质其实是一种言论,而言论的本质就是流通和共享,具有公共属性。See *HiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-16783(2017).

⑤ 简要说来,美国的数据库保护只涉及数据库中原创性汇编的要素,对数据库中的事实部分或不具有原创性汇编的数据库,法律不加以保护。而与美国做法不同的是,欧洲除了对数据库的原创性汇编部分进行保护之外,也为数据库的特殊权利(*sui generis rights*)提供保护。根据这一特殊权利保护的规定,当“创造数据库需要足够的人力、技术和财政资源”时,数据库就受到法律保护。一旦数据库被创造出来,他人就不得使用或复制数据库的全部数据或大部分数据。

⑥ See Miriam Marcowitz-Bitton, *A New Outlook on the Economic Dimension of the Database Protection Debate*, 47 *IDEA: The Journal of Law and Technology*, 158 (2006).

⑦ See Yuval Feldman, *The Behavioral Foundations of Trade Secrets: Tangibility, Authorship, and Legality*, 3 *Journal of Empirical Legal Studies*, 197 (2006).

的“创造性毁灭”往往会接踵而至,虽然一个企业在一段时间占据主导地位,但很快就被另一个企业替代。^① 在这种背景下,网络与科技企业增加自身的用户黏性不一定会妨碍竞争,而削弱用户黏性也不一定就有利于市场的良性竞争。

总之,从竞争效应的角度分析,可以发现数据携带权是一把双刃剑,如果运用得当,那么这种权利有可能在某些场景下促进市场良性竞争;如果运用不当或不加考虑地将其作为一种基本权利对待,那么这种权利非但无法促进竞争,反而还可能会促发短期探底竞争与不正当竞争。

四、数据携带权的中国应用

对数据携带权原理的分析已经表明,数据携带权尚不具备成为一种基本权利的条件,其既可能会促进市场良性竞争,也可能会造成市场的恶性竞争。因此,中国未来的个人信息立法首先不应照搬《一般数据保护条例》中的数据携带权,不应将数据携带权上升为一种具有普遍效力的基本权利。但如同上文的分析所指出的,数据携带权所服务之目的具有很强的正当性。如果在具体场景下应用恰当,那么数据携带权将会为用户提供便利,促进数据的快捷流转和合理使用,还将可能促进市场良性竞争,防止数据的“锁定效应”。因此,将数据携带权视为一种“柔性权利”或追求目标,在具体场景中赋予个体以数据携带权,可以提升用户福利和促进市场与社会的公共利益。这一部分将以中国语境下企业与公共部门的数据问题为例,分析在何种场景下应当赋予个体以数据携带的权利。

1. 企业数据中的数据携带权

在中国语境下,对于企业数据中所包含的个人数据,首先面临的问题是,个人是否可以较为方便快捷地获取个人数据以及相关数据。对于这样一种强化版的“访问权”,本文认为应当将其赋予个体,要求企业在技术可行的情形下赋予个人下载个人数据与相关数据的权利。例如,各类电子公告板系统、博客、云盘和社交媒体应当提供下载选项,而且即使是非个人数据,但如果是由个人所提供,那么也应当允许个人下载。当然,这种下载必须在验证个人身份和保证数据安全的前提下进行,企业所提供的下载选项不应增加个人相关数据被泄露的风险。

其次,对于个人在不同企业之间转移或移植个人数据的权利,本文认为应当慎重,视具体情况而定。对此,我们可以两个典型案例进行分析。

第一个案例是微博与今日头条之间关于用户生成内容是否可以在用户授权前提下被“爬虫”的争议。2017年8月10日,微博发布公告称:“某第三方新闻平台在微博毫不知情、并未授权的情况下直接从微博抓取自媒体账号的内容”,^② 微博这里所称的第三方平台即是今日头条的产品“微头条”,“微头条”通过获取用户的授权而绕开微博的授权,直接利用“爬虫”手段获取用户的微博内容。在这一案例中,对于今日头条的行为是否合法,可以从多个不同角度进行思考,如今日头条是否违反不正当竞争法,是否侵犯微博的知识产权。^③ 但用户是否具有数据携带权,将对案件的性质产生重要影响。

具体来说,如果赋予个人数据携带权,那么今日头条的行为就很可能属于合法行为,因为即使没

^① See Spencer Weber Waller, Antitrust and Social Networking, 90 The North Carolina Law Review, 1800 (2012).

^② 参见汪传鸿:《谁的用户:微博欲诉今日头条非法抓取内容》, <http://finance.sina.com.cn/roll/2017-08-15/doc-ifyixcaw4855222.shtml>, 2018-11-08。

^③ 参见李妙玲、岳庆荣:《我国用户生成内容的版权侵权问题治理模式研究》,《新世纪图书馆》2015年第5期;刘珊、黄琴:《网络用户生成内容版权侵权自治模式的法治化探索》,《中国出版》2018年第12期。

有微博的授权,今日头条也可以根据个人的数据携带权而转移数据。事实上,根据数据携带权的要求,微博反而应当配合今日头条进行数据转移,当今日头条与个人签订排他性数据协议或者限制用户的数据携带权时,此类协议就可能涉嫌违法或无效。相反,如果个人不享有数据携带权,仅仅以合同法或不正当竞争法来看待“用户—微博—今日头条”三者的关系,那么今日头条的行为就存在违法的嫌疑。

对于这一难题,本文的初步判断是,对于具有商业性质的知名认证用户,一般不宜赋予他们以数据携带权,因为这些用户具备与微博等企业进行平等协商的能力,他们甚至常常配备律师和顾问。在这样的背景下,知名认证用户与微博之间的协议应当被视为有效的商业合同。^①并且,对于微博和今日头条而言,知名认证用户所发的内容更具有直接的商业价值或财产属性,根据竞争法的一般原理,一般不应当允许市场竞争主体无偿获取对方的财产。

而对于非知名认证用户的普通用户,应考虑更多赋予他们以数据携带权。原因有三:其一,这些用户并不具备与微博等企业进行平等协商的能力。面对微博的排他性协议,用户个人很难有真实的选择权,用户与微博之间的关系更类似于数据主体与数据控制者之间的关系,需要对数据主体进行赋权和倾斜保护。其二,此类数据属于公开数据,因此即使赋予用户以数据携带权,也不会影响用户的隐私期待。其三,即使赋予用户以数据携带权,也不会导致微博用户的整体迁徙而对微博的数据权利产生整体性的影响。基于这三点理由,本文认为,在技术允许的情形下赋予用户以数据携带权,这符合数据保护的基本原理,数据携带权不仅可以为用户带来更为便捷的体验,而且有利于互联网企业之间进行良性竞争。数据携带权将促使互联网企业不断改善自身的产品设计,以产品设计来留住普通用户。^②

第二个案例是2019年初爆发并引起社会极大关注的字节跳动公司所属的抖音、多闪与腾讯公司所属产品微信之间的数据争议。在这次争议中,腾讯公司指责抖音违反诚信原则超范围和违规使用来源于微信等软件上的用户头像、昵称等数据,并擅自将腾讯公司提供给抖音的微信账号授权登录服务提供给多闪使用。^③而字节跳动公司则反过来指责微信关闭对抖音与多闪的“开放平台”接口,并且指出“用户的头像、昵称的权益理应归属于用户。不是腾讯授权我们使用用户的头像、昵称,而是用户授权我们使用他们的头像昵称”。^④对于这个案例,如何理解与运用数据携带权,无疑会对处理结果的走向产生重要影响。

从用户的数据权利出发,个人无疑拥有对头像、昵称的控制权,而且在不同平台之间转移头像与昵称,这从技术上并不难实现,成本也接近于零。从这个角度讲,字节跳动公司的声明完全正确,用户

^① 例外情形是具有公益性的个人数据或用户生产内容,如知名认证用户发的公益广告或公益信息,对于此类信息应当允许数据携带权的充分行使,以促进此类信息的流通和共享。

^② 相较而言,平台对于知名认证用户的争夺常常通过支付高额报酬的方式进行。

^③ 以上为第一点指控,腾讯公司还提出其他三点指控:“2.抖音违反开放平台用户协议、商业道德以及相关法律,将来源于微信/QQ开放平台的微信/QQ头像、昵称等数据提供给多闪使用。3.更为严重的是,在用户仅注册了抖音、未注册多闪的情况下,多闪仍然非法从抖音获取了用户的微信/QQ头像和昵称。4.我们认为,用户个人信息的获取和使用必须遵循‘合法、正当、必要’原则和三重授权原则。抖音和多闪的上述行为,严重侵犯了开放平台共享数据的安全,更直接侵犯了用户合法权益。”参见《多闪称被禁用微信/QQ头像昵称,腾讯:偷换概念的无稽之谈》,http://www.sohu.com/a/302422680_561670,2019-04-03。

^④ 参见《多闪发声声明:不认同腾讯主张,昵称、头像相关权益应归属用户》,http://m.sohu.com/a/302808039_118792,2019-04-03。

头像与昵称并不属于某个公司。甚至可以说,用户头像与昵称不属于任何人,如果此类头像与昵称可以通过公共途径获取的话,那么用户头像与昵称就成为公共数据,任何人都可以获取。

但在此案中,较为复杂的是用户头像与昵称背后的数据。双方的争议虽然开始聚焦于用户头像与昵称,但深究之下,其实双方在乎的都是用户的关系链数据:哪个用户与哪个用户是朋友或可能是朋友。腾讯公司介意的是此类数据被字节跳动公司获取,而字节跳动公司想要获取的也正是此类数据。孤零零的用户头像与昵称,其实对双方企业都没有实质性意义。

从关系链数据出发,可以发现赋予用户头像、昵称以数据携带权,首先会面临前文所提到的隐私期待问题。当用户将自己的头像与昵称从微信转移到字节跳动旗下的抖音与多闪时,字节跳动公司就可能利用自身的算法与相关技术来推算用户之间的关系,并且向用户推荐可能认识的好友。因此,这里有必要考虑隐私期待问题,即一个理性用户在此类场景下的合理隐私期待是否会面临严重威胁。就这一点来说,我们可以再次看到积极性的数据携带权与相对消极的隐私期待之间的张力。

此外,在此案中赋予用户以数据携带权,也需要考虑商业秘密保护。对于社交平台企业而言,关系链数据是企业的核心资产,具有重要的商业价值,而且属于企业采取技术与措施进行重点保护的数据完全符合商业秘密的条件。因此,赋予用户以数据携带权,不应当影响企业对商业秘密的保护,尤其不应当影响企业在合作关系中通过合同法对商业秘密的保护。

综上,我国的数据携带权应当按如下方式应用:首先,在技术可行与成本较低的情形下,企业应当满足个人下载其数据与实现数据移转的愿望。其次,数据携带权应当考虑隐私期待或企业的商业秘密等合法数据权益。在不涉及其他用户隐私期待与企业合法权益的前提下,企业与平台就应当努力落实数据携带权;但在影响用户隐私期待或企业合法权益保护的情形下,对这一权利的运用就应当保持谨慎。

2. 公共数据中的数据携带权

对于公共部门所收集和储存的个人数据,我国对数据携带权的运用应该更为积极。对于这一点,本文的判断与《一般数据保护条例》刚好相反。关于个人对公共部门的数据携带权,《一般数据保护条例》第20条第3款进行了限定性规定:“对于控制者为了公共利益,或者为了行使其被授权的官方权威而进行的必要处理,这种权利不适用”。这一规定意味着,当对个人数据的处理是为了法律需要或者为了公共利益需要时,个人将无法行使数据携带权。

对于这样一种限定,《一般数据保护条例》“重述”或第29工作组发布的指南没有给出过多的解释,而仅仅声称这是“其本身的性质”决定的。或许欧盟认为,数据携带权所附加的责任过重,当数据收集者或控制者为了合规需要或为了履行公共职责时,就不应对其再附加责任。^①

如果将数据携带权视为一种刚性的权利,那么本文同意《一般数据保护条例》对于数据携带权在公共部门领域的豁免。但如果将数据携带权仅视为一种“柔性权利”或追求的目标,那么数据携带权将可以促进我国政府和事业单位打破部门藩篱,消除“数据孤岛”,促进数据的共享与便民化服务。

对于“数据孤岛”给民众带来的困扰,可能很多人都感同身受。无论是入学申请、入职申请还是办理证件,只要与公共部门打交道,就会感受到重复填写各种表单的烦扰。而具体的政府部门和事业单位也常常感到无奈,因为对于数据的收集与核验是其职责所在。造成这种困境的部分原因是,政府部

^① See Guidelines on the Right to Data Portability 2017, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf, 2018-06-18.

门和事业单位之间的数据可携带性非常弱,亟须通过加强不同政府部门与事业单位之间的互操作性来加强公共部门的数据共享能力。

对于这种“数据孤岛”造成的困扰,目前我国政府推行的方案是通过自上而下的改革来解决。例如,浙江的“最多跑一次”改革,就是通过政府强力推动来实现政府内部的各种数据共享,以此来提高政府的办事效率,改善百姓在与政府打交道过程中的体验。^①

本文完全认同自上而下的政府改革与推动,但赋予公民以针对政府部门和事业单位的数据携带权,以自下而上的方式来推动政府改革,也是一条走出“数据孤岛”困境的有效途径。毕竟,很多时候普通百姓对于“数据孤岛”的感受最为深切,最有动力提起申诉。如果能将普通个体的申诉请求与政府自上而下的改革决心结合起来,那么将能够更为有利地消除某些政府部门和事业单位的惰性,促进数据共享更为合理和有效地实现。如果政府能够成立跨部门的层级较高的数据共享联合工作机构,受理个体所提出的合理的数据携带权请求,那么此种联动机制将可能倒逼政府不断进行改革,推动公共数据的共享与个体数据的便携性。在理想的情形下,公民在一个部门所填的申请表,应该可以根据个人的请求而无障碍地移植到另一个部门。如果此种目标能够实现,那么个人数据将变得像“一卡通”那样便于携带,真正造福于民众。

五、结语

作为一种新型权利,数据携带权在欧盟问世后,引起全世界的关注。数据携带权虽然非常值得追求,但也面临争议。综合而言,数据携带权尚未具备成为一种成熟型权利的条件,不应当将被数据携带权上升为类似数据访问权的基本权利,而应当将数据携带权视为一种“柔性权利”或努力目标。对于这样一种目标,不应要求所有的数据控制者都承担无差别的责任。相反,应当根据不同主体与不同场景而要求数据控制者满足个体获取与转移数据的请求;同时,应当预防数据携带权可能带来的不正当竞争与恶性竞争,结合用户与企业的合法权益确定是否以及在何种程度上赋予个体移转个人数据的权利。

在中国语境下借鉴与运用数据携带权,首先要避免在个人信息立法中照搬照抄欧盟的数据携带权规定。我国未来的个人信息保护法应当更多强调场景化保护与数据权利合理预期的进路,通过场景化界定与数据权利合理预期来指导个人信息保护法的制定,确立个人信息权利或个人数据权利的边界。其次,数据携带权的中国应用需要结合具体场景,对企业与公共部门施加不同类型与程度的数据携带权。只有在具体场景中勾勒与确定数据携带权的边界,这一权利才可能真正有利于公民权益与产业发展。

责任编辑 王虹霞

^① 参见《今年浙江要这么干!打破信息孤岛实现数据共享推进“最多跑一次”改革工作要点出炉》, http://huzcx.zjzfw.gov.cn/art/2018/4/16/art_1220331_17373872.html, 2018-11-26。