

可携权在商业数据保护中的失衡与矫治

阙梓冰

(清华大学法学院,北京 海淀 100084)

摘要:就可携权与商业数据保护之间的冲突,既有探讨多秉承企业基于商业投入形成的数据权益应受保护的观念,主张对可携权进行限制。此种模式虽能保护企业数据利益,但无助于发挥可携权旨在降低个人转换平台成本、促进市场竞争的制度功用。可携权保护私益的同时也承载着公共目标。应在公私法协同治理的语境下重新审视可携权的功能定位,并对可携权所涉利益冲突进行再平衡。可携权的公益促进面向决定了可携带的数据范围在特定情况下应有所扩张,私益保护属性则要求对数据接收者进行必要限制从而保护数据控制者的商业利益。应区分用户自主携带数据的行为和大规模数据转移行为,并将数据接收者处理数据的目的限定在特定范围,从而矫治可携权在商业数据保护中的失衡状态。

关键词:个人数据可携权;商业数据保护;公私法协同;三重授权;目的限定

中图分类号:D922.6

文献标识码:A

文章编号:1008-7699(2023)04-0037-09

自欧盟《通用数据保护条例》(以下简称“欧盟 GDPR”)确立个人数据可携权以来,理论界和实务界对如何通过可携权实现数据流通利用较为关注。我国《个人信息保护法》将可携权成文化,但并未明确规定权利的行使条件和客体范围,可携权何以从规范成为现实仍有探索空间。^①作为个人数据权能的组成部分,可携权承载了立法者增强个人对其数据的控制权以及促进市场竞争的重要价值期待,与此同时,权利的不当行使也可能产生诸多消极效应。^②在借鉴国外经验引入可携权规则后,如何立足中国实践对该规则予以细化,是当前迫切需要解决的问题。

一、问题的提出

《个人信息保护法》第 45 条第 3 款规定,个人有权“请求将个人信息转移至其指定的个人信息处理者”,这在规范上确立了个人数据可携权。^②可携权确立的初衷在于增强个人对其数据的控制,以及预防平台垄断行为、维护公平竞争。^②但可携权的行使也给企业商业数据保护带来挑战。

个人数据可携权包含个人数据获取权和个人数据转移权两项权能,分别对应个人与数据控制者、数据控制者与数据接收者之间的利益冲突。就个人与数据控制者而言,若扩张可携权的范围,将增加数据控制者的负担,因为数据控制者必须提供“结构化的、普遍使用的和机器可读的”数据供用户携带;数据控制者与数据接收者之间则存在竞争利益冲突,用户从数据控制者处携带的数据将被数据接收者所获取,数据接收者可以对相应数据进行加工使用,这可能损及数据控制者的竞争利益。

收稿日期:2022-11-28

基金项目:国家社会科学基金重大项目(18ZDA149)

作者简介:阙梓冰(1994—),男,福建三明人,清华大学法学院博士后,法学博士。

^① 2021 年,国家互联网信息办公室发布《网络数据安全条例(征求意见稿)》,该意见稿第 24 条对可携权的行使要件作出了规定,但该条例至今尚未出台。

^② 在逻辑关系上,数据是信息的载体,是信息在符号层的句法呈现,承载个人信息的数据为个人数据。参见申卫星:《数字权利体系再造:迈向隐私、信息与数据的差序格局》,载《政法论坛》2022 年第 3 期,第 96-97 页。需要说明的是,对于个人数据的范围界定仍存争议,本文所称的个人数据,并非归属(结果)意义上的个人数据,而系事实意义上的承载个人信息的个人数据。

既有讨论已经充分认识到可携权对商业数据保护的挑战,并提出了相应协调策略。针对个人与数据控制者之间的冲突,不少意见认为应借鉴欧盟 GDPR 的规定,对可携权的范围进行限定,即可携带的数据不包括衍生数据(推测数据)。^[3]针对数据控制者与数据接收者之间的冲突,既有研究多认为应当对数据接收者的权利进行部分限制,例如应遵守三重授权原则;^[4]数据接收者仅能就接收的数据用于特定用途,不应商业化利用等。^[5]如此既可以方便个人行使可携权,也能够有效保护数据控制者的利益。相反观点认为,不应为了保护商业数据限制可携权的范围,否则相应制度促进数据流通利用的初衷将无法实现。在特定场景下,可携权范围应包括数据控制者处理过的数据,甚至衍生数据。^[1]数据接收者更愿意接收能够满足再利用需要的数据,若限定可携带的数据范围,将使得携带后的数据脱离其基础环境,数据的价值也大打折扣。^①比如,在社交平台场景下,若把个人数据从前后文中单独摘出,个人数据往往就失去了再利用的价值。^[6]

可见,现行规范虽然确立了个人数据可携权,但对于可携权的行使要件、客体范围均未置明文,从而面对可携权行使对企业商业数据保护构成的挑战。本文聚焦可携权对商业数据保护的挑战及应对方案。首先,系统性回顾针对可携权与商业数据保护协调方案的既有文献,梳理出旨在通过限制可携带的数据范围以保护商业数据的模式,分析相应模式的守成与不足;其次,回归可携权的规范意旨,重思可携权所涉的利益关系,并基于公私法协同的理念,在价值层面探讨私益保护与公共目标再平衡;最后,探索应对可携权与商业数据保护挑战的总体思路,从制度设计的角度提出协调二者的具体方案。

二、可携权限制模式:守成与不足

(一)可携权限制模式的提出及其理据

回顾学界关于可携权的讨论,在《个人信息保护法》确立可携权的前后,已有不少文献关注到了可携权对商业数据保护的挑战。自欧盟 GDPR 确立可携权以来,理论界的质疑之声未曾断绝。其中,核心质疑意见认为,若将可携权的客体界定得过于宽泛,将可能减损甚至否定数据控制者享有的数据利益;^[7]将数据传输给数据接收者,还可能侵犯数据控制者的商业秘密或知识产权。^[8]各企业之间甚至可能利用数据可携权抢夺数据,从而加大垄断和不正当竞争风险。^[9]

针对前述质疑,既有观点提出了应对策略,即通过对可携权进行两方面的限制,来保护商业数据。其一,应限制可携权的主动效力,即限制可携权能够携带的数据范围。参考欧盟 GDPR 的规定,可携权的范围应限定为个人主动提供给数据控制者的数据,以及订立、履行合同所必需的数据;不包括经过数据控制者匿名化处理且无法复原的数据以及推测数据。^[10]《网络数据安全条例(征求意见稿)》第 24 条秉承此种观点。其二,应限制可携权的被动抗辩效力,针对企业间的数据获取行为,原则上应遵守脱胎于裁判实践形成的“三重授权”原则,可携权不能成为数据接收者抗辩不当数据获取行为的工具。^[11]论者之所以倾向于采取前述模式,从形式上看是借鉴国外经验,在价值根源上则是出于偏重保护数据控制者合法利益的考量。

首先,在规范层面,比较法上的诸多规范都已关注到可携权与商业数据保护之间的紧张关系,对于二者的平衡,不少规范给予了明确答案。比如,欧盟 GDPR 第 20 条第 1 款将可携权的客体范围限定于基于数据主体同意或为履行合同所必需而收集,且以自动化方式处理的个人数据。这意味着欧盟 GDPR 系通过限制可携权的方式调和二者的冲突。欧盟第 29 条工作组(WP29)发布的《关于 GDPR 下数据可携权的

^① “Porting one’s own data removes that interaction context. In many applications, network effects and interactions are important in the value of the data.” MARTENS B, PARKER G, PETROPOULOS G, et al. Towards efficient information sharing in network markets[J]. Working paper, 2021(12): 24. Available at SSRN: <https://ssrn.com/abstract=3956256>.

解释指南》再次重申可携带的数据不包括衍生数据和推测数据。^① 美国《加州消费者隐私法案》同样采取此种方案。^② 与此同时,欧盟 GDPR 第 20 条第 4 款明确,可携权的行使不得影响他人的权利和自由,这被解读为系回应数据控制者和数据接收者之间的利益冲突问题,即相应权利的行使不得对数据控制者的知识产权和商业秘密构成妨碍。^[12] 在我国,《个人信息安全规范》(GB/T 35273-2020)第 8.6 条将可携权的范围界定为包括个人基本资料、个人身份信息、个人健康生理信息、个人教育工作信息四类,这显示出标准制定者对可携带数据范围的谨慎态度。

其次,在价值层面,对个人和数据接收者进行限制,被视为平衡个人与数据控制者、数据接收者的利益。简言之,可携权虽具有刺激数据流动、促进公平竞争和技术创新的作用,但这些均建立在数据“可以”被再利用的基础上。可携权项下能够携带的数据范围关涉到个人与数据控制者之间的利益平衡,应合理分配双方的权利义务。明确个人可以携带的数据范围包括其主动提供的数据和订立履行合同所必需的数据,能够加强个人对其数据的控制,经过数据控制者算法处理后的数据,已经不属于个人数据。明确不能携带相应数据,能够有效降低数据控制者的负担,平衡个人和数据控制者的利益。另外,经过数据控制者处理过的数据可能已经符合企业商业秘密的保护标准,若允许个人将其转移到数据接收企业,将可能使数据控制者的核心商业秘密被数据接收者反向破解,从而产生相应的商业或法律上的风险。^[13] 相反,限制可携权的范围,要求数据接收者仅能取得特定数据,能够平衡数据控制者和数据接收者的利益。

概括而言,既有文献多认为应通过限制可携权的方式,调和可携权与商业数据保护的冲突。这既是比较法的通常做法,也得到了我国国家标准的确认,而且能够在维护个人和数据接收者利益的同时,避免给数据控制者造成过重负担和不利影响。

(二)可携权限制模式的守成与失衡

前述可携权限制模式在保护商业数据问题上具有守成优势,能够有效缓解我国引入可携权的担忧。但与此同时,此种模式将导致数据接收者能够获取的数据极为有限,可携权的制度功用无法得到良好发挥。

1. 守成:企业商业数据的充分保护

在《个人信息保护法》立法过程中,就是否引入可携权存在诸多争议,不少意见担忧可携权的确立将大幅增加企业的经营成本,导致企业竞争优势的丧失,甚至对我国数字经济的发展造成阻碍。^[8] 而将可携权的范围和效力限定在一定范围内,能够保护企业的合法投入,降低企业对于不正当竞争的担忧。

一方面,此种模式充分肯定了劳动创造价值论。根据洛克的劳动财产理论,付出劳动者应享有劳动产品的财产权,数据控制者通过数据处理行为所取得的利益理应受到财产法的保护。^[14] 同时,在数据的采集和加工过程中,数据控制者需要投入巨大的资金及其他成本,肯定相应权益受法律保护也是出于鼓励其市场积极性的考虑。^[15] 另一方面,此种模式能够充分保护数据控制者的竞争利益。在司法实践中,无论是“新浪与脉脉纠纷案”“腾讯与微播纠纷案”还是“百度与大众点评纠纷案”,关涉数据权益的纠纷主要都发生于企业与企业之间,争议焦点亦在于用户数据的获取问题。司法实践出于保护企业商业数据的需要,确立了“三重授权原则”,要求数据接收者在取得数据控制者的商业数据时,需要获得用户向数据控制者的授权、数据控制者向数据接收者的授权以及用户向数据接收者的授权,秉承三重授权原则的价值本位是维护企业数据竞争利益。^③ 若允许用户通过行使可携权的方式任意携带数据至数据接收者处,数据接收者就完全可以主张此类数据是合法获得的,不构成不正当竞争。因此,只有将可携带的数据范围

^① See Guidelines on the right to data portability | WP 242 rev. 01 (5 April 2017). <https://ec.europa.eu/newsroom/article29/items/611233>, Last visited on Oct. 25, 2022.

^② See California Consumer Privacy Act of 2018, 1798. 140(v), https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5, Last visited on Oct. 25, 2022.

^③ 参见北京知识产权法院(2016)京 73 民终 588 号民事判决书。关于三重授权原则的具体解读,可参见刘辉:《个人数据携带权与企业数据获取“三重授权原则”的冲突与调适》,载《政治与法律》2022 年第 7 期,第 120-121 页。

限制在一定范围内,才能确保与三重授权原则保持一致,从而有效维护企业的竞争利益。

切实保护企业商业数据是确保数据市场健康发展的重要一环,但并非全部,尤其是在“赢者通吃”的互联网市场里,居于领先地位的平台能够利用其数据优势,享受递增的规模收益,进一步蚕食剩余的市场份额。^[16]只有促进数据更好地在市场中流通利用,才能够为新进经营者开辟发展空间,这对于数字经济的长远发展至关重要。

2. 失衡:可携权的功用难以发挥

前述限制可携权的规范设计,虽能够维护企业商业数据,但使得可携权制度的初衷无法有效发挥。可携权的规范目的既包括增强个人对数据的控制,也包括刺激数据流通、鼓励市场竞争。可携权限制模式虽具有部分守成优势,但不足也十分明显,这表现为既不利于个人有效转换平台,也无助于促进市场竞争。

首先,对于个人而言,可携权的制度目的之一在于方便用户在不同的平台间进行快速转换,从而打破“锁定效应”,但若将个人能够携带的数据范围限定为主动提供的数据,很可能无法实现制度初衷。例如,在本地生活平台场景下,个人能携带的数据仅限于主动提供的姓名、联系方式、地区等信息,至于个人的评论数据、偏好数据等,则可能被认定为商业数据而无法携带,而后者往往是个人更为在意的转移对象。此种模式将使得通过行使可携权转移的数据对于个人的意义大幅减损,个人转移平台的意愿也将降低,这无疑将进一步加剧锁定效应,不利于市场竞争。在社交平台场景下,若个人无法直接携带通讯录、聊天记录、照片等数据,则根本无法顺利地在新平台进行社交活动。^①可携权之于打破平台锁定效应的意义也将因此丧失。

其次,对于数据接收者而言,其最希望获得市场价值大的观测数据和衍生数据。此类数据若无法包含在可携带数据的范围内,将使得用户携带的数据欠缺再利用价值,鼓励市场竞争的制度初衷也将无法实法。以社交平台为例,和朋友的互动数据、共享的照片都是最具市场价值的信息。^[17]数据接收方正是期待运用算法等手段对此类数据进行分析,进而通过了解个人数据关系链的模式实现相应的商业目的。^②若将可携权的客体限制为主动提供的数据,个人行使可携权时能够携带的数据极为有限,这无法满足市场主体尤其是数据接收者的需求。^③如此,可携权制度促进市场竞争的初衷将无法彰显。

综上所述,针对可携权的行使对企业商业数据保护构成的挑战,既有方案从比较法镜鉴和价值平衡等角度出发,主张采用可携权限制模式,即将可携权的主动和被动效力限定在一定范围。此种方案虽有助于保护数据控制者的商业利益,但同时也将产生不利于个人有效实现平台转换、无法给数据接收者提供有效数据等负面效应。

三、协同视野下的失衡矫治:强化与制衡

法律对利益关系的关注最终要落实在对主体的关切。前述可携权与商业数据保护的协调策略之所以出现守成有余但功用不足的情况,根源还是在于未能全面把握可携权背后的利益冲突关系,并以一贯之的思路去协调相应冲突。可携权的复杂性在于其背后的利益纠葛并非是双向的、线性的,而是呈现出多维度的网状结构。其中,国家作为公共利益的代表者所发挥的作用不可或缺。直面可携权背后的复杂利益关系,并区分不同场景下的调和路径,能够在发挥可携权制度功能的同时,避免损及其他利益。

^① 在国外实践中,ProgrammableWeb网站的专家成功下载了Facebook的诸多个人数据,但因缺乏“前后文”的信息,使得个人在新平台上根本无法找到好友。See MARTENS B, PARKER G, PETROPOULOS G, et al. Towards efficient information sharing in network markets [J]. Working paper, 2021(12): 24. Available at SSRN; <https://ssrn.com/abstract=3956256>.

^② 在通讯录数据背后,映射的是社会关系资本,包含着巨大的商业利益。参见包晓丽、熊丙万:《通讯录数据中的社会关系资本——数据要素产权配置的研究范式》,载《中国法律评论》2020年第2期,第149页。

^③ 转移的数据容易脱离既有的价值网络,从而无法确保同样的数据在另一个竞争性平台上获得原有价值。参见胡凌:《功能视角下个人信息的公共性及其实现》,载《法制与社会发展》2021年第5期,第186页。

(一)可携权所涉利益关系的再衡量

1. 可携权的功能定位:从私益保护到公私法协同

回顾前述针对可携权与商业数据保护协调方案的讨论,不难发现,论者所预设的利益冲突均局限在私主体之间,即主要精力在于分析个人与数据控制者、数据控制者与数据接收者之间的利益关系。在个人、数据控制者、数据接收者之间的私益保护冲突背景下,对于一方的偏重保护意味着对另一方的限制,可携权与商业数据保护呈现非此即彼的关系。也正是在此种预设下,相应方案的选择成为单纯的优劣比较或价值取舍。基于可携权潜在的增加数据控制者负担、纵容不正当竞争的负面效应,论者多在选择上偏向商业数据保护,由此形成可携权限制模式。

前述论断实质上是可将携权作为一种旨在保护私主体利益的制度,但这并不能完整呈现可携权的全貌。作为个人数据权益的组成部分,可携权不仅具有私益保护功能,还具有公益促进面向。个人信息保护的整体制度呈现出公私法融合特征,无论是法律渊源、调整关系、保护群体、保护法益以及损害赔偿、违约救济等部分,都采取了公私法协同模式,个人信息保护法不仅保护个体的自主利益,同时也承载着促进创新等公共职能。^[18]

可携权作为《个人信息保护法》确立的个人信息权益,具有公私法融合的特征。立法者在已经认识到可携权潜在的负面作用的情形下,仍确立了可携权制度,不仅是为了体现自然人对其个人数据的支配性、方便个人转换平台,更是为了“打破数据领域的垄断问题,激励行业竞争和技术创新”。^[19]立法者的这一期待与私益保护并不直接相关,更多体现的是促进公共利益的面向。正如有的学者所概括的那样,可携权是一种策略性的规制工具,秉承反垄断、促进竞争的理念,发挥鼓励技术创新和促进产业发展的作用。^[5]

若仅集中精力于形式化方案的推演和优劣比较,难免会忽视甚至遗忘制度背后的功能预设,以至于得出的结论明显背离人们对相应规则的功能期待。^[20]可携权制度的功能预设与知情同意权、查阅复制权、更正删除权并不完全相同,相较于后者所表现出的私益保护面向,前者更多地表现出推动数据流通利用、促进市场竞争、打破数据垄断进而提升社会福祉的公共功能。因此,其他利益在与可携权发生冲突时,相应的利益衡量都应置于公私法协同的场景下进行考察。在公私法协同视野下,个人、数据控制者、数据接收者的利益需要与技术创新和产业发展等公益目标之间进行“再平衡”。

2. 公私法协同下的利益冲突再衡量

在公私法协同视角下,可携权所承载的公益目标,需要通过扩张可携带的数据范围予以实现。因为只有最大程度保障个人将有价值的数​​据携带至数据接收者,才可以更好地释放数据所蕴含的经济效益,并预防和打破平台经济主导下的数据垄断行为,促进商业数据的高效流通利用。^[21]

数据控制者和数据接收者的算法模型、所积累的其他数据资源均有所差异,故而针对相同数据的挖掘可能会产生不同的经济效益。商业数据只有经过反复利用、与不同数据进行关联聚合,才能更好地释放所蕴涵的社会经济价值。商业数据不断地被利用与分享,有助于提高资源利用效率,减少收集信息的重复劳动,进而促进社会共同福祉的提升。^[14]正是在此种数据高效流通的背景下,数据企业想要取得竞争优势,必须不断优化其算法和算力,从而与其他企业良性竞争,如此,才能最终实现惠及社会大众的整体目的。我国司法实践也充分证实了此点。在前锦诉逸橙案中,法院认为数据接收者经由个人授权(获取用户在数据控制者处的账号密码),从数据控制者处迁移数据的行为不构成不正当竞争,因为“将该行为放置在反不正当竞争法促进市场经济健康发展,鼓励和保护公平竞争,保护竞争者和消费者合法权益的立法目的下”,相应行为属于创新行为。^①可见,如果数据转移行为整体有利于公益目标的实现,此时

^① 参见前锦网络信息技术(上海)有限公司与上海逸橙信息科技有限公司其他不正当竞争纠纷案,上海知识产权法院(2019)沪73民终263号民事判决书。

数据控制者仅以可能损害其利益为由的主张,就无法得到法院的支持。

可携权协同维护公私法利益的本质,决定了其在促进公益的同时,不能置私主体利益尤其是数据控制者利益于不顾。某项行为即便在整体层面有助于公共福祉的提升,也不必然就具有正当性。法律规范在鼓励“做大蛋糕”的同时,也应注重私主体之间的分配正义,即兼顾个人、数据控制者和数据接收者的利益诉求。可携权在发挥公益促进功能时,可能损及数据控制者的利益,故有必要对个人能够携带的数据范围以及数据接收者处理行为予以必要的限制。第一,应划定个人可携带数据的负面清单,对于涉及企业核心商业秘密、企业具有知识产权的数据,不属于可以携带的数据。^[22]即便此种携带有助于社会整体利益的提升,企业的商业秘密和知识产权保护属于法律所倾斜保护的利益,对于立法者作出的此种判断,裁判者应予以尊重。第二,应明确数据接收者接收数据行为的底线,对于非基于个人自主意志的数据转移行为,原则上仍应予以否定评价。第三,应引入目的限定原则对数据接收者的行为进行限制。目的限定原则是对《个人信息保护法》第6条的发展,要求数据接收者的处理行为应当与原平台处理的目的保持一致,这主要是对数据接收者起到规制作用,以避免损害数据控制者的竞争利益。

在公私法协同视野下,可携权需要充分发挥维护市场竞争秩序以及促进数据经济发展等宏观目标,故而扩张数据可携权的范围诚有必要,但此种扩张应当与可携权的制度功能相一致。与此同时,数据控制者的核心竞争利益也应得到维护,在扩张可携带的数据范围的情况下,应明确不可携带数据的类型,并以目的限定原则限制数据接收者对数据的处理,从而解决不正当竞争的隐忧。由此,可携权与商业数据保护的协调开始具有较为清晰明确的思路,具体可以从强化个人数据可携权和制衡数据接收者处理行为两方面展开。

(二)商业数据携带缺憾的补强

个人主动提供的数据属于可携权的客体,并无争议。类似的,匿名化且无法复原的数据不属于个人数据,自然无法携带。有疑义的是观测数据和衍生数据能否携带。在私益保护模式下,基于商业数据保护的需要,观测数据和衍生数据往往都不应纳入可携带的数据范围,因为这些数据在收集和整合过程中,更多体现的是企业的技术和财力优势,故相应数据不再属于个人数据的范畴。^①此种结论在纯粹私益冲突的场合并无问题,例如,当数据控制者和数据接收者均为普通平台时,并不存在反垄断等公益目标,从利益衡量的角度出发,此时应当偏重保护企业的商业数据,但在涉及公共利益场合,应当以公私法协同思维考虑相应问题。在特定情境下,可携带的数据范围应当包括观测数据。相应场景表现为观测数据构成新进数据处理者的必要基础设施,而新进数据处理者又无法以合理的价格或条件获得的情形。^[23]具言之,数据企业的竞争优势取得需要靠数据资源的积累,也依赖于通过算法等技术对数据资源进行加工、整合与分析。用以加工、整合与分析的原始数据是企业竞争优势的基础,通过算法等技术进行挖掘分析后产生的衍生数据或者数据产品方是企业竞争优势的核心。面对相同的原始数据,不同的算法技术可能得出迥异的结论。观测数据作为价值较大的数据,往往可能成为新进数据处理者必不可少的基础设施,相应数据的自由流动是打破数据垄断、促进市场竞争的关键。也正是在意识到数据资源可能自由流通过后,企业方才更有动力更新自身的技术,这正是可携权制度所希望描绘出的市场图景。对于衍生数据,数据控制者于其中投入了更多的财力,且此类数据还可能蕴含数据控制者开发的算法等核心商业秘密,故其原则上不应当纳入可携权的客体范围,否则将给数据控制者的利益造成较大损害。但也有例外,当衍生数据成为新进企业的必要设施,且相应数据落入《反垄断法》的规制范围时,才可以例外地以对优势企业科以衍生数据的移转义务。

前述例外情况仅适用于作为“守门人”的大型互联网平台。大型互联网平台依照《个人信息保护法》

^① 对此也有反对意见,比如费泽就主张对个人行为作广义解释,无论是个人主动生成的数据,还是被动记录的数据,如由机器生成或自动化的反映数据(Reflexive Daten),均属于个人行为生成数据。Vgl. Karl-Heinz Fezer, Digitales Dateneigentum-ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft, S. 112.

应当履行“个人信息守门人”的义务,同时也属于反垄断法的重点规制对象,平台对于可携权的行使应当进行更大程度的配合。在比较法上,欧洲《数据市场法》对大型互联网平台赋予了可携带的强制性义务,要求其免费为商业用户或商业用户授权的第三方提供有效、高质量的聚合或非聚合数据,以确保用户能够实时、持续地进行访问和使用。在美国相关法案里,具有支配地位的大型平台(covered platform)也被科以强制性的数据转移义务,这同样体现出鲜明的反垄断倾向。例如,美国参议院通过的《美国创新与选择在线法案》禁止平台通过协议或技术限制的方式阻止商业用户将其数据移植到其他系统或应用程序;^①美国众议院通过的《2021 服务交换法案》则要求大型平台应维持数据的“可携带性”,确保数据能够符合议案规定的标准结构化、常用和机器可读的格式,经用户明示同意后,按用户指示向其他平台企业安全传输数据。^②法案提出的背景是,谷歌、亚马逊、Facebook 等大型互联网平台利用自身软硬件与网络基础设施,拒绝或限制竞争企业或存在潜在竞争关系的企业与其互联互通,同时通过协议或技术手段阻碍用户数据转移。相应法案的提出,正是为了打破大型平台的垄断,促进市场竞争。

此外,对于商业数据的携带,也应考虑建立合理的收费补偿机制。这是因为,数据处理者对于个人数据的处理付出了劳动,也投入了大量资金,建立收费补偿机制同样是在强化可携权的基础上平衡数据控制者与数据接收者的重要途径。^[24]

(三)不正当竞争隐忧的化解

可携权制度的初衷是鼓励竞争,而非纵容不正当竞争,故在对可携权进行强化后,对于企业担忧的不正当竞争问题,也应设置相应的机制予以化解。具体包括两个方面,一是应对用户的自主转移行为与数据接收者引导的转移行为分别进行规制,二是应要求数据接收者恪守目的限定原则。

首先,应区分数据转移的原因是用户行使可携权的自主转移,还是在数据接收者的不当引导下进行的大规模数据迁移,后者仍属于不正当竞争行为。从数据的价值创造过程看,单一用户的数据、集成大量用户的大数据和基于大数据开发的衍生数据(数据产品)价值逐渐递增。单一用户的数据相较于孤立的个别数据具有更大的资源性价值,无论是浏览记录、聊天记录、邮件内容,都能够被新平台用以对用户喜好进行深度分析进而提供更好的服务;大量用户的大数据还可以被用于挖掘用户群体的偏好信息,以及用户之间的关联关系,从而进行流量变现和产品开发;基于大数据开发的衍生数据和数据产品则是平台取得经营优势的核心竞争力。比如,社交平台取得文字、图片、视频等数据后,通过加工可以分析出不同用户的行为习惯与消费偏好之间潜在关联的新数据,进而用以辅助商业决策、精准营销等。^[25]数据价值的演进过程决定了大量用户的大数据和数据产品承载了数据控制者的核心竞争利益,在强化可携权效力时应当对此有所回应。为了避免以可携权为由进行的大数据爬取行为,需要区分用户自主的转移行为和数据接收方组织或引导用户批量转移数据的行为,前者符合制度目的,后者具有明显的不正当竞争色彩。司法实践在一定程度上证实了此点,在腾讯与搜道网络等不正当竞争纠纷案,被告运用其开发的“聚客通群控软件”大规模收集用户聊天记录等数据,虽其抗辩称系用户授权,但正如法院指出的那样,数据资源的整体与单一原始数据个体享有不同的数据权益,整体爬取的方式对腾讯公司基于数据资源整体获得的竞争权益构成了实质性损害。^③

其次,数据接收者处理所接收的数据时,应遵循目的限定原则,从而控制不正当竞争风险。在扩张可携权范围的同时,目的限定原则要求数据接收者的处理行为应当与原平台处理的目的保持一致,这主要

^① See S. 2992-American Innovation and Choice Online Act, <https://www.congress.gov/bill/117th-congress/senate-bill/2992/text>, Last visited on Oct. 28, 2022.

^② See US House of Representatives: Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, <https://laweconcenter.org/wp-content/uploads/2021/06/Augmenting-Compatibility-and-Competition-by-Enabling-Service-Switching-Act.pdf>, Last visited on Oct. 28, 2022.

^③ 参见深圳市腾讯计算机系统有限公司等与浙江搜道网络技术有限公司、杭州聚客通科技有限公司不正当竞争纠纷案,杭州铁路运输法院(2019)浙8601民初1987号民事判决书。

是对数据接收者起到规制作用,从而避免损害数据控制者的竞争利益。目的限定原则主要适用于社交平台的数据携带场合,在社交平台中,个人行使可携权可能携带大量涉他数据,在原平台里,数据控制者处理相应数据系取得了个人和涉他数据中的第三人的同意。对于数据接收者而言,相应数据的携带系个人完成,数据接收者处理数据的权限也应仅限于特定目的范围内,也即数据接收者对于数据的使用权限无法超过原平台。^[26]例如,在平台之间转移通讯录数据,接收方需基于相同的处理目的处理该数据,即仅供信息主体使用联系地址和方式,便利个人重新找到好友。数据接收者不得对涉及第三人的数据进行超目的处理,如用于挖掘用户与第三人之间的社交关系,向第三人进行精准营销等,除非数据接收者额外取得了用户和第三人的同意。

综上,可携权不仅是私益保护制度,同时也承载着反垄断、促进市场竞争的公共功能,有必要在公私法协同治理的语境下,厘清可携权所涉的利益关系,并将私法利益与公益目标之间进行再平衡。可携权所承载的公共职能决定了个人能够携带的数据范围应有所扩张,应严格遵守可携权的制度目的,并区分一般平台与大型平台予以适用。在扩张可携权的同时,有必要设置配套制度保护企业的合法利益,包括应区分用户自主携带数据的行为和大规模数据转移行为,明确后者仍属于不正当竞争行为;引入目的限定原则对数据接收者的处理行为予以限制,从而有效矫治可携权在商业数据保护中的失衡景象。

四、结论

推动商业数据共享与再利用,个人数据可携权于其中扮演重要角色。既有讨论多从企业商业数据保护的立场出发,认为应对可携权的主动和被动效力进行限制,此种模式有助于守成保护企业的合法利益,但不利于实现立法者的制度初衷,可携权在商业数据保护中呈现失衡景象。究其原因,是对于可携权的功能定位未能厘清,致使对于利益冲突的讨论被局限于私益保护层面。可携权作为一项规制市场的工具,其承载的规范意图不仅在于增强个人对其数据的控制,还在于通过私人权利的行使实现促进数据流通和市场竞争的公共目的。此种目的决定了在特定情境下应当对可携权进行强化,部分商业数据也属于可携带的数据范围。与此同时,数据控制者的利益保护也不可偏废,应区分用户自主携带数据的行为和大规模转移数据的行为,后者仍构成不正当竞争,此外还应引入目的限定原则对数据接收者的数据处理行为进行限制,以保障公平合理的市场竞争秩序。

参考文献:

- [1] 王锡锌. 个人信息可携权与数据治理的分配正义[J]. 环球法律评论, 2021(6): 5-22.
- [2] 杨合庆. 《中华人民共和国个人信息保护法》释义[M]. 北京: 法律出版社, 2022: 115.
- [3] 金耀. 数据可携权的法律构造与本土构建[J]. 法律科学, 2021(4): 109.
- [4] 刘辉. 个人数据携带权与企业数据获取“三重授权原则”的冲突与调适[J]. 政治与法律, 2022(7): 117-118.
- [5] 邢会强. 论数据可携权在我国的引入——以开放银行为视角[J]. 政法论丛, 2020(2): 23.
- [6] 胡凌. 功能视角下个人信息的公共性及其实现[J]. 法制与社会发展, 2021(5): 186.
- [7] 卓力雄. 数据携带权: 基本概念, 问题与中国应对[J]. 行政法学研究, 2019(6): 129-144.
- [8] 张浩然. 用户数据携带权益保障的制度路径[J]. 知识产权, 2022(7): 54.
- [9] 京东法律研究院. 欧盟数据宪章:《一般数据保护条例》GDPR 评述及实务指引[M]. 北京, 法律出版社, 2018: 93.
- [10] 郭江兰. 数据可携带权保护范式的分殊与中国方案[J]. 北方法学, 2022(5): 85.
- [11] 丁晓东. 论数据携带权的属性、影响与中国应用[J]. 法商研究, 2020(1): 84.
- [12] 朱真真. 数据可携权与知识产权的冲突与协调[J]. 科技与法律(中英文), 2022(5): 99-100.
- [13] 杜小奇. 个人信息可携带权的立法检视与适用展开[J]. 河北法学, 2022(6): 178-179.
- [14] 冯晓青. 知识产权视野下商业数据保护研究[J]. 比较法研究, 2022(5): 31-45.
- [15] 申卫星. 论数据用益权[J]. 中国社会科学, 2020(11): 128.

- [16] 李伯轩. 数据携带权的反垄断效用:机理、反思与策略[J]. 社会科学, 2021(12): 109.
- [17] 汪庆华. 数据可携带权的权利结构、法律效果与中国化[J]. 中国法律评论, 2021(3): 196.
- [18] 丁晓东. 个人信息公私法融合保护的多维解读[J]. 法治研究, 2022(5): 14-25.
- [19] 程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021: 344.
- [20] 熊丙万. 法律的形式与功能——以“知假买假”案为分析范例[J]. 中外法学, 2017(2): 321.
- [21] 向秦. 三重授权原则在个人信息处理中的限制适用[J]. 法商研究, 2022(5): 144.
- [22] 崔聪聪, 刘传新. 数据可携带权的法理逻辑和制度构建[J]. 重庆邮电大学学报(社会科学版), 2022(6): 70.
- [23] 付新华. 数据可携的双重路径探析——以个人数据保护法与竞争法为核心[J]. 河南大学学报(社会科学版), 2019(5): 67.
- [24] 包晓丽, 熊丙万. 通讯录数据中的社会关系资本——数据要素产权配置的研究范式[J]. 中国法律评论, 2020(2): 167.
- [25] 沈健州. 数据财产的权利架构与规则展开[J]. 中国法学, 2022(4): 99.
- [26] 孙跃元. 数据可携权权利客体研究:结构、效果与中国化[J]. 河南财经政法大学学报, 2022(3): 88.

Weakness and Correction of the Right to Portability in Commercial Data Protection

QUE Zibing

(School of Law, Tsinghua University, Beijing 100084, China)

Abstract: As regards to the conflicts between the right to portability and the protection of commercial data, most of the discussions have drawn the conclusion that the data generated by enterprises based on commercial inputs should be protected as a priority, and the right to portability needs to be restricted. Although this model can protect the interests of enterprises' data in a conservative manner, it is not conducive to the institutional function of the right to portability, which aims to reduce the cost of transferring platforms for individuals and promote market competition. The right to portability, as a private interest protection system, also carries public objectives. It is important to re-examine the function of the right to portability in the context of public-private law governance and to rebalance the conflicting interests involved in the right to portability. In terms of public interest promotion, the scope of data that can be transmitted should be expanded under certain circumstances, while in terms of private interest protection, the commercial interests of the data controller should be protected by imposing necessary restrictions on the recipient of the data. The weakness in the commercial data protection of the right to portability should be effectively remedied by distinguishing between the autonomous data transmitting by users and the mass data transmitting, and by limiting the purpose of data processing of recipients to a specific scope.

Key words: right to personal data portability; commercial data protection; public-private law synergy; three-fold authorization; purpose limitation

(责任编辑:董兴佩)