数据与个人信息法治专题

文章编号:1008-4355(2023)05-0105-17

数据要素的权利界定与制度保障:基于效率的法律激励

谷 川

(北京市水务综合执法总队,北京 100036)

摘 要:从数字私人领域的外部激励需求入手,引申出数据要素法律界权的必要性。在数据供给与处理环节,个人数据的权利应赋予用户,数据处理者收集或使用个人数据,应以事先告知并取得用户个人同意为原则。在此基础上,作为数据处理者的平台企业与第三方数据运营者就平台内数据的利益分配,应满足前者的数据收益和安全保障需求,后者在访问、收集或使用平台内数据时应给予合理补偿。在数据流通环节,针对数据交易的经验类型,通过自愿交易、强制交易、管制交易以及禁止交易等四种基本制度安排,增进法律界权后的数据权利在交易过程中的有效保护,提高数据要素在私人领域的优化配置水平,进而奠定数据交易法律秩序的基础。

关键词:数据界权;个人信息;平台企业;数据交易;法律经济学

中图分类号:DF523 **文献标志码**:A

DOI:10.3969/j.issn.1008-4355.2023.05.08 **开放科学(资源服务)标识码(OSID)**:

在数字生产和流通领域,数据要素是指将数据作为开发、利用的对象,并以此获得相关收益或产出的一种新型生产资源。作为数字经济的重要组成部分,数据要素已成为推动互联网时代经济与社会发展的新动力。通常情况下,数字市场的要素配置与正常运行,不仅需要内部参与者[①]在要素供需层面上的交往与互动,而且也往往离不开外部力量的支撑和保障。在此基础上,对数字私人领域的有效公共干预,激励参与者的数据供给、处理[②]和流通等数据行为,对促进数据价值的社会最

收稿日期:2023-03-27

作者简介:谷川(1982),男,北京人,北京市水务综合执法总队工作人员,法学博士。

① 即在数字私人领域,参与数据供给、处理以及交易流通等过程的行为主体。若无其他说明,本文关注的数据参与者主要涉及用户个人、平台企业以及第三方数据运营者。

② 本文所指的数据处理主要涉及两部分内容,一是数据的收集,二是数据的使用。前者是指以处理为目的,对用户数据或其他数据进行的采集;后者是指对收集后的数据进行的开发利用,包括但不限于平台企业以数据预处理为主导的加工处理和以数据挖掘为主导的分析处理(自动化决策),以及相伴随的数据存储、传输、公开、提供或删除等行为。

优化产出有着重要的意义。为此,《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见(2022年12月2日)》指出,要积极探索建立保障权益、合规使用的数据产权制度体系,不断激发数据要素潜能,进一步满足数字市场的发展需求。[①] 在数据权益的制度设计中,以法律为主导的公共干预主要涉及到三个重要环节:一是数据要素权益的边界划分,看对其是否有法律干预的必要,即法律界权与否的"门槛"环节;二是若法律界权确有必要,那么,该如何界权明晰主体对数据要素的利益范围以有效促进数据的价值产出,即法律界权的"事前"安排环节;三是在权益边界划定后,法律该如何保障参与者对数据权利的行使,以避免或减少因数据权利滥用或交易事故所带来的社会成本增加或危害,即法律界权的"事后"保护与救济环节。

以上三个环节关系到数据要素在生产开发与交易流通中的价值产出,有效的法律干预可以进一步激励参与者在数据价值生产与交易环节的产出水平,减少由于技术力量的分布差异或信息不充分等原因,给数字私人领域参与者带来的社会损失或成本增加,并由此增进社会预期福利水平。在此意义上,本文运用法律经济学的分析方法,基于效率考量的视角,围绕数据权益制度设计可能涉及的上述环节进行如下探讨:第一部分从参与者供需关系的视角出发,分析数据界权,特别是数据法律界权在数字私人领域的必要性与可行性;第二部分着重讨论数据要素的权利划定问题,以明晰参与者数据法律权利的范围与边界;第三部分主要关注法律界权后如何对数据权利进行有效的制度保障与救济,才能促使数据要素在流通交易环节的社会产出更具效率;第四部分为结语。

一、为何需要数据的法律界权

在法律经济学的视角上,界权的主要功能在于解决主体之间因对资源的利益分歧或不同主张所带来的社会成本控制问题,其更多的是通过区分权利的"内容"来实现,如道路使用的权利、污染物排放的权利或保护隐私的权利等,而非仅以所有权、知识产权以及债权等权利的"类型"加以体现。在此基础上,本文所谓的数据界权,是指对参与者数据资源的利益范围或边界进行划定的行为,是数据资源在不同主体间的一种利益分配。现代社会,资源利益的界定主体往往以第三方公共权威为主导,且通常表现为立法、行政或司法部门,故也被称为法律界权。当然,除法律界权外,也存在通过传统习惯、惯例或私人合意等非正式机制来划分资源的利益边界或范围,本文将其称为通过社会规范[②]的界权,即仅以私人力量而无需公力救济的方式,就参与者对资源的利益范围或边界予以划定、维护,以及监督的一种界权机制。通常情况下,资源的利益界定往往是交易和流通的前提,不同的界权方案不仅会影响到后续的交易流通,而且资源界权本身也是有代价的。[③]

无论是数据资源的法律界权,还是社会规范界权,总要有一个基本的前提,那就是在数字私人领域,参与者至少要有数据界权的需求。也正因为存在此种需求,才会进一步产生数据界权的供

① 参见《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见(2022年12月2日)》,载中国政府网,https//www.gov.cn/gongbao/centent/2023/content_6736707.htm,2023年3月1日访问。

② 主要通过私人资源来实现对个体行为约束或规训的社会控制机制。See Robert C. Ellickson, *Law and Economics Discovers Social Norms*, 27 The Journal of Legal Studies 537, 537-538 (1998).

③ 其中较为典型的两种成本分别为界权信息成本和界权机会成本,前者涉及资源定界所需的信息代价,比如搜寻成本、评估成本、实施成本以及监督成本等,后者则为不同界权方案选择的机会成本。

给，这是解决数据界权的首要问题。其次，在此环境下既有的社会规范是否能够满足参与者数据界权的需要，在数据界权问题上，法律介入是否有必要？倘若参与者对数据利益存在分歧或争议，但这种分歧或争议能够通过非正式机制或私人规范加以解决，从而满足参与者的不同利益主张或需求，那么，法律的介入就没有必要。通常情况下，无需求也就无供给，法律不介入恰好具有效率。否则，一旦决策者“对促成非正式合作的社会条件缺乏眼力，他们就可能造就一个法律更多但秩序更少的世界”。① 但如果社会规范的界权供给仍不能解决参与者的利益分歧，哪怕是经前者界定后，仍需要公共部门的进一步确认，那实际上就意味着有法律界权和通过法律强制力对界权后的成果加以保障的社会需求。结合上述分析，我们可对数据法律界权的必要性与正当性理由作如下分析：

一方面，从经验上看，参与者对数据资源既有不同的利益主张，也存在相应的利益分歧，且在资源生产与利益交换过程中，往往具有对数据利益范围进行界分的需求。在这一具有“全景敞视”功能的赛博空间中，平台使用者的一举一动都会转化为相应数据并被平台所自动记录②，致使平台主体成为实实在在的数据控制人，在事实上管控着平台内数据的命运。但是否由此就可将平台企业视为当然的数据利益垄断者呢？如果不是，数据资源被收集、使用的前后，谁是相应的利益主体，作为数据主体的用户个人是否也具有相应利益，有什么样的利益，第三方数据运营者可否不经企业同意而访问或使用其平台内数据，等等。这些问题在数据界权之前，均难以得到相对可靠的回应。但无论怎样，归根结底，数据资源特别是经处理后的数据资源，在使用上具有显著的潜在价值增量，其开创了在数字经济环境下的新型生产方式③和经济关系④，故由此才引发了各参与者对数据资源的不同利益主张和分歧。而这些不同的利益主张和分歧，则使各方参与者对数据资源利益范围的界定需求更为迫切。

另一方面，对数据利益存在分歧的情况下，以社会规范为主导的私人规范、技术架构等对数据的利益边界进行划分后，仍不能满足参与者对数据界权的需求，数据利益的分歧和不同主张依旧存在。以经平台企业处理后的数据资源为例，此类数据往往被平台采取相应的技术措施，并通过用户/开发者协议、平台服务使用规则等私人单方规范对该类数据资源的开发、使用等事项进行界定，以划分数据的利益范围。但不少参与者，尤其是作为竞争者的第三方数据运营者仍以各种方式在未经平台主体同意的情况下，访问、获取和使用平台数据，并主张平台不应将这些原本由数据主体供给的数据资源据为己有，应允许被其他数据参与者开发利用，以最大化发挥数据资源的使用价值。然而，这些主张并未得到平台企业的广泛认同，各方对数据资源的利益主张亦未能形成一致，相关分歧仍旧存在。⑤ 由此可见，在涉及多方利益主体的情况下，一方凭借其技术或信息上的显著优势地位，界定自身与相关参与者的数据利益边界，虽可在一定程度上缓解数据界权机制的供给短缺问题，但这些以私人资源为主导的界权方案，往往处于一种不稳定、非均衡性的状态，并促使各方

① ［美］埃里克森：《无需法律的秩序：相邻者如何解决纠纷》，苏力译，中国政法大学出版社 2016 年版，第 304 页。

② 参见林子雨：《大数据技术原理与应用：概念、存储、处理、分析与应用》，人民邮电出版社 2021 年版，第 6 页。

③ 参见胡凌：《“非法兴起”：理解中国互联网演进的一个视角》，载《文化纵横》2016 年第 5 期，第 120-122 页。

④ 参见［英］维克托·迈尔-舍恩伯格、肯尼恩·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛等译，浙江人民出版社 2013 年版，第 158-189 页。

⑤ 相关调研资料，可参见中国信息通信研究院：《数据要素白皮书（2022 年）》，载中国信息通信研究院网站，http://www.caict.ac.cn/kxyj/qwfb/bps/202301/t20230107_413788.htm，2023 年 6 月 10 日访问。

数据参与者在不同程度上寻求更具可持续性且符合自身需求的界权机制,以期有效预防和控制这种不确定状态下的利益风险。

这种需求具体表现在以下两个方面。其一,针对业界频频出现的利用爬取技术未经授权擅自获取或使用平台内的数据行为①,平台企业为了防范收益减损和安全风险,往往在私人预防和控制的同时,积极寻求其他部门的相应救济,期望借助纠纷处理或公断来进一步加强对自身数据利益的保障。其二,面对平台企业利用"使用规范或用户协议"等格式条款或不可变更条款划定各方对数据要素利益边界的情况,处于相对劣势地位的其他数据参与者通常要么接受,要么选择放弃,这会导致大幅减少这些参与者对数据利益主张的议价机会,从而增加企业在数据利益边界划定等事宜上的专断、滥用的可能性。这不仅给其他参与者既有权益的保障带来一定的风险,而且亦影响到对数据资源的创新利用水平,致使相关参与者对此产生质疑或在参与者之间形成利益分歧,同时也会使其积极寻求外部力量的介入,并试图替代这种以技术优势者为主导的单方数据界权机制。

为了满足上述需求并结合既有经验做法,或许作为第三方公共权威的法律部门或机制进行数据界权更为适合。因为在通常情况下,其既与数据参与者无具体的利害关联,又往往会以促进社会总体福利水平的目标来协调参与者间的利益分歧,从而提升公共治理的效益水平。另外,为进一步满足参与者法律界权需求,适当的公共干预亦可寻求更为稳定的数据行为预期,以此达到减少因未来不确定性所带来的社会损失或成本增加的目的。这或许就是制度"为了降低人们互动中的不确定性而存在的"②主要功能体现。故若从可持续发展数字市场的角度来看,相比于无为而治,法律干预下的数据界权或许更能满足数据参与者的需求。经验上的例证恰好支持这一论断。无论是"新浪微博诉脉脉案"③、"百度诉奇虎360案"④,还是"腾讯诉浙江搜道网络案"⑤等,这些以不正当竞争形式呈现出的诸多数据权益纠纷类案件,大致反映出相关参与者对私人界权方案的不确信的担忧,进而导致最终的救济手段往往是由主张数据利益被侵害的一方通过诉讼方式,寻求法律(包括但不限于司法)对自身数据利益的支持。而在实践中,尽管当时存在数据权益界定的立法缺失,但司法机关并未将此类案件拒之门外,而是借以其他法律制度(如反不正当竞争法等)作为相应的替代机制⑥,尝试性地通过个案方式解决相关数据权益的纷争,协调不同参与者就数据要素开发利用与利益保障的关系,促进数字经济的可持续发展。当然,法律介入数据界权并不意味着没有代价,除去日常的公共管理成本外,不同法律干预方案的选择,以及干预的偏差或错误,也会导致数据法律界权净收益水平的下降。故审慎、务实的制度设计与可行性的后果考量亦为数据界权法律干预的必备要件。

① 较为常见的是,第三方数据运营者故意破解或规避技术措施访问平台内数据,或不当利用爬虫等技术手段,获取平台内数据等。相关述评,可参见孙晋等:《数字时代数据抓取类不正当竞争纠纷的司法裁判检视》,载《法律适用》2022年第6期,第112-120页。

② [美]道格拉斯·C. 诺思:《制度、制度变迁与经济绩效》,杭行译,韦森译审,格致出版社等2016年版,第29页。

③ 参见北京知识产权法院(2016)京73民终588号民事判决书。

④ 参见北京市高级人民法院(2017)京民终487号民事判决书。

⑤ 参见杭州铁路运输法院(2019)浙8601民初1987号民事判决书。

⑥ 诸如反不正当竞争法等规则,其主要功能在于维护和保障以竞争为主导的市场结构,通常不是数据权益界定的正式制度安排。

二、法律如何界权:从个人与企业的数据利益定界展开

在数据利用过程中,一方参与者的数据行为可能会在不同程度上对其他参与者的利益产生负面影响或风险。比如,平台对数据进行开发利用,就会给用户个人利益带来潜在风险。较为常见的是,因数据使用不当造成的数据泄露、质量瑕疵,或数据被滥用等状况发生,进而威胁到用户的人身权益和财产利益。相反,如果仅顾及用户的个人福利不受减损,那么平台对数据的利用就会受到不当的约束或限制,而这一约束或限制达到最高水平——禁止平台的数据处理或开发利用活动时,用户的数据利益才可达到绝对安全的状态。但这样一来,数据的利用及其产出,甚至是数字经济就无从谈起。由此可见,数据的"开发利用"与"利益保护"之间存在着此消彼长的关系,一方参与者在行使自身利益过程中,给对方带来的负外部性[①]便具有相互性(reciprocal nature)[②]的特点。故数据法律界权除了要促使数据要素的充分利用,合理保障参与者投入激励之外,也要在数据开发利用中尽量避免或减少参与者对他人利益的负外部性影响,以此达到各方在数据使用中的利益均衡,增进数据效用和社会总体福利水平。

在数据处理或开发利用过程中,可以是否能够单独或结合其他信息识别出特定自然人为标准,将数据分为个人数据和非个人数据。前者是指能够单独或结合其他信息识别出特定自然人的数据,后者则是经处理后已无法识别特定自然人的数据(匿名化数据),或仅为物(自然物和人造物)及其组织的数据。同时,上述数据主要涉及的利益主体大致可分为三类,即用户个人(以下简称"用户")、平台企业和作为第三方的数据运营者。相比而言,后两者是数据开发利用的主导性力量,无论在技术控制还是信息掌控水平上,都比用户个人具有显著的优势地位,故可将后两类参与者看成一个整体来对待,即数据处理者(以下简称"处理者")。大体上,可先探讨用户个人与处理者之间的权利界定问题,然后再关注数据处理者——平台企业与第三方数据运营者之间在数据利用方面的权利分配问题。

(一)用户与处理者在数据上的权利分配

在个人数据相关权利中,事实上存在用户的个人数据权与处理者的数据使用权两个方面的问题。对用户来说,数据处理或利用虽可增进其交易便利化水平,但此类数据所承载的个人利益能否得到保障,则关系到用户自身福利的有效性问题,即数据处理给用户个人带来的收益与损失(成本)的比较。故用户对其数据所享有的利益,大体上就是该数据承载的个人既有利益,其中具有代表性的便是隐私利益,特别是有关特定自然人的身份或个性特征等方面的识别利益,比如:姓名、账户与密码、电话号码、指纹与其他重要生物特征信息、在线浏览行踪、行为倾向或需求偏好等。另外,也涵括隐私之外的其他个人利益,比如个人对其已公开的文本、图片、音频或视频等资料享有的利益;数据内容所承载的主体声誉利益,比如个人的名誉、信用、荣誉以及其他评价利益等。以上利益与

① 通常是指参与者的数据行为给他人(利益相关方)带来的未经其同意的损失或成本增加,这类增加的成本便是数据行为的外部成本。一般而言,数据行为的社会成本由两部分组成:一是参与者的私人成本,比如平台对数据处理、开发利用的成本投入,二是该数据行为给其他参与者带来的不利影响,即外部成本。

② See R. H. Coase, *The Problem of Social Cost*, 3 The Journal of Law and Economics 1, 2 (1960).

主体具有同一性,通常不可分离或分离后给主体带来的潜在危害会显著增加。为方便起见,从权益保护的视角出发,本文暂将用户对其数据的利益称为“个人数据权”。对处理者来说,数据的收集和使用是其生产运营和商业模式的基础,也是数据价值产出和数字经济发展的基本保障。事实上,处理者基于获得此类数据的价值产出而期望享有数据使用权。通常情况下,用户与数据处理者在行使各自权利时,都会产生相应的负外部性影响。就像厂商在生产运营中污染物的排放与居民对清洁环境的需求一样,效率往往要求结合两者的特点,寻求更小的负外部性方案来解决此问题,以促使两者的利益达到均衡状态。具体来说,关键点就是在此类数据能够交易的条件下,将权利赋予用户或处理者哪一方,由此带来的预期社会损失或成本能达到最小化。

为此,大体上可分为两种赋权方案,第一种方案是将数据权利赋予用户,即用户享有个人数据权。通常情况下,非经用户同意,他人不得擅自收集和使用个人数据;或者他人在收集和使用此类数据后,应给予用户相应补偿。第二种方案是将数据权利赋予处理者,即处理者享有数据使用权。一般而言,处理者有权收集和使用个人数据,未经处理者许可,用户不得采取相应预防措施;或者用户可采取相应预防措施,但应给予处理者合理补偿。

结合各自在技术、信息等方面上的能力,很显然,面对在算法技术和信息等方面优势地位显著的处理者,用户难以凭借其自身能力来获取足够的信息并以此进行有效的决策;再加上信息优势者实施潜在“机会主义”的行为(欺诈等)广泛存在①,倘若将权利赋予处理者,其后果则会使原本在技术和信息上的不对称程度继续加大,同时,处理者在不经合意或充分告知等情形下利用个人数据,亦在不同程度上增加了信息优势者在数据使用中的道德风险,进而会造成更多的数据收集或使用事故。相比用户个人来说,由占据更多技术和信息优势的处理者来预防数据利用事故所需的成本往往会更少,故将权利赋予用户不仅可节约预防数据利用事故的成本,而且更有利于数据保护与进一步开发的相对均衡。② 法律关于个人数据权的范围划定,大体与该数据信息所承载的既有个人利益范围相当,内容上包括用户隐私与其他个人利益,其形式则可表现为用户为保障上述利益所具有的知悉真情(参与和被告知)、自主决策(同意与否)、数据访问(查阅使用)、数据修改或删除(便利处置)以及授予第三方数据处理者访问或使用此类数据等具体权利。

(二)平台企业与第三方数据运营者在数据上的权利分配

除用户享有的个人数据权之外,对于平台企业与第三方数据运营者来说,平台内数据(含个人或非个人数据)的权利赋予哪一方,更有利于数据的开发利用与价值产出,进而促进社会总体福利水平的增长,则需要进一步分析。就数据持有者——平台企业来说,其通过投入就数据进行收集、存储以及挖掘分析,对数据集或分析成果的形成与贡献通常是最大的。在持有与控制此类数据的基础上,企业不仅具有相应的收益对价,而且还具有采取相关技术措施对平台及平台内数据进行安

① 较为典型的例证,便是平台企业针对用户使用的“大数据杀熟”等措施,致使用户消费权益的减损。另外,以APP收集使用个人信息为例,相关平台运营者未经用户同意或授权收集使用个人信息、频繁启动弹窗索要授权或无关权限、收集信息超出必要范围以及隐瞒敏感个人信息收集或使用等行为在业内依然普遍、多发。相关述评,参见国家计算机网络应急技术处理协调中心等:《APP违法违规收集使用个人信息监测分析报告(2021年12月)》,载中华人民共和国国家互联网信息办公室网站,http://www.cac.gov.cn/2021-12/09/c_1640647038708751.htm,2023年6月10日访问。

② 这便是成本较小者通常承担事故预防责任的法律经济学原理。相关支持性研究,也可参见桑本谦:《法律简史:人类制度文明的深层逻辑》,生活·读书·新知三联书店2022年版,第79-85页。

全保障的权利。[①] 在此基础上,他人在访问、收集或使用平台数据的过程中,往往不仅需要支付相应对价,还不应给企业的平台运营带来更多安全隐患或成本负担。总的来看,平台企业对其数据享有的事实权利主要包括数据收益权和安全保障权。而对于第三方数据运营者来说,其对数据的期待利益,主要就是对此类数据的访问、收集和使用,并在此基础上,进一步予以开发处理,获得更高的数据价值产出。故暂且可将第三方数据运营者对数据的事实权利大体概括为数据再利用权。[②]

事实上,平台企业与第三方数据运营者在各自行使自身利益的同时,也会产生相应的冲突。比如,平台企业对其内数据的控制和持有,第三方数据运营者往往会面临平台企业在对价上的不合理条件,导致难以达成合理使用平台内数据的协议,进而影响对数据的再次利用机会。而这又与数据的非竞争性[③]相悖,进而制约数据及其创新利用的价值产出。如何协调二者间的利益,也可预设两种方案:

第一种方案是将数据权利赋予平台企业,即企业对其内数据享有收益和安全保障的权利。具体而言,可表现为非经平台企业同意或授权,第三方不得访问、收集或使用平台内数据;或者第三方获取或使用平台内数据的,应当给予平台相应补偿。第二种方案是赋予第三方数据运营者对平台内数据的再利用权,即除非获得第三方数据运营者同意,否则,平台企业针对第三方访问、收集或使用数据所采取的预防措施均被视为侵权;或者平台企业采取上述防范措施的,应当给予第三方数据运营者合理补偿。

前一种方案的优势在于,能够激励平台企业对数据的价值产出,同时也会进一步提高平台企业对其平台内数据控制、管理的安全保障水平,但这里也存在一定的问题。尽管平台企业与第三方数据运营者均属于数据企业,在同等规模条件下,所具备的技术或信息能力大体不存在严重的不对称性,但相比于第三方数据运营者来说,平台企业对其内数据的实际控制以及架构规范的制定权,仍要比第三方数据运营者占据相当的优势地位,而这种优势地位一旦被滥用,就会带来一定的社会危害。比如,过度限制平台数据的合理流动;以安全保障为由,不当限制或制约第三方数据运营者对平台内数据的合理访问或使用,特别是对第三方数据运营者来说,属于"必要设施"的数据资源受到限制或制约;[④]更有甚者,平台会以此排除或限制其他数据企业的合理竞争,形成数字市场中的不正当竞争或垄断,削弱数字市场的资源配置能力,等等。故赋予平台企业数据收益和安全保障权后,如何有效避免或减少平台企业因权利滥用而带来的社会成本,从而降低对第三方数据运营者合理利用数据的限制水平,将成为受关注的主要方面。[⑤]

---

① 典型例证,可参见"抖音短视频抓取案",北京知识产权法院(2021)京 73 民终 1011 号民事判决书。

② 某种程度上,第三方数据运营者在数据的使用上,对数据要素的开发创新亦具有一定贡献。

③ 从现代微观经济学的视角来看,所谓非竞争性(nonrival),一般指的是新增一人对资源的消费,不会减损原主体对资源的消费水平。参见[美]罗伯特·S. 平狄克等:《微观经济学》,李彬译,张军校,中国人民大学出版社 2020 年版,第 564 页。就数据而言,在不考虑其他因素的情况下,同一组数据被不同主体合理开发利用,通常不会减损或有害于用户或数据持有人的利益,也不影响其对数据的再次使用,这与一般私人财产具有的竞争性特质区别较大。

④ See Zachary Abrahamson, *Essential Data*, 124 The Yale Law Journal 867, 867-881 (2014).

⑤ 这方面问题正在得到学界和业界的广泛关注。以平台企业的数据垄断为例,企业(特别是大型数据企业)是否具有数据垄断或独占的需求,对数据的垄断是否有助于其商业模式发展或收益增长,以及对数字市场支配力水平的测度等问题,已成为相关研究的热点之一。相关文献可参见 Marina Lao, *Networks, Access, and "Essential Facilities": From Terminal Railroad to Microsoft*, 62 SMU Law Review 557, 575-586 (2009); D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 Geo. Mason L. Rev. 1129, 1135-1140 (2016).

后一种方案则是将数据的再利用权赋予第三方数据运营者,使平台内的数据原则上成为公共产品。这就意味着第三方数据运营者不仅可以不经平台企业的许可,无偿访问或利用平台内数据,且平台不得阻挠他人访问、收集或使用平台内数据。此方案的优势在于,能够进一步实现数据的非竞争性、非排他性的功能,使数据能够得到更多开发者的利用并产出相应的价值增量,满足不同第三方数据运营者,特别是"寄生性"运营者对数据的开发、利用需求。① 但此种赋权方案也会导致如下问题亟待解决:一是忽视了平台企业对数据的价值创造,也会严重影响平台运营的商业模式效能。这种不付费的开放利用方式,会给第三方数据运营者释放出"搭便车"的信号,进而抑制平台企业对数据的产出水平;二是给平台内的数据安全带来一定隐患。平台企业对平台内数据的持有和控制,一方面是其商业模式运营所必需,以便获取相应的收益作为对价;另一方面也在于保障平台内数据的安全所需。第三方数据运营者在访问或获取平台数据时,可能故意或过失地将有害于数据安全的各种因素带入平台,从而影响到平台内数据的安全,使数据权利主体的预期损失有所扩大。

通过两种赋权方案的对比,可以看出,第一种方案侧重于激励数据生产者的投入,以及平台内数据的安全;第二种方案则更为关注数据的再次利用,开放的数据利用方式降低了第三方数据运营者对平台内数据访问、收集或使用的成本,也在一定程度上促进了数据的跨平台流动。遗憾的是,这两种方案都不够完美,都存在相应的不足。前者在于平台企业"机会主义"行为可能带来的社会成本增加,后者则疏于对数据生产者投入的激励以及平台内数据的安全保障。如果从机会成本的视角对比两种方案,我们会发现,第一种方案的代价主要影响的是数据的再次利用效率以及由此获得的更多预期产出;后一种方案所忽视的最高收益则为对数据生产激励及数据安全保障的进一步激励。

从价值产出过程来看,平台内数据的生产激励与安全保障,是数据得以再次开发利用的基础和前提,甚至可以说是一种派生关系。他人只有在平台企业生成数据(集)后,才可进一步处理或开发。故就数据的初始价值增量来看,一般而言,生产者的贡献要大于对此类数据的利用者。那么通常情况下,按照贡献与利益的正向分配关系,数据生产者的权益往往也要优于数据利用者。否则,如直接赋予数据利用者使用权,除了可能对平台内数据带来更高的安全风险外,数据的生产者还因缺乏足够的激励而呈现低于社会最优产出水平,造成数据产出的短缺,从而提高第三方数据运营者对数据开发利用的成本。在此基础上,第二种方案的机会成本通常要高于第一种赋权方案,故赋予数据生产者——平台企业对此类数据的收益权和安全保障权,或许更能够满足平台内数据开发利用的社会需求。当然,法律也要对此进行必要的限制,以预防平台企业滥用其优势地位,造成数据合理利用或数字市场竞争的阻碍。

(三)小结

综上所述,就个人数据而言,将权利赋予用户,即用户享有个人数据权,则更有利于激发用户的

① 在这种"寄生性"关系中,作为第三方数据运营商的"寄生者",往往是新技术的开发与运用者,其对作为宿主的平台企业之内的数据资源或商业模式,具有一定的依附或依赖关系,并由此形成了"平台内数据保护"与"新技术创新利用"两种利益之间的博弈。相关案例评析,可参见仲春等:《数据不正当竞争纠纷的司法实践与反思》,载《北京航空航天大学学报(社会科学版)》2022年第1期,第25-26页。

数据参与和供给,在保障用户个人权益的基础上,亦能降低因自身所处的技术劣势所带来的高昂预防成本。在此基础上,作为数据处理者的平台企业和第三方数据运营者对平台内数据进行利益分配,赋予平台企业数据收益权与安全保障权,则会进一步促进平台企业与第三方数据运营者之间的利益均衡,提高数据开发利用的潜在效率。

三、界权后的制度保障与救济:数据交易的法律秩序

对数据要素进行法律界权的目标在于避免或减少因数据价值增量产生的利益冲突或分歧,同时亦恰当激励数据生产和投入,以增进社会总体福利水平。因此,就需要提供相应的保障与救济机制,以促进数据要素向更高利用价值的方向流动,助力资源的优化配置。这不仅涉及到数据要素的交易流通问题①,更是关乎数据界权后,法律如何有效保障主体的数据权利问题。需要指出的是,本文所谓的数据交易,主要是指在数字私人领域,平台企业分别与用户、第三方数据运营者之间就数据访问、收集或使用所发生的交易。它既包括参与者间的自愿交易,也包括数据相互间的非自愿交易,比如未经授权访问、收集或使用他人数据,或虽经授权,但在数据访问、收集或使用中因处理不当导致相应损失或成本增加等。在数据交易范围上,它涵括了在数据供给、处理与流通等环节发生的涉及数据收集、存储、挖掘分析或向他人提供等各种以数据处理为目的的活动。对于以数据产品等形式向需求方提供服务的,若需求方不对此类数据进一步处理,则对数据权益主体的潜在负外部性影响较小,故不将其纳入数据交易范畴。

(一)数据交易的经验类型

大体上而言,数据资源的交易与流通是促进数据交换价值产出的重要环节,但在此过程中,也可能产生不同程度的社会成本或危害,以至于会降低数据交易的总体效用水平。那么,如何既能促使数据交易的价值增长,又能够有效地减少因数据交易所带来的社会损失,这就成为数据法律界权后的当务之急。为此,依据数据交易可能对社会产生的不同影响,在经验层面上,可将私人领域中的数据交易划分为以下几类:一是经当事人合意,且通常交易成本较小或产生外部成本不大的数据交易;二是没有合意而与他人发生的数据交易(非自愿数据交易);三是交易前若不进行有效防范,就可能发生更多外部成本的数据交易;四是无论合意与否,通常都会带来重大外部成本或危害的数据交易。

第一类属于当事人意思自治的数据交易,即自愿数据交易。此类交易通过数字市场自主定价,促使数据资源获得较高利用价值,不仅会产生交易的合作剩余②,亦可提升数据资源的利用水平。比如,经公共预防后,平台企业与用户经合意对用户个人数据进行的收集、使用;平台与第三方数据运营者就平台内数据访问或利用达成合作等。第二类主要体现为缺乏当事人间的合意,一般需要借助外部公共力量得以完成的数据交易。鉴于自愿数据交易可能出现的因事前交易成本过高,或

① 若无其他说明,本文将数据交易视为界权后数据流通的主要表现形式,且暂不对数据交易和数据流通进行实质性区分。但也有学者将数据流通的含义仅限定为数据持有人(平台企业)向他人提供数据或使他人接触或使用数据的行为,而忽略原始数据生产者向平台企业(数据集生产者)提供数据的过程。参见高富平:《数据流通理论:数据资源权利配置的基础》,载《中外法学》2019 年第 6 期,第 1416 页。

② 指合作者通过合作得到的纯收益。

难以满足数据利用需求等原因导致的效率损失,作为自愿交易的一种替代机制,有时通过外部公共力量促使数据交易完成或许更具效率。不少情况下,此种交易方式会涉及到公共部门对数据权利的强制性定价,以此促成此类交易的完成。第三类情况主要是针对交易方可能产生的外部成本而言的,即在某些情形下,无论是自愿交易还是非自愿交易,若无事前的有效预防和控制,那么,交易的预期社会成本或危害程度就有上升的趋势,从而加大数据流通的安全隐患。这意味着此类数据交易对相对方或第三方产生损失或成本的风险较高,仅凭交易相对方或第三方自身的预防能力或决策水平,尚难得以减少风险或改善预防成本过于昂贵的情形,故往往需要公共部门的干预,以激励参与者对外部成本的预防和控制。比如,对网络与数据安全、数据处理质量或数据境外提供等领域采取的公共预防措施。相比于前三类数据交易而言,第四类交易所涵括的数据通常会涉及到国家安全、公共利益或重大个人权益等事项,故此类数据的私人交易往往会增加危害社会程度,进而给社会总体预期福利水平带来严重的负面影响。比如,对涉及国家秘密的信息进行交易,或买卖个人信息等。

(二)数据权利保障与救济的一般制度安排

结合上述,针对以上四类常见数据交易行为,法律可设置相应规则保障与救济机制,在保护数据权利的基础上,促进数据正常交易与流通,避免或减少因不当交易或交易事故带来的社会损失、成本增加或危害。①

第一类为自愿交易规则,或意思自治规则。即在数字私人领域中,对于通过交易主体的自愿协商与自主定价,实现合作剩余的数据交易行为,法律予以承认并鼓励的制度安排。具体来说,便是法律要求需求者收集或使用数据前,原则上以取得数据权利人的同意或授权为必要。需要注意的是,此类规则实施的约束性条件,通常是以信息足够充分、交易成本不高等作为外部环境基础。该类规则的经济学原理在于,在满足或大体上满足上述约束条件下,激励参与者通过自主、合意的方式实现交易,更有利于资源在流通环节的边际价值产出。故法律在此种条件下,应当促进不合作转向合作、以损失较小的不合作替代损失较大的不合作,从而最大化地减少参与者合作失败的成本。②

在立法实践中,《中华人民共和国网络安全法》《中华人民共和国数据安全法》以及《中华人民共和国个人信息保护法》对个人信息的保护与利用进行了统一且一般性的制度安排。其中,最为显著的特点之一,便是在符合网络与数据安全的条件下,确立了企业以“告知+同意”方式作为处理或使用个人信息的原则。仅从私人领域的视角看,倘若将信息利用视为数据交易或流通的前提,这也就意味着我国针对参与者就个人信息发生的交易,选择了以意思自治为导向的规则安排。只不过这种意思自治需满足以网络和数据安全等为主导的公共管制要求这一先决条件,其目标或许更多的在于避免或减少因数据利用可能带来的事故或危害。相比而言,美国除联邦层面对征信、金融、

① 该部分内容是以法律经济学中的经典理论——“卡—梅框架”(C&M Framework)以及后续研究者的理论成果为借鉴,结合数据权利的法律保护与救济实践,进行了相应尝试性的改进与创新。相关文献可参见 Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One view of the Cathedral*, 85 Harvard Law Review 1089, 1089-1128 (1972); Lucian A. Bebchuk, *Property Rights and Liability Rules: The Ex Ante View of the Cathedral*, 100 Michigan Law Review 601, 601-639 (2001);凌斌:《法律救济的规则选择:财产规则、责任规则与卡梅框架的法律经济学重构》,载《中国法学》2012年第6期,第5-25页。

② See Robert Cooter, *The Cost of Coase*, 11The Journal of Legal Studies 1, 27-29 (1982).

电信、医疗以及未成年人等易发生隐私滥用或侵害等事故的特殊领域进行个人信息立法保护①,以及相关州出台的消费者隐私保护法案之外,在制定法未涉及的诸多其他领域中,是以信息隐私(information privacy)自治为主导的普通法原则对个人信息权益予以救济保障。这种"特殊领域管制,即一般领域自治"的干预模式,体现了以自愿交易规则作为导向的个人信息利用的制度安排,即以市场交易的模式,促使用户、企业或第三方间以意思自治方式实现个人信息的利用,并以此寻求更多且富有弹性的信息自由流通机制。② 鉴于用户个人在数字市场中处于的交易劣势地位,法律主要侧重于对欺诈或未经(超越)授权等行为的矫正或对消费者保护以及其他增进数据交易公平等事宜的干预,以期避免或减少因参与者间信息或技术的严重不对称性所导致的数据滥用或其他交易事故。结合上述个人信息保护与利用的规则特点可以看出,我国更侧重于以"数据安全"为导向的自愿交易安排,通常强调数据安全与使用的利益平衡。

有悖于自愿交易规则的行为通常表现为需求者在未经数据权利人同意或授权的前提下收集或使用数据,这类行为往往以获取不当收益为目标且积极为此准备、谋划,而这又会增加不当收益获取的可能性,进而加重了此类交易负外部性的预期危害后果。故相应的救济方式原则上可以惩戒为主,比如,在停止侵害的基础上予以惩罚性赔偿,在情节或后果严重时,亦可施加必要的公共制裁,以增强的威慑力,提高非自愿交易的成本③,使边际惩罚成本相当于边际不法收益水平,从而达到降低潜在有害非自愿交易数量的目的。相关司法裁判亦反映出此种趋势。以"微博舆情数据抓取案"为例④,人民法院在审理中认为,被告作为互联网舆情信息服务提供者,为获取高额利润,未经原告及其运营的社交平台内用户的同意或授权,破坏或避开平台技术措施,大量抓取平台内未公开的用户数据,此行为不仅给平台正常运行带来额外负担,影响其交易机会和期待收益,而且还会降低平台对用户数据处理的安全保障水平,导致用户数据安全隐患和风险的不确定性增加,进而减少平台内众多用户的预期福利水平。据此,人民法院认定被告具有明显的主观恶意,并在裁判中适用了惩罚性倾向的赔偿标准。此裁判旨在提高类似不当数据获取行为的违法成本。

第二类为强制交易规则。即法律对行为人未经合意收集或使用他人数据等行为进行强制定价,以此实现数据权利主体的预期收益或弥补损失,并进一步增进交易效率的制度安排。此种制度安排的经济学基础在于:并非所有的自愿交易都是有效率的,比如,过高的议价成本、信息优势方权利的滥用以及严重的不正当竞争等市场失灵现象产生的边际社会成本,大幅降低了自愿交易可能带来的效益水平。由于市场失灵可能引发的社会损失,当法律模拟市场机制并能够确定权利的交易价格,且相比于市场交易成本或市场失灵带来的损失,这种强制定价的成本处于更低水平时,为了有效降低高昂的市场交易成本,强制交易规则通常就会成为自愿交易规则的有效替代机制。

结合数据交易情况来说,该规则大体可分为三类:其一,当行为人未经同意收集或使用数据,且没有给数据权利主体带来其他损失时,可参照市场价格向权利主体补偿其通过市场可获得的预期

① 比如,《公平信用报告法》(FCRA)、《电子通信隐私法》(ECPA)、《计算机欺诈与滥用法》(CAFF)以及《健康保险携带与责任法》(HIPAA),等等。

② 参见高富平等:《论个人数据保护制度的源流——域外立法的历史分析和启示》,载《河南社会科学》2019年第11期,第43页。

③ 有关价格与威慑理论的述评,可参见 Robert Cooter, *Prices and Sanctions*, 84 Columbia Law Review 1523, 1523-1552 (1984).

④ 参见北京市海淀区人民法院(2018)京0108民初28643号民事判决书。该案二审被维持原判。此案系2023年北京知识产权法院发布的涉数据反不正当竞争十大典型案例之一。

收益来完成交易。实际上,此种规则安排的目的主要在于实现数据要素的开放利用,以防范平台企业滥用优势地位导致的数据歧视交易等不正当竞争,或阻碍数据利用创新所带来的社会成本。其二,当行为人未经同意收集或使用数据,或虽经同意收集或使用数据,但因处理不当造成数据安全或质量等事故,给权利主体带来其他损失时,除补偿数据利用的预期收益外,法律通常还要按照"外部成本内部化"的原则,强制行为人赔偿数据权利主体的损失,从而使交易得以完成。其三,在特定情形下,出于公共利益或其他合理事由,强制要求数据参与者之间进行交易,以便实现更大的社会价值。比如,在应对突发公共卫生事件或紧急情况时为保障个人生命健康或财产安全、因订立或履行合同所必需的数据、个人或经他人合理公开的数据,以及在合理范围内的新闻报道、舆论监督等情况下,平台企业可以收集和使用用户个人数据,而无需取得用户同意。另外仍需强调的是,强制交易规则大体以法律的事后消极干预模式[①]为主导,其中,法律的角色往往是被动、消极的,非经当事人的启动不会主动介入,进而相对节省了法律干预数据交易的成本。

第三类为管制交易规则,也可称为经积极干预的交易规则。即为避免或减少数据交易事故可能带来的社会损失,法律预先设置一定的条件或标准,待相关交易主体符合这些条件或标准后,方可进行交易。此类规则较为常见作用于数据交易的行政审查(评估)和各类规制行为。前者表现为公共部门对交易中涉及到的相关数据境外转移、流通等行为的风险评估、审查或许可,如《中华人民共和国个人信息保护法》第36条、第38条涉及的国家网信部门对向境外提供个人信息进行安全评估的规定。后者则是对网络和数据安全、数据处理质量标准或缓解技术/信息的严重不对称性等方面的保护性或预防性的强制干预,如要求平台企业建立健全数据安全预防机制,设定专人或机构负责数据安全保护工作等。必要的管制交易,是为了有效避免或减少数据交易可能给第三方或相对方带来的损失或成本增加,特别是与此有利害关系的社会公众,其往往是作为信息劣势方的参与者,故法律一般会以公共利益或社会利益的名义进行主动、积极干预,以防范技术或信息优势者从事的各种"机会主义"行为所带来的社会危害。而对于违反者,通常给予的救济途径是法律惩戒,且往往以行政处罚为主。

总的来看,管制交易规则体现的是法律的事前积极干预模式,常态化的执法检查与日常监管是此种模式的主要特点。在技术水平保持不变和预算约束的条件下,管制交易规则的范围越广或项目越多,其耗费的公共资源就越多。由此可见,管制交易规则一般限于易发生(高频率)的数据交易事故或重大数据交易事故时的防范与监管,如果采取过于宽泛的管制与干预也可能会带来公共预防的效率损失。以欧盟《一般数据保护条例》(GDPR/2016)对个人数据保护与利用的干预为例,该法以《里斯本条约》和《欧盟基本权利宪章》为基础,将个人数据权益提升至一项以人格尊严为核心的基本权利范畴。据此,欧盟委员会或其成员国在上述宪章和条例的授权下,获得了更为宽泛的行政执法权,即只要数据企业就个人数据的防护未达到基本权利的保护水平,监管部门就可进行相应的处罚,并通过加大对违规者的惩戒严厉程度来威慑不法行为。[②] 尽管GDPR的目标之一是以建立欧洲"数字一体化市场"战略为基础,通过加强欧盟个人数据的保护水平以增进参与者之间的认同与互信感,进而惠及更多的欧盟个人和数字企业,以提升区域内的数字经济发展水平;但过于宽泛

① 通常是指当一方数据参与者认为自身权利受到损失后,通过启动法律强制机制请求对方给予补偿。

② 参见张金平:《欧盟个人数据权的演进及其启示》,载《法商研究》2019年第5期,第187-189页。

的合规管制范围与较高的数据保护水平,也会追加更多甚至是巨额执法成本、公共资源的投入,同时还会额外制约数据利用并增加企业在数据保护中的预防和管理成本①,其效果是否真的能够给企业带来预期制度红利,以及正向激励参与者对数据进行流通、再利用或创新,前景或仍不明朗。

第四类为禁止交易规则。即不允许特定数据私人交易的制度安排。与前三类规则不同的是,无论自愿与否,此类规则不允许特定数据资源在私人之间交易,即取缔特定数据交易的私人市场。比如,涉及国家秘密、网络安全等可能危害国家安全、公共利益或严重侵害他人权益的数据交易。之所以禁止此类数据的交易,主要原因在于此类数据交易可能产生的社会成本和危害巨大,高昂的社会成本会严重减损社会总体福利水平。故禁止此类数据交易带来的社会收益会远大于因取缔特定市场而带来的损失。违反禁止交易规则的救济途径,主要是通过法律制裁包括刑事制裁、行政处罚以及民事惩罚性制裁等,以提高此类数据的交易代价,减少此类交易的潜在数量。

(三)数据权利保障与救济的具体制度安排

1. 用户个人数据的权利保护与救济

就用户的个人数据权利保护来说,以管制交易与自愿交易相结合的规则安排,是对此类数据有效保护的大体进路。在信息完全充分或大体充分的情形下,数据处理者与用户通过意思自治便可实现数据的收集和使用。一方给另一方造成的不利影响,也可通过自主协商的方式加以解决,实现各方利益的最大化目标。但在信息严重不充分的条件下,情况就会发生变化。相对于处理者来说,用户无论在技术上,还是在信息持有方面,均体现为劣势。而这种优劣状态的明显对比,就容易引发作为优势方的数据处理者滥用自身的优势地位,不当收集和使用用户数据,进而增加用户的潜在损失,并由此增加数据开发利用的安全隐患水平。在此情况下,用户在信息不充分增加且严重不对称的条件下,通常无法做出对自身有利的决策,更无法有效预防和减少在交易中因不知情、欺诈等数据偏差行为给自身带来的损失或成本增加。若采取禁止交易规则,虽可使受害方免于损失,但数据开发利用也就无法进行;若以强制交易规则进行调整,在无事前公共预防的前提下,又会进一步增进原本处理者在技术、信息方面占据显著优势地位的水平,并扩大其与用户的信息把握差距,从而会增加数据处理者“机会主义”行为的数量,引发更多的数据交易事故。故法律事前对用户个人数据权利采取管制性的保护措施,降低数据供给环节可能带来的更多社会成本,在某种意义上就具有必要性。

具体来说,除强制性要求平台企业或第三方数据运营者对用户个人数据的收集或使用,以事先告知并取得用户同意作为原则外,在具体的内容安排上,还应进一步提高用户对处理者收集和使用个人数据可能给其既有权益或福利水平带来影响的认知程度,以便使用户做出相对合理的决策,进而保障作为技术和信息弱势方的个人既有权益。具体的规制事项包括但不限于下述内容:处理目的及其适当性与必要性;收集和使用数据可能给用户带来的风险及相应预防措施;对数据处理或利用的安全和质量管理;对出现数据收集和使用事故的处理和救济,以及其他可能影响用户权益的信息披露等。通过管制规则的强制性信息披露与矫正,可进一步提高用户议价的预期,增进决策的透明性,降低与平台企业的信息不对称水平。

① 进一步的述评,可参见许可:《数字经济视野中的欧盟〈一般数据保护条例〉》,载《财经法学》2018 年第 6 期,第 76-80 页。

一般而言,经法律事前干预后,用户的决策信息得以进一步充实,数据交易事故或风险水平相对降低,大体可形成交易方自愿议价的交易环境。故在处理者满足法律管制或公共预防的条件或标准后,个人数据的开发利用便可以用户与处理者的自主协商方式完成,法律可通过默认(缺省)规则等方式,指导主体合理履行交易,而不作强制性干预。对数据处理者违反相关管制交易规则的情形,通常是以行政处罚为主导的惩罚措施作为救济途径。除此之外,对于故意违背用户意愿或未经授权而收集或使用数据的,用户可主张相应的惩罚性赔偿等请求,并要求行为人停止现有以及未来侵害,以提高此类行为的违法成本。

2. 平台企业数据收益和安全保障权利的保护与救济

除用户权利的保障之外,平台企业数据收益权和安全保障权的保护,因其对数据持有的不同开放水平,施以强制交易规则和自愿交易规则相结合的制度安排更为妥当。一方面,针对公开数据——用户自行公开且平台企业未设置访问权限的数据而言,原则上可以强制交易规则作为主导,即在不与互联网通用技术规范相悖的情况下,第三方数据运营者通常可直接访问、收集或使用经公开的数据,无需事先经权利人同意,但事后应向平台企业支付合理对价。从数据交易的场景式视角来看,公开数据通常意味着用户和平台企业期望将数据向他人展示,并以此吸引外部主体的关注、参与,进而实现获得更多交易机会、商业价值等目标。故此类数据原则上可通过"先使用,后付费"的强制交易规则加以保障,省去第三方数据运营者与海量用户、平台企业可能发生的高昂交易成本,以进一步提升数据要素在不同企业间的利用效率,并与网络互联互通的宗旨相吻合。

另外,以强制交易规则干预公开数据的交易,也有利于克制具有优势地位的平台企业从事相应的"机会主义"行为,进而促进数据要素市场的公平竞争。在美国的"hiQ Labs 诉 LinkedIn"一案中,hiQ 作为一家数据分析企业在爬取 LinkedIn 平台默示为自由访问且用户业已公开的数据时,遭到平台的禁止。平台针对 hiQ 实施了反爬等防范性技术措施后,hiQ 采取规避上述措施并继续访问、使用平台数据。据此,hiQ 作为原告向法院申请禁令,要求 LinkedIn 平台取消相关技术措施,允许原告通过爬取手段获取被告已公开的数据。该案历经州法院、联邦法院的多次审理后,2022 年 4 月,联邦第九上诉法院经重审后作出裁判,认为 hiQ 的爬取和避开反爬措施等行为不属于《计算机欺诈与滥用法》(GFAA)中的"未经授权",对于用户就公开信息未明确主张隐私需求的,hiQ 有权访问或获取平台内此类数据,而不论其获取方式。[①] 如果都像 LinkedIn 平台一样,持有海量公开数据的企业选择性地排除特定潜在竞争者对这些数据的访问或使用,其后果不仅会影响到对此类数据的创新利用,也会构成法律上的不公平竞争行为。[②] 实际上,这也意味着该案在一定程度上未将"授权"作为第三方获取数据正当性的唯一判定标准,取而代之的是结合涉案数据的开放状态、交易场景以及数据优势者的潜在"机会主义"行为可能对市场竞争的影响等因素,认为 LinkedIn 平台在交易对象上的选择性限制以及采取的反爬等防护性措施,不仅有悖于用户的数据开放意愿,亦可能造成平台对数据持有与运营的滥用,进而影响到数据在不同平台间的流通与创新效率。尽管该裁判仍存争议和不确定性[③],但与传统的数据持有者单方授权思路相比,这种兼顾并平衡多方数据参与者利益

① See *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F. 4th 1180,1194-1202 (9th Cir. 2022).

② See *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F. 4th 1180,1193-1194 (9th Cir. 2022).

③ 相关述评可参见熊丙万等:《数据确权:理路、方法与经济意义》,载《法学研究》2023年第3期,第67-68页;

的司法策略,亦成为第三方需求者以非合意方式获取平台数据具备正当性的一个典型例证。

另一方面,对于平台内非公开数据来说,权利人更多的或许是出于对个人隐私、平台数据安全与商业模式等方面的利益考量,尽管也有数据流通、交易的需求,但往往更加注重对潜在交易对象的选择,以避免因数据交易事故可能对用户隐私、平台内数据安全以及运营模式等带来的重大隐患或损害。为此,除平台使用规范或用户协议等私人规范加以约束外,此类数据也通常会被平台企业投入更多的防护措施。如设置相应的技术措施、访问权限,预防他人未经同意或授权而获取、使用数据。在此基础上,此类数据的保障可以自愿交易规则为主导,即第三方数据运营者应事先经平台企业及用户的同意或授权,方可从事相应的访问、收集或使用平台内数据的活动,以满足平台及用户对自身数据利益的保障需求。对于平台内的非个人数据来说,鉴于其不再具有特定自然人的识别功能或无涉人的数据,故其利用原则上只需经平台企业同意或授权即可。

需要注意的是,以上对平台企业数据权益保障的两种制度安排都存在一定的不足。就公开数据的保护与救济而言,强制交易规则在降低平台与第三方之间的交易成本以及相关负外部性的同时,也是要付出代价的——即由此产生的强制定价的成本。以司法强制定价为例,与市场机制不同的是,法院由于缺乏对价格信息的了解,往往不擅长对数据的强制定价,进而可能引发较高的定价信息成本,甚至是定价错误的风险。① 为了降低或减少这一强制定价成本,增进强制交易规则可能带来的净收益水平,鼓励和倡导私人资源的积极参与或许是一种更为有效的办法。较为可行且务实的措施,便是激励作为数据市场媒介的参与者(经纪人),面向社会提供数据要素的价值咨询或评估等服务,以降低第三方定价部门的信息成本,为同类数据的潜在交易者提供价格参考,同时亦为以数据估价等信息咨询、评价为主导的行业分支建设奠定基础,助力数据产业的全方位发展。

而就非公开数据的流通而言,自愿交易虽可降低参与者对数据价值的评估成本,但这种以合意方式的数据获取模式,往往会使平台企业、用户与第三方数据运营者在数据利用的协商环节耗费大量议价成本,同时也会导致作为数据持有者的平台企业滥用自身优势地位,从事不合理的选择性合作、通过平台或用户服务协议对其他运营者采取歧视或不公平等偏差措施,进而影响数据的流通效率与再次利用水平。为了解决以上问题,激励平台企业合理明确第三方数据运营者利用平台内数据资源的具体规范,特别是“数据访问(接触)权限机制”②、“协助第三方获取用户授权或同意的机制”③以及“满足保障平台运营安全的必要指标测评体系”等内容,或可有效降低平台内数据流通中的交易成本,提高数据的利用效率。

与此同时,在个人和非个人数据领域,无论是公开数据还是非公开数据,激励相关社群的广泛参与,支持和鼓励数据行业协会或研究机构定期收集、发布相应数据资源的交易指南和参考价格,亦能满足数据参与者的交易需求,并可进一步降低数据流通的交易成本。相关实践已在国内外陆续展开。在国内,以中国信息通信研究院云计算与大数据研究所为代表的通信科研机构,针对传统

① 有关司法定价不当或错误的实例剖析,可参见侯猛:《中国最高人民法院研究——以司法的影响力切入》,法律出版社 2007 年版,第 27-30 页。

② 该机制在某种程度上可借鉴网络版权保护中的技术措施制度安排,可参见谷川:《法理学视域下技术措施法律保护研究》,载《河北法学》2014 年第 3 期,第 156-164 页。

③ 一般而言,在平台企业不参与的情况下,第三方往往难以获得平台内数据主体——用户授权或同意的机会,故平台主体对第三方获取用户授权或同意应予以必要的协助,以保障此类数据得以进一步被开发利用。

数据集、API接口交付以及新兴隐私计算融合结果交付的权责划分等问题，出台了《数据交易合同示范文本》[①]，为行业内的数据交易提供了指引性规范，提高了数据交易的标准化水平；在域外，日本经济产业省和物联网加速联盟于2017年发布了《数据使用权合同指南》，该指南在交易目标数据的来源、范围、转让方对目标数据的贡献水平、受让方对数据的使用权限、数据利用管理与风险及其预防等方面对交易者作出了较为全面、务实的规范性指引[②]，其不仅有助于数据交易便利化的提升，而且这种由主管部门与相关行业部门联合制定的数据交易规范指南，在其预期效用的发挥上，也具有鲜明的特色。一方面在于利用行业部门的信息优势地位，可有效节约不同数据要素交易的信息成本，进而在一定程度上避免或降低数据交易事故增加的可能性；另一方面，公共主管部门的参与也在不同程度上提高了此类规范的权威性，促使规范实施的可预期水平得以进一步增强。

除强制交易规则与自愿交易规则之外，法律也可对第三方数据运营者访问、收集或使用平台数据所需的基本安全标准、数据的处理质量，以及被用于数据处理技术改进的“关键设施”“数据访问(接触)技术措施”等部分事项采取管制规则进行事前干预，以有效降低技术或信息优势者的道德风险，预防和控制平台企业与第三方可能发生的交易事故。除此之外，为了公共利益或其他方面的需要，法律强制许可他人访问或使用平台内数据，以实现更大的社会收益，亦为可行。

除了上述对数据的保护和有效救济方式，对于可能引发严重社会成本或危害的数据交易，法律是予以禁止的，这便是禁止交易规则在数据交易中的具体表现。比如，涉及国家安全、公共安全或特定个人隐私等内容的数据，一旦交易，其预期收益通常远低于给国家、社会以及用户个人带来的重大损失，进而大幅降低社会总体福利水平。故与自愿交易、强制交易以及管制交易等可交易规则相比，对此类数据采取禁止私人交易的保护方式，或许更有利于社会福利的增进。

四、结 语

本文采用法律经济学的分析方法，以效率考量的视角，剖析了由数据行为的外部激励需求引致的数据界权法律干预的必要性，再到法律界权的具体安排及其界权后的制度保障与救济等问题，初步建构了提升数据要素在私人领域社会效用的法律激励机制及理论框架体系。在具体层面上，一方面是探索了法律对数据供给、处理以及流通交易环节不同数据参与者的合理激励方式，以提升数据价值的产出、创新效率及要素的优化配置水平；另一方面，在于通过不同制度安排的激励，有效避免或减少因数据开发利用导致的在参与者之间的利益冲突或分歧，及其产生的社会损失或成本增加，进而提高社会的总体福利水平。

大体上，法律对数据界权的有效干预，是提高数据社会效益的重要途径。在数据供给与处理环节上，明晰要素权利的法律界定，赋予用户的个人数据权，以及赋予平台企业的数据收益和安全保障权，不仅便于促使离散于外部的收益内部化，以增进数据要素供给及其开发利用的价值产出，更能有效降低因参与者的数据利益冲突或分歧所带来的负外部性影响；而在数据的流通交易环节，则

① 相关述评，参见中国信息通信研究院：《数据要素白皮书(2022年)》，载中国信息通信研究院网站，http://www.caict.ac.cn/kxyj/qwfb/bps/202301/t20230107_413788.htm，2023年6月10日访问。

② 参见付新华：《企业数据财产权保护论批判——从数据财产权到数据使用权》，载《东方法学》2022年第2期，第141-142页。

应注重界权后要素权利的法律保障与救济,在不减损参与者数据权益的基础上,以数据要素的合理开放利用为主导,通过不同的权利保障机制和制度安排以提高数据要素的优化配置水平。与此同时,无论是在数据要素供给、处理环节还是在交易流通环节,建立以效率为主导的法律激励,不仅内含对数据行为社会收益与社会成本二大因素的考量,且在此过程中,数据行为的公平①、安全②等内容也会在不同程度上得以体现,成为数据要素权利法律界定与保障的重要因素。在此意义上,基于效率的法律激励,并未忽视效率之外的其他评价因素,而是将其融入到效率激励的法律框架内,更好地满足数字经济的可持续发展需求。JS

The Legal Limitation of Property Rights and Protective System of Data as Productive Factors: Legal Incentives Based on Efficiency

GU Chuan

(Beijing Water Resources and Affairs Law Enforcement Corps, Beijing 100036, China)

Abstract: The necessity of the legal limitation of property rights of data as productive factors is extended from the external incentive demand in the digital private sphere. In the part of data supply and processing, the legal right to personal data should be given to the user. The platform enterprise should inform the user and obtain their consent before collecting or using them. On this basis, the benefit allocation of data in the platform would be embodied that the platform enterprise should hold the rights of data income and security to the platform, and other data processors shall give reasonable compensation when collecting or using that data. In the part of data transaction, four basic institutional arrangements, including voluntary transaction, compulsory transaction, regulated transaction and prohibited transaction rules, shall enhance the effective protection of data rights according to experience types of data transaction after legal limitation of property rights to data resources, and improve the optimal allocation level of data as productive factors in the data market, meanwhile lay the foundation for the legal order of data transaction.

Key words: limitation of property rights to data resources; personal information; platform enterprise; data transaction; law and economics

本文责任编辑:林士平

青年学术编辑:赵　吟

① 比如,利用法律界权促使数据参与者之间的权利配置达致均衡的目标;通过制度安排缓解不同数据参与者之间技术或信息严重不对称的情况,等等。

② 比如,法律对私人领域数据行为安全保障的公共预防制度安排与私人预防的激励措施等。