

企业数据权益原论：从财产到控制

梅夏英*

摘要 企业数据权益在法律上如何定位和保护是当前互联网法学面临的理论难题。既有的理论主张主要从信息私权和财产权角度试图将数据纳入实体权利的框架中，参照传统私权规则来对企业数据进行调整。信息私权中的“数据库保护”和“商业秘密保护”规则与企业数据保护具有形式上的相似性，但在实质利益形态和涵盖范围上有根本差别，由此导致“信息内容保护”导向的失败。企业数据保护问题源于互联网的普及，只在数字技术语境中才有意义，故必须在区分信息问题和数据问题类型的背景下进行考察，由此企业数据权益应在整体上作为一个纯粹的数据问题予以讨论，企业数据财产理论因其客体无法确定很难成立。企业数据在利益形态上表现为对现实数据的有限自我控制，这种事实控制所含法律利益本质上体现为信息自由。基于此，企业数据的保护应当以维护数据的控制为基础，可通过侵权法、合同法和竞争法对围绕数据控制的争夺可能涉及的各种实际利益进行保护。

关键词 数据权益 数据库 信息私权 数据控制 纯粹数据问题

企业数据确权问题已在法学界经历了诸多讨论。这一问题是继互联网发展早期出现的个人信息保护和虚拟财产界定问题之后自然发生的，但在早期讨论中，企业数据常常与个人数据、虚拟财产等相提并论甚至纠缠在一起，其独立的价值和利益形态并未获得充分认识和理论彰显。当代大数据和人工智能技术的发展，使企业数据的价值和地位被重新认识，社会普遍认识到企业数据作为生产要素存在的必然性，近年来中央和地方相继出台的各种政策和法律文件，将企业数据提升到事关数字发展战略和智慧管理体系建设的一个新的高度，并对数据产权

* 对外经济贸易大学法学院教授。本文系国家社会科学基金重点项目“数据的分享和控制法律体系研究”（项目编号：19AZD026）的阶段性成果。

的界定和数据要素市场的培育提出了实际要求。^{〔1〕} 企业数据产权问题再次成为法学领域的争论焦点。但目前关于数据产权问题的法学研究进展并不顺畅,甚至陷入一个缓滞的状态:其一,尽管数据产权问题被充分重视,但在中央和地方的重要政策和立法文件中,并未体现出这一问题前置性价值,相关文件更多集中于个人数据、公共数据分享、数据安全和保护、数据市场监管和数据竞争等内容,数据产权并未处于重要地位,甚至被一笔带过;^{〔2〕}其二,现有的研究范式囿于传统私法权利思维模式,^{〔3〕}在物权、债权和知识产权之间寻找企业数据的利益形态表达术语,通常很难自圆其说,尤其是无法处理好数据的分享与独占、公开与控制以及技术载体与信息内容之间的紧张关系,每种理论方案的涵盖面有限,例外情形甚多;其三,现有讨论局限于信息内容的归属,很大程度上忽视了电子数据这一新生事物的独立运行规律。事实上,数据产权问题的产生并非源自信息内容的归属问题,而是电子技术致使信息高度集中的后续应对问题,依目前情形看,现有的理论探讨并未在数据与信息的界分和两者交互的相对独立性上建立富有创新性的理论尝试。

有鉴于此,关于企业数据确权问题,目前缺少的是对于企业数据利益形态的基本理论判断,这种判断应是宏观的、基础和方向性的,是建立在对于电子数据本身的充分了解和传统信息法律的精确运用上,以及对于数据、信息和传统稀缺客体等法律调整规律的宏观比较研判上,而非自我设限将关注点集中于传统权利体系的框架之内。目前既有的理论探讨素材和丰富的行业实践使对企业数据基本理论进行总结性探讨变得可能,本文拟在此方面做出努力,文章将在回顾传统信息领域的法律规制数据局限性的基础上,考察企业数据利益的问题类型和性质,探讨将其归于独立数据问题的可能性,并探讨企业数据价值的来源、表现形式和保护方式,以供同仁商榷。

一、传统信息私权调整企业数据利益:信息内容保护导向的失败

将数据权属问题归属为传统法律体系中有关信息权益保护范畴,是目前法学界流行的做法。这种做法致力于在传统法律体系中找到与信息保护相关的制度,并比照既有的相关制度来界定数据权益的保护规则,其理论基础是,电子数据无非服务于信息的生成、传输、流通和利用等,将信息归属问题解决之后,数据归属问题亦随之解决。这种做法的产生是自然而然的,因为我们先前无法找到将数据本身作为独立要素进行法律规范的先例和理论依据,且这种做法也可以直接实现“保护数据的目的在于保护信息”的初衷。由此,传统以信息内容的保护为目的的私法制度被陆续挖掘出来,为企业数据权益的定义和定性提供营养。但从现有私法对于信息保护的制度来盘点考察,其能提供的具体权益类别和保护制度甚少,具体体现在人格权

〔1〕 2021年3月,第十三届全国人民代表大会第四次会议批准并发布了《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》,明确统筹数据开发利用,加快建立数据资源产权等基础制度和标准规范。

〔2〕 《深圳经济特区数据条例》征求意见稿中曾经提出“数据权”的概念,但在最终正式版中删除。

〔3〕 参见张文显:“中国民法典的历史方位和时代精神”,《经贸法律评论》2018年第1期,第6页。

法中的隐私和标识性人格权(姓名、肖像等),以及知识产权(专利、商标、著作权、商业秘密和数据库)等。对于除此之外的信息,人类几千年来并不提供任何私法上的保护(公法规制在此不论),将之悉数置于公共分享领域。人类对信息的私法限制相当谨慎,正是这一显而易见的事实使数据权属问题变得困难。即使如此,在上述对特定信息保护的种类和框架中,企业数据亦难以获得一席之地,以下详述之。

(一)以传统信息权益规则调整企业数据的理论主张及评析

在传统私法关于信息利益的保护方式中,人格权和知识产权均为考察对象。但企业数据适用人格权法保护的局限比较容易理解,目前也鲜有学者提出此种主张。因为无论是隐私,还是标识性人格权,都不可能完全适用于企业数据。但将个人数据及相应部分的企业数据推及至人格要素或利益的做法,却成为目前我国个人信息保护法的主流理论基础。关于个人信息是否一定属于人格要素,以及个人信息权益与隐私权如何协调,甚或个人信息保护法是否以阻止公众分享个人信息为目的等问题,都尚有讨论余地,在此存而不论。^{〔4〕}现实情况是,企业数据虽然包含了大量的个人信息和人格要素信息,但是分属固有的不同法域(如个人信息保护法和人格权法)调整,其他企业数据则被置于另一领域独立讨论。同时在企业履行去标识化或匿名化义务后,企业数据利益与人格权中的信息保护规则又被区分开来,企业对其所控制之大数据享有何种利益便成为一个独立的问题。

企业数据适用知识产权保护则是目前理论界关注的重点。就专利权和商标权而言,理论上很少有将企业数据利益归入专利权和商标权的主张,否定的理由主要是企业数据缺乏专利和商标所应具备的创新性、新颖性等法律要件,这类理由是合理的,但并不充分,因为企业数据不适用专利和商标规则的根本原因在于,专利和商标的获取、流通和利用等都以信息公开为前提,这与企业数据依赖自我控制以防外泄的理念完全不符。除此之外,尚有著作权保护的观点,此类观点并不轻率地主张企业数据适用著作权法保护,而是通过当代既有的数据库保护理论来获得支持。至于“商业秘密”保护的主张,亦有相当数量学者和业内人士赞同。因此,目前主张在知识产权领域保护企业数据的有影响的观点主要有两种,即“数据库保护说”和“商业秘密保护说”,在此进行重点剖析。

1.数据库保护模式

数据库保护源于著作权法对具有独创性的汇编作品的保护,即虽然作品内容由汇编人收集,并未提供独创性贡献,但如果内容收集者对于数据的选择、整理和编排做出独创性贡献,则能够从整体上对该数据集享有汇编作品的著作权。这种做法始于上世纪六十年代北欧国家尝试的“目录规则”(the Nordic Catalogue Rule),其后1996年欧盟颁布的《关于数据库法律保护的96/9/EC号指令》(以下简称“数据库指令”)则有所丰富和深化,该指令同时采用著作权和特殊权利模式来保护数据库,其中著作权保护适用于原创性数据库,特殊权利保护则适用

〔4〕关于个人信息与隐私权以及个人信息保护的立法目的等问题,参见王利明:“和而不同:隐私权与个人信息的规则界分 and 适用”,《法学评论》2021年第2期,第15—24页;王利明:“论个人信息权的法律保护——以个人信息权与隐私权的界分为中心”,《现代法学》2013年第4期,第63—72页。实际上,即使《民法典》也未能将个人信息完全权利化,参见赵宏:“《民法典》时代个人信息权的国家保护义务”,《经贸法律评论》2021年第1期,第2页。

于非原创性数据库。^{〔5〕} 欧盟“数据库指令”反映了从传统汇编作品向电子数据库保护的转变,且对两者的保护同时兼顾。但在电子数据库产生以来有关企业数据库的立法争论中,著作权的影响在逐步消失,企业数据库的特殊保护力度也在逐步弱化。如美国针对当代互联网电子数据库问题曾提出多个数据库特殊保护立法方案,均因科学界和网络行业的反对而失败,现今美国只是在司法创设的“热点新闻学说”(hot news doctrine)的框架下,对不受著作权保护的实时事实消息提供非常有限的保护。^{〔6〕}

采用数据库保护模式保护传统汇编作品和企业数据,无论是著作权方式还是特殊权利方式,都可理解为一种权宜之举,这主要体现在:其一,数据库保护只是保护“条目”的独创性或所谓的资金“投入”,因此对于经多方途径收集而来的数据库内容(无论公开与否),都不能由数据库创建人主张权利。只要分享者调用数据库的信息量不超过影响数据库整体价值的程度,原则上都应该是被允许的;其二,数据库保护与数据个别内容的保护相互区隔,即数据库内含的人格要素内容或知识产权内容受相应法律保护,法律对整体数据库的保护相对独立。^{〔7〕} 无论个别数据内容是否公开,数据库保护都无需搭具体内容保护之便车,除非当事人行为触犯了数据库的独创性和整体价值;其三,数据库保护倾向于原创性数据集合,即对现实生活中已经存在的数据内容进行收集、整理和编排形成的数据集合,而非针对尚在形成中的、处于动态收集状态的数据集合。这一点对于传统汇编作品当无疑义,因为传统数据库(包括纸质和电子形式)的价值就在于对现有零散信息的归集和整理,但对于网络企业数据库而言,就存在一个非原创的问题,欧盟“数据库指令”特殊权利保护的主体是否确定适用于尚处于通过动态信息收集阶段的数据库,即非原创性的、动态数据库,存在着一个由肯定到否定的理解过程。

依上述对数据库保护模式的分析,可以发现电子数据库保护的立法目标并未建立在一个稳固的法律基础上。如果说原创性汇编作品因具有“条目”的独创价值和社会增益功能,适用著作权法保护比较容易理解,那么对于当代企业电子数据库而言,因其涵盖内容庞大,并处在数据收集和分享过程中,且“条目”的价值因算法的客观存在和搜索、复制等网络技术的运用,其独创性价值大大降低,此时便不宜再适用著作权规则保护了,这已成为业界共识。在无法适用传统信息私权保护的情形下,欧盟“数据库指令”采取特殊权利保护的主体就不再清晰明了。虽然该“数据库指令”在第7条第1款规定要保护数据库制作者做出的实质性投资,似乎此一规定可以适用于非原创性的、动态的企业数据库,但在解释“数据库指令”时,欧盟法院强调提供激励的目标是基于已经存在的信息创建数据库,而非创建新元素后再基于此搭建一个数据库,亦即针对获取数据库内容所作投资给予的保护,并不涵盖数据库创建者为创建单独

〔5〕 欧盟《关于数据库的法律保护的指令》第7条第1款规定:“各成员国应为在数据库内容的获取、检验核实或选用方面,对证明在质量与或数量做出实质性投资的数据库制作者,赋予防止对数据库内容的全部或在质量或数量做出实质性投资的数据库为实质部分进行摘取(extraction)与或反复利用(re-utilization)的权利。”

〔6〕 参见崔国斌:“大数据有限排他权的基础理论”,《法学研究》2019年第5期,第7页。

〔7〕 参见欧盟《关于数据库法律保护的指令》第96/9/EC号指令》第3条第2款。

要素所进行的投资。^{〔8〕}美国联邦最高法院在 *Feist Publications, Inc., v. Rural Telephone Service Co.*案中,既不支持对缺乏独创性的数据库予以保护,亦不承认建立数据库的投资是获得著作权保护的充分理由,并据此认为,数据库权不保护未经加工创造的原始数据。^{〔9〕}至此,企业电子数据库的特殊权利保护方式前景黯淡,对数据内容集合进行合理保护的必要在电子化时代几近失败,其中的主要原因在于,立法上找不到一个合理控制数据库内容信息流动的强有力理由,这是私法对信息予以保护和控制的前提条件。^{〔10〕}

2. 商业秘密保护模式

在所有传统信息私益的保护方式中,商业秘密应是最接近企业数据保护目的的选项。因为其他人格法益或知识产权方式都不完全强调信息内容必须保密,其权利利益由内容决定,而非源于针对内容外泄的自我防护。支持商业秘密保护企业数据的合理理由:一是企业数据中有相当部分本身即构成传统法律中的“商业秘密”,如用户或客户数据、交易记录、经营信息、行程记录等,这些都无形中支撑了对企业数据进行保护的必要性;二是企业数据通常都被有效储存于平台服务器的私人空间,并为保密措施所覆盖,致使他人大规模获取甚为困难,客观上也使企业数据因具有一定的保密性,而产生适用商业秘密规则的可能性。即使在通常情况下少量数据信息由他人分享,亦不影响整体数据的商业秘密性质;三是企业数据具有特定的适用语境和归集、整理和筛选方式,“这使得大数据集合中数据条目信息的存在状态与公共领域的分散数据形态有很大差别,更加符合商业秘密保护的秘密性要求。”^{〔11〕}上述理由使商业秘密规则对于企业数据保护的必要在现实中有所呈现,因为在一些特定行业平台中(比如航空公司和医疗机构等),数据集合构成商业秘密的集合,适用商业秘密保护即为已足。

但是采用商业秘密规则来保护企业数据只是在局部范围或特定情形下可以奏效,并没有普遍适用的意义,因为毕竟两者属于不同的范畴,在比照适用中会遇到无法逾越的障碍。具体而言:首先,商业秘密保护的主张无法合理解释企业电子数据库和非电子数据库在定性上的差别。目前企业数据库保护问题的产生源于在线企业电子数据库的兴起,而在传统媒介时代,企业依然存在自身的非电子数据体系,这些企业数据也不可能被置于公共领域并有管理制度制约,但从未产生过企业所有的数据都适用商业秘密保护的问题,商业秘密规则通常被限制在一个特定的范围发挥作用。信息表达形式的变换是否就直接导致信息内容定性的改变,是值得慎重思考的问题。其次,企业数据是否都具有商业秘密的价值性,也值得推敲。商业秘密通常

〔8〕 相关判例首次出现在欧盟法院关于 *Case C-203/02, BHB Horsereading* [2004] ECR I-10415 案判决的第 31 段。即便如此,欧洲法院于 2005 年在 *British Horsereading Board v. William Hill* 案中大大缩小了数据库的权利范围,认为通过大量投资搜集的数据不属于《欧盟数据库保护指令》的保护范围,只有数据库的原创性结构才是保护对象,所以部分调用数据库中的数据不构成侵权。

〔9〕 See 499 US 340 (1991).

〔10〕 对数据库要素提供事实上的保护(特别是对单一来源资料的保护),实际上相当于以专有权的形式来保护数据库内容。为避免这一风险,欧盟《关于数据库法律保护的第 96/9/EC 号指令》规定了一项内容提取的门槛(第 7 条第 1 款),一项欧委会的报告义务(第 16 条第 3 款)以及适用一般性竞争规则的提示(指令前言部分第 47 条)。

〔11〕 崔国斌,见前注〔6〕,第 6 页。

意味着对企业的经营和发展具有实质价值的信息,并以具体信息内容展现出来,而企业数据就其所含庞杂的信息而言,并不一定都符合这一要求,事实上对于一些“头部”平台企业(如腾讯和中国电信等)而言,定期清除用户的通信记录或交易记录是其惯常作法。在此基础上,以企业数据被保密为由,主张企业数据在整体上具有商业秘密的价值也很难成立,这可类比现实生活中广泛存在的排斥他人访问的藏书馆、资料库等,相关机构对其所控制的整体信息从未产生类似商业秘密保护的问题。第三,企业数据的保密性远不如商业秘密所应具有保密性。企业数据通常会通过多种途径由他人分享,如部分开放给用户、通过 API 等方式与其他平台进行数据互享以及依法定程序提供给政府机构等,这些都不是商业秘密的题中应有之义。尤其当企业数据整体与他人互通或整体提交他人分享时,“商业秘密”的权益属于谁就成为问题了。关于商业秘密与企业数据保护的违和之处尚有其他情形,在此不予赘述,但商业秘密保护法理与企业数据的保护并不完全契合,在诸多方面甚至有根本差别,充分说明理论界对于企业数据保护的理解存在着某种结构上的偏差。

(二)企业数据保护中“信息内容保护导向”失败的原因

上文将传统私法上的信息权益比照企业数据保护所作的分析,是对目前企业数据保护的目的在于保护数据所承载信息内容这一普通观念和与之相关制度的解读。关于企业数据权益的其他观点(包括所有权和用益权的二元区分方法)将会在下文涉及,此处不论。结合上文分析来总体观察,从信息内容保护的角度来定义和设计企业数据保护的规则和规则,总体来说是失败的,上文对最具参照意义的“数据库”和“商业秘密”保护规则在企业数据保护领域失灵现象所做的分析,就可以部分证明这一点。通常观点认为,对企业数据进行保护即同时保护了数据所承载的信息,这种命题并没有谬误;但若反过来,企图通过保护信息内容的方法来达成对企业数据的保护,依上文所做的分析就不尽合理,甚至是失败的。但为何通过“信息内容保护”方式难以达到企业数据保护的,其原因可做如下阐述。

首先,传统私法对于信息内容进行法律上的干预和控制,需要强有力的理由。在人类私法自萌芽始直至今天的漫长过程中,私法对信息鲜有干预和控制。目前私法体系中只有人格权法和知识产权法对于特定信息内容(如隐私、作品或商业秘密等)予以赋权保护,且有与法律所尊崇的系列基础价值直接相关的充分理由,除此之外其他所有的信息都被置于公共自由领域,由公众自由分享。当然,特定信息也会基于公共安全或舆情管控等原因而被公权力限制流布,但这些信息管控措施也必须服务于必要的、特定的公共目的。对于企业数据而言,通过对其所含信息进行广泛的、抽象的法律赋权,来达到限制或阻止公众分享信息的目的,尤其是对人格要素或知识产品之外的信息也做如此安排,其正当性和合理性何在? 信息的社会化分享历来是人类社会得以生存和延续的基础规则,它构成社会交流和行为自由的重要组成部分,信息媒介的进步通常会强化信息交流,而不是相反。^[12] 因此,对企业数据库信息进行整体性赋权,既与公共的信息自由相冲突,又缺乏基础性的、强有力的法律理由。

其次,对企业数据库进行信息赋权与企业数据保护的保密机理并不相符。传统相关信息

[12] See Arun Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*, Cambridge: The MIT Press, 2017, p. 47.

私权中,除了隐权和商业秘密是将自我保密作为权益保护的先决条件外,其他信息私权(包括标识性人格要素和专利、商标和著作权标的等)都不要权利人实施信息的自我控制,甚至在大多数情况下都以标的信息的公开为原则。如姓名、肖像、专利、商标等相关信息自权益发生时即处于公开状态,著作权作品也不例外,自作品创作、发表至流通各个环节,法律并不禁止他人获知作品信息,只是禁止未经权利人许可非法出版和流通。人格权规则重在救济,知识产权规则重在保护特定信息的商业化利用,都不完全依赖信息的自我保密,如侵犯隐私的行为并不影响隐私的完整存在,盗版他人作品也不影响著作权的完整性。至于商业秘密保护方式,虽然强调自我保密,但又局限于特定信息,学者对其是否属于一种财产性法益仍然存在争议。^{〔13〕}但企业数据库的保护则完全不同,它以防止泄露和被他人非法分享为目的,适用信息学上的“阿罗不可能定律”,这种宽泛的保护及于所有数据信息,与信息内容并不发生直接联系,故这种建立在自我防护基础上的法律运行机理与传统的信息权益具有根本差别。^{〔14〕}

第三,对企业数据所含信息进行赋权会造成权利叠加和权利冲突的现象。抽象地将企业数据赋予一个类似数据库或商业秘密的定性,会造成这种定性与信息内容自身法定性的叠加,比如数据库中的作品信息既属于著作权保护对象,又属于企业的商业秘密;数据库中的企业自身的商业秘密同时又附加了数据库本身的商业秘密等,甚或本已公开分享的普通信息因存在于数据库中,又成为了数据库权益的组成部分。这种信息权益的机械叠加会造成不必要的法律适用的混乱。权利冲突则体现在,当企业数据因自愿、约定或法律规定由公众、相对方或政府机关分享时,企业数据的信息权益便不再明确了。比如当企业数据通过 API 方式与其他平台共享或提交给政府时,此时企业数据的数据库利益或商业秘密的归属就很难确定,很显然企业数据一经大规模分享,传统的信息权益保护方式在此对于后续数据获得者的约束力不再有效。

除此之外,尚有整体赋权与局部信息分享的矛盾问题等,受篇幅限制在此不予展开。通过寻找“信息内容保护”导向在企业数据保护上失败的原因,可以将社会的关注力转移到电子化信息的分享规律上。实际上,在没有私法上信息“原权”保护的情形下,电子信息的分享和流通仍然适用传统信息运作的“元规则”,即由信息控制者享有在“保密”和“分享”之间的自主选择,此外无他。在信息控制者不愿分享的情形下,因保密措施不力或他人非法获得信息,外泄的信息本身若无“原权”保护便自始进入公共领域,无从救济。但对于非法行为的责任追究,适用的便是其他相关法律,与信息本身不再有实质联系。

二、作为整体的企业数据保护:一个纯粹的数据问题

从信息内容角度保护企业数据,因面临信息“原权”的缺失而无法胜任企业数据保护的目

〔13〕 参见黄武双:“商业秘密的理论基础及其属性演变”,《知识产权》2021年第5期,第3—14页。

〔14〕 关于“阿罗不可能”定律, see F. Scott Kieff, “On the Economics of Patent Law and Policy”, in Toshiko Takenaka (ed.), *Patent Law and Theory: A Handbook of Contemporary Research*, Cheltenham: Edward Elgar Publishing, 2008, pp. 4—5.

的。但企业对所拥有的数据库应该享有某种客观利益,这一点是不容否认的,法律应当对现有的网络企业数据进行相应的保护,也已成为目前理论界和业界的普遍诉求,甚至成为数据要素市场的一个前提条件。因为若法律不对企业数据进行一定的利益界定和保护,企业数据的控制和流通秩序便无法建立。在通过对数据的信息内容赋权进行保护的方式失效之后,法律如何看待或定义企业数据的性质,以及以何种方式保护企业数据库,已成为数据立法中的争论焦点。除了上文所提到的在知识产权领域内寻找数据的权利外衣之外,法学界尚有从财产权角度对企业数据进行确权的尝试,如“数据资产权”说、“数据所有权与用益权”的分离说、“数据公开传播权”说、“数据块权利”说等。^[15] 这些理论主张倾向于在数据的来源方、数据控制者和第三方分享者之间建立一个数据利益的分配和平衡秩序,并且大多坚持数据的来源方即用户为最终所有人,企业数据控制方为用益人或实际权利享有人。这些主张都有各自的合理关怀,具体论证细节在此不予介绍,但都面临对两个根本问题的进一步回应,即企业数据保护的对象是电子数据库的形式还是内容,是作为整体的数据库还是个别数据的集合? 对这两个问题的深入探究有助于在理论上还原企业数据的真实利益形态。

(一)作为整体的企业数据保护属于纯粹的数据问题

通过传统财产权规则来定位企业数据库的权益形式,面临的共同问题是,企业数据库保护的是数据本身的完整,还是保护数据所载信息内容的归属,两者的区别在现今的理论论述中常常被忽视,同时数据和信息作为探究对象在概念上被不加区分地使用甚至被相互混淆,致使所论述的对象并不固定。比如说在论述用户与企业数据关系时,采用数据所有人与控制人(资产方或用益人)的表达,很明显这里数据指向的是“信息内容”,因为用户与企业之间传递的只是信息内容,数据形式可能不尽相同。但在论述企业数据被爬虫等非法获取时,此时数据指向的则是服务器中储存的“数据形式”。又比如数据财产权主张中常常提及个人信息被收集成为数据库的一部分,数据指向的是“信息内容”,但在论述个人信息被去标识化或匿名化后形成一个抽象的权利客体时,数据指向的无疑又是“数据形式”。同样的问题也存在于企业数据保护的对象究竟是整体数据库还是单个数据的集合上。比如用户通过代码分享平台数据库的相关信息时,此时数据库指向的是“单个数据的集合”,而在用户违背“robots 协议”分享操作权限之外的信息时,此时数据库指向的则是数据整体,因为此时数据内容并不重要。这种企业“数据”指向上的游移不定并非单纯文字游戏,而是提出了一个重要问题,企业数据保护针对的究竟是数据还是信息。

数据和信息概念的区分问题已受学界普遍关注,只是关于这种区分有何法律意义,学界一直缺乏深入探究。仅从概念上进行区分,并没有太大的实际意义,因为在数字化时代数据成为

[15] 关于“数据资产权”说,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,第63页;关于“用益权”说,参见申卫星:“论数据用益权”,《中国社会科学》2020年第11期,第117—120页;关于“公开传播权”说,参见崔国斌:“大数据有限排他权的基础理论”,《法学研究》2019年第5期,第20—23页;关于“数据块权利”说,参见许可:“数据权利:范式统合与规范分殊”,《政法论坛》2021年第4期,第92页。

信息的主导形式,且网络大系统中的数据与信息直接相对应,很难适用传统媒介和信息的区别,两者之间甚至只存在一个“读取与否”的差别。^[16] 在各种场合的表述中,数据和信息概念的互换并不能使人产生误解。但数据和信息概念的差别终究会在特定的场合适时显现出来,即依据数据信息纠纷中不同诉求指向对象的差异,理论上可以把数据纠纷中的问题类型区分为信息问题和数据问题,对此已有论述。^[17] 信息问题和数据问题的主要区别在于,前者指当事人对于信息内容进行主张,以维护自身的信息权益,如知识产权的网络侵权、个人信息保护和信息安全等;后者指当事人对自身控制的数据完整和安全提出主张,以防止因他人非法访问和攻击而致使自身控制的数据变动或流失,如虚拟财产、算法规制和网络安全等。在此前提下,信息问题所要解决的是信息内容免受侵犯,法律随顺信息的流向予以救济,无论信息流向何地;数据问题则要解决数据的访问和流通秩序,它产生于网络系统,亦在网络系统内通过适用特定法律予以解决,且以自我防护为主。除了上述纯粹的信息问题和数据问题以外,网络世界中尚存在两类问题兼有的实际诉求,比如政府电子数据库的开放、数据跨境流动等,就同时涉及信息的流动和数据形式的维护,但在解决问题时两者相互独立,并不冲突。

信息问题和数据问题区分的主要意义在于,它可以帮助我们确定信息数据问题中的具体对象和利益形态。依此观察,企业数据问题应当归入纯粹的数据问题范畴,其原因在于:其一,企业数据问题的发生源于数字技术和互联网的兴起,这是将其归入数据问题类型的基础。因为在传统社会中亦存在以其他媒介形式存在的“数据库”,也存在该类信息库被侵犯的问题,但并未产生类似企业数据保护的诉求,这充分说明企业数据保护问题来源于互联网技术系统,而并不源于信息内容本身,依此逻辑,既然企业数据问题是互联网数字系统的原生问题,其解决方式亦不应脱离该系统而存在。其二,目前的企业数据保护并不区分各类数据所含信息的内容,而是在整体上都适用一个抽象的保护方式。无论是个人数据、隐私数据、知识产权数据甚至无用数据,也无论是公开数据还是非公开数据,都适用企业数据保护规则,此时基于具体信息的保护规则和抽象数据的保护规则同时存在,且互不矛盾。这充分说明了企业数据的保护具有抽象性和工具性,其形式保护的属性决定了企业数据保护属于数据问题类型的合理性。其三,企业数据保护并不排斥部分数据内容的公开或分享。任何平台企业都会公开部分数据由用户分享,或通过“API”方式与其他平台互享,或依法提供给政府机关,在上述诸情形下,信息内容已由他方整体或部分获得,但并不影响企业对其数据库保护的需求,企业数据保护问题仍然完整存在。上述诸多原因的存在,决定了企业数据保护问题属于典型的数据问题类型,这种理论判断对于企业数据保护具有重要的理论意义。

(二)将企业数据保护定位于纯粹数据问题的法律意义

将企业数据问题聚焦于数据问题领域,可以在理论上锁定企业数据的利益范围,消除现有学术争议在概念上的模糊或矛盾之处,并为探讨企业数据保护的解决之道建立一个确定的理

[16] 关于数据和信息的差异,参见许可:“数据安全法:定位、立场与制度构造”,《经贸法律评论》2019年第3期,第54—56页。

[17] 参见梅夏英:“信息和数据概念区分的法律意义”,《比较法研究》2020年第6期,第151—162页。

论背景。具体而言,其法律意义存在于下述方面:首先,将企业数据保护归为数据问题类型,可以有效消解物权法思维对该问题的误读。因为无论采用何种论证思路,物权或财产权主张都强调一个排他性的财产或客体的存在,并在此基础上实现权利分离。但在权利对象的设定上,物权法思路时而将之确定为信息内容,如在个人信息与企业数据的生成关系与前后制约方面的论述,以及在企业数据库被分享或交易时企业对第三人利用信息的限制等情形下,将企业数据的利益定位为内容的排他性控制;时而又将之确定为数据形式,如企业数据在被他方超越权限爬取时,企业数据利益又被理解为企业对电子数据的技术控制。这两种指向对象的交替适用,使企业数据权益变成了一个在物理上具有固定的代码空间、在内容上又具有追溯力的强大权利,这种权利对信息的控制力度甚至远远超过传统法律对作品、隐私、商业秘密等特定信息保护的力度,也与网络作为公共媒体所应具有更快更利于信息分享的传播功能相违背。另外,物权法思路在将信息内容作为客体时,既不符合物权法对于客体稀缺性的要求,也无法将客体固定下来,甚至在私法上从未存在过将信息“物权化”的成功做法,能够在形式上确定的只能是平台控制的以比特形式存在的数据。因此,将企业数据作为纯粹数据问题看待,有效缓解了理论上企图将信息内容归于特定主体“所有”的乌托邦幻想,又可将企业数据问题还原为对企业自身控制的电子数据保护的事实,因为客观来说,只有在比特数字世界中,企业数据保护问题才是真实且可为的。

其次,将企业数据作为纯粹数据问题看待,才能将企业数据保护当作一个整体性的问题,而免受整体与局部关系的干扰。如果将信息内容作为企业数据权利来源,将不可避免地会遇到整体数据库和部分数据之关系的难题,比如企业数据内容被用户分享或第三方共享时,企业数据权益因内容的输出应该受到影响,但通常又认为此种情形并不影响企业数据权益的完整;^[18]又比如针对企业数据相当部分由收集到的个人信息组成的事实,依物权说主张,用户个人对其信息的“所有权”与企业对相应信息的“利用权”形成主次关系,但此时这种关系仅仅只是适用于部分涉及个人信息的企業数据,企业对其数据库中非个人数据的利益在此被忽视,如果认定企业对非个人数据享有所有权,则企业数据权益将变成部分所有权和部分用益权的大杂烩。^[19]另外,从对信息内容支配的角度来理解企业数据权益,还会遇到企业对其数据库中的公开数据享有何种权益这一问题,如果企业对此不享有信息上的权益的话,那么物权或财产权的主张就无法对整个企业数据权益作一个完整的定义和描述。因此,企业数据保护问题只有作为一个整体的问题对待才有意义,才使法律规则的探讨变得可能,根据信息的走向来探究企业数据利益,只会使问题变得支离破碎,且偏离解决问题的正常轨道。将企业数据作为整体来探讨,意味着企业数据保护问题不再与信息的来源、内容和流动直接相关,它无差别地对待企业所控制的电子数据,所有的数据分享同一个确定的局部代码空间,并且受到平等保护。

[18] 例如,在腾讯和今日头条的争议中,用户基于个人信息权益同样有权将其头像、昵称授权第三方使用,今日头条可因用户主动的提供行为重新将头像和昵称数据化,生成新的数据权利,但其不能在未取得腾讯的同意下,直接调取或通过抖音间接取得微信或QQ平台中的数据,因为后者侵犯了企业数据的完整性。

[19] 参见程啸:“论大数据时代的个人数据权利”,《中国社会科学》2018年第3期,第121页。

第三,将企业数据保护定位为纯粹数据问题,就可以将其作为电子网络领域的特定问题,并通过互联网的方式来解决。上文已述及,企业数据库早已以不同形式存在,但企业数据保护问题却是随着数字化技术的发展应运而生,说明该问题是派生于数字技术的原生问题,并没有脱离网络环境的普遍存在性。从信息内容控制角度进行的理论探讨,因其不适用于传统媒介的数据库,同样也不应适用电子数据库。只有将比特形式的数据和代码空间作为观察对象,才能使我们找到一个解决数据保护问题的立足点,美国学者莱斯格(Lessig)在其著作《代码 2.0——网络空间中的法律》中将代码(code)作为理解和解决网络问题的钥匙,这一点无疑也应适用于企业数据的保护。^[20] 企业数据保护并不一定涉及确认新的权利存在,正如汽车的出现改变了人们的出行方式,并催生了现代交通规则,电子数据改变了信息分享方式,也需要产生适用于互联网的数据分享规则。但是,正如交通规则并不涉及交通工具的权属一样,企业数据保护亦无须过于关注以电子形式存在的信息的归属,以互联网的方式解决企业数据应当成为企业数据保护的着力点。

关于企业数据保护问题的类型性质及其法律意义的分析,是研究企业数据利益形式和保护方式的前提条件,这是对企业数据问题的一个基础理论判断。在此前的理论研究中,学术界常将关注点置于信息流动的轨迹和结果上,并尝试用传统私权理论来制约信息的流动,一定程度上忽视了数字化技术本身也会产生独立的新问题,并对适用于这类问题的新规则的产生提出了客观要求。

三、企业数据利益的法律形态:有限的数据自我控制

目前网络经济已经进入“数据驱动型”时代,企业数据和公共数据的价值引起社会高度关注,企业数据的保护和政府数据的开放成为时下热点问题。同时,促进数据利用和保护数据权益构成各国数字经济战略的双重目标,如2020年2月欧盟委员会发布的《欧洲数据战略》,便以推动欧盟成为世界上最具吸引力、最安全和最具活力的数据敏捷型经济体为直接目标;^[21] 又如英国近期发布的《数字监管计划》即明确将保护创新、释放数字技术的巨大利益,同时将现在和未来的风险降到最低,作为该计划的宗旨。在此大背景下,社会对数据分享和数据安全两者的需求因同样强烈而处于一种空前的紧张关系,并考验各国在数据治理方面的智慧。如何理解和界定企业数据的利益形态,是一个无法回避的法律问题。

(一)企业数据利益的法律来源

企业数据的价值是对其进行产权干预的基础。企业数据的巨大利用价值和商业价值在数

[20] (美)劳伦斯·莱斯格:《代码 2.0——网络空间中的法律》,李旭、沈伟伟译,清华大学出版社2009年版,第138—141页。

[21] See European Commission, “European Data Strategy: Making the EU a Role Model for a Society Empowered by Data,” <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy>, last visited on 24 June 2021.

数字经济时代不言自明，目前社会都接受其作为一种生产要素具有鲜明的“资产性”，并存在商业估值的可能性。如有商业机构尝试以将“数据势能”概念引入公共数据的估值体系，强调数据的价值不在于建立其所依赖的成本，而是更多地体现为公众使用过程中潜在的社会和经济效益的逐步释放。^{〔22〕}这一理论也部分适用于企业数据，即大数据的价值释放是在社会的分享或利用过程中实现的，这也是企业数据商业价值的来源。大数据的这种价值实现方式充分体现了数据的充沛性原理，并以此与物权法的稀缺性背景相区分。但大数据价值主要通过分享来实现的特性，却直接与大数据的产权界定存在天然的矛盾，也给企业数据保护的法律基础的确定带来了理论上的困难。目前基于企业数据的价值而主张为其赋权成为企业数据保护的通行观念，这主要是考虑到企业为数据的收集和创建付出了成本（包括劳动和资金投入等），如若不对其进行保护而由他人搭便车自由分享，将损害企业经营大数据的积极性。这种将成本与产权直接联系的主张面临如下质疑：

首先，企业投入的劳动或资金是否与数据库的创建存在直接对应关系，是值得商榷的。除非是以汇编既有信息为目的的传统数据库，当代网络企业的相应投入并非指向企业数据，而是以构建有竞争力的平台运营模式为目的，在此过程中，数据的收集只是某种“副产品”，正如汽车的行驶并非只是为了获取“行车记录仪”的信息一样。事实上社会生活中的任何行为和事件都会产生信息，且通常都为“副产品”，在互联网出现前后，“没有任何法律原则要求，数据信息权利必须从一开始就分配给特定的法律主体。”^{〔23〕}事实上，传统社会中的无数人为收集信息付出了诸多努力，在法律上却从未出现过为其赋予某种信息权的尝试，单纯电子信息工具的进步并不能导致新的信息权利的产生。

其次，企业创建数据库并不代表企业能独占数据库的社会和经济价值。企业的投入只是收集了现实生活中的相关数据信息，而信息主要是生活事实的记录，它没有天然的“主人”，也没有起始的权利（信息私权除外），在这个意义上讲，为企业数据赋权会遇到与数据来源的关系问题。利用物权法的权能分离理论来解释此问题时，通常会强调信息来源方即用户个人的“所有权”，企业为数据的利用方，但在信息流动的情况下，用户对其提供给企业的数据真的享有“所有权”吗？如果用户提供给平台的信息既不为自身所创造，又是通过某种途径继受获得，那么就不能认定其为原权利人，原权利人的确定还得向信息源追溯；同样，企业从他方收集的数据可以由其他人分享，那么我们如何认定分享之后企业相对于分享人具有某种优越的地位，并以此制约分享人对数据的再利用和传播？因为从形式上来看，数据一经分享，企业和分享人之间对数据的掌控和处分的可能性没有任何差别，两者都是信息流动环节的一个节点，除非通过

〔22〕 参见《开放数据资产估值白皮书》，普华永道会计师事务所2021年7月10日召开的2021世界人工智能大会“数据新要素，转型新未来”论坛上发布，载微信公号“168大数据CDO研习社”，2021年7月4日上传。

〔23〕 Josef Drexler, Reto M. Hilty, Jure Globocnik, Franziska Greiner, Daria Kim, Heiko Richter, Peter R. Slowinski, Gintarė Surblytė, Axel Walz, Klaus Wiedemann: “马克斯·普朗克创新与竞争研究所就欧盟委员会‘关于构建欧洲数据经济征求意见稿’的立场声明”，刘维、张嘉莹译，《电子知识产权》2017年第7期，第92—100页。

自我约束,法律没有合理的理由通过排他性权利来区分信息流动中数据控制人之间的利益。

第三,信息的公共性特征决定了信息的价值实现以社会分享为常态,以法律控制为例外。信息的公共性特性表现在,信息与有形世界的资源不同,它只有在以分享为基础的社会场域中才有意义,单个主体对信息的绝对控制并不能达到信息交流的目的,最终的结果是既不能完全利己,又不能有效利他。信息在人类历史的绝大多数时间都是以互惠利他的方式来进行传播的,互联网技术的出现并不能改变信息传播的基本规律。故基于简单的成本、劳动或投入观念将信息赋予特定主体专有,是对信息公共性特性以及它所具有的强大社会“势能”的忽视,也可理解为对社会公共信息资源的“侵占”。除此之外,赋予企业数据专有权还会造成干扰经营自由和竞争自由的,以及阻碍其他依赖存量数据的市场参与者进行经营活动的风险,并对下游数据市场的发展产生负面影响。^{〔24〕}数据专有权会创造出一个影响竞争的市场壁垒,传统社会中信息天然具有的自由分享基因在网络上可能会被不当限制甚至消除。

关于企业数据利益的法律探讨,除了以成本为法律赋权理由外,尚有以信息权益和财产权益为代表的各种主张,上文已不同程度上都有涉及并进行了分析,在此不赘述。总体而言,理论界就企业数据的保护尚未形成适应数字化技术的有说明力的法律理由,诸多理由和主张都在信息提供、获得、控制和流通领域探讨企业数据利益的来源,并与个人信息保护、信息开放和数据安全等问题纠缠在一起,愈发增加了为数据确权的困难。如果我们将企业数据作为数字代码世界中产生的一个新问题,并将其作为一个纯粹的数据问题看待,那么企业数据问题将因不受信息内容的牵绊而变得简洁明了,且在规则确定和适用上更有成效。

(二)企业数据利益与企业有限的自我控制

从数字化技术对于信息的获取和交流角度来观察,企业数据问题属于数字技术的派生物,即比特形式的数据快速大规模聚集形成了巨大的数据池,并被平台企业实时控制。这种对信息的掌控方式为传统社会难以想象,因为传统社会信息的零散收集和获取依赖于独立的媒介,信息库的形成也依赖于存放媒介的物理空间。但正如传统信息获取并不导致信息归属问题一样,企业数据库的形成也并不必然与信息归属相关,而是信息集中后的应对问题。依照传统信息领域的“元规则”,即信息持有者享有保密和公开的选择权,企业数据的利益形态即为企业对数据库的自我控制。企业对数据的控制并非一项权利,它是一种法律事实,也是企业对信息处理方式进行选择的事实基础。法律对这种控制状态予以尊重和保护,并非基于财产因素,而是对信息自由的一种承认与尊重。这一点也适用于对传统信息持有者的保护,即除非个人自愿,无人能强迫信息持有者提供信息(公共利益除外)。依此而言,企业对数据的控制并不必然与财产利益相关,它可以基于自身的考虑,选择控制或公开自身获得的全部或部分数据,亦即企业数据对于企业是否构成一种正面利益,并不来源于企业对数据的控制本身,而是源于自身对数据处理方式的选择,如果公开分享数据对自己更有利的话,企业就会做出相应的选择。但企业对数据的自我控制成为企业做出选择的前提,法律尊重企业对数据的控制状态类似于物权法上的“占有”保护,故这种数据控制事实不能构成实体权利,只能作为一种防御性的“法益”存

〔24〕 同上注,第94页。

在,且在诸多情形下,这种事实控制也是相对有限的。对于企业数据的法益形态,可从下述方面来予以理解。

1.企业数据控制利益是一种相对较弱的利益,体现为一种非基于内容的有限排他权

企业数据利益主要是基于企业对数据的事实控制,上文提及的商业秘密保护则是基于特定信息内容的价值,故企业数据保护的力度应弱于商业秘密。有观点认为,虽然单个数据信息可能不构成商业秘密,但数据库因具有整体价值可能构成商业秘密。^[25] 但企业数据整体被他人非法获取的情形鲜见,另外在部分企业数据被他人非法获取时,是否构成侵害商业秘密就又成为问题。何况企业对其数据并不总是严加控制的,它总会释放部分数据由社会分享,这也与商业秘密强调保密的做法不同。就上文所介绍的数据库保护方式中,也可以发现法律对于非原创的、动态的电子数据集逐步摒弃了知识产权和特殊权利的保护方式,致使对动态电子数据库的保护在理论上仅剩下一个“空壳”,有学者称之为“有限排他权”,具体内容称之为“公开传播权”,这种判断从形式上看是合理的,同时更意味着从客体对象来为企业数据确权的失败。^[26] 企业数据利益的弱势表现并不意味着企业处于弱势地位,它只体现在企业对信息流动和分享过程干预的弱化上,与此同时,企业的信息处理自由和公开传播自由则是完整和充分的。

2.企业数据法益范围依赖于自身对数据的控制力度

企业依赖数据的自我控制来实现自身的数据自由和数据利益,意味着企业对数据控制的力度决定了其所享有自由和利益的大小。这种控制体现在技术控制 and 安全管理上,与传统信息库的控制原理相同,只是传统媒介构成的信息库主要依靠物理空间的隔离来实现,在技术创造和延伸上远不如电子数据库。平台企业在保护自身数据时,都会首先采取相应的技术措施来实现这一目的,有时也会基于公法目的(如个人信息或基础设施平台数据的保护)对数据施以更加严格的保护,同时也会通过数据安全管理制度建立来杜绝或最大限度地减少数据泄露的机率。企业的控制与数据安全是直接相关的,通常平台企业部分公开的数据或非经过特殊技术手段可以轻易获得的数据,则客观上已进入公共领域,无法获得法律的保护,这种保护上的局限可能会使平台企业倾向于减少数据的外部分享,同时努力将数据分享控制在自身服务器范围内,力求“数据不出门”。为了扩大企业对数据的有效控制,技术的创新和进步是首要的。如防爬安全技术、隐私计算技术、联邦学习技术、数据集多版本控制以及访问权限控制技术的开发利用,甚至运用区块链技术对于数据的分享进行跟踪控制,都使得对企业数据的控制手段和范围得以增强。^[27] 企业对数据控制所做的努力,旨在实现企业在数据被分享的同时,还能尽量保留其对数据的有效控制,将数据利用的效用最大化。

3.企业对数据的控制有可能产生数据“垄断”,国家干预和技术进步大有可为

基于数字化技术的特性,企业对于数据控制的规模超出想象,由此形成了头部企业在数据

[25] Drexl 等,见前注[23],第 95 页。

[26] 崔国斌,见前注[6],第 20 页。

[27] 程啸:“区块链技术视野下的数据权属问题”,《现代法学》2020 年第 2 期,第 120—131 页。

控制上的“垄断”优势地位。这种“垄断”地位阻止了新的市场参与者获取既存企业数据,又使得头部企业缺乏动力授权新的竞争者访问自身数据,当这种累积达到影响竞争和创新的程度,强制性数据访问的监管就会产生。如《欧盟运行条约》第101条就为市场参与者获得访问权限提供了竞争法上的依据,但设置了严格的条件。^[28]当然,采用竞争法干预方式会遇到诸多不确定因素的影响,很难作为常规方式来干预企业数据的访问,但不排除未来会通过企业数据访问规则的立法来限制企业对大数据的垄断性占有。同时,对于原始数据垄断的破除也在尝试中,欧盟《一般数据保护条例》第20条关于数据可携带权的规定即为其例。除此之外,以技术方式打破企业对数据的“垄断”已成为一个新的领域,如2019年万维网创始人蒂姆·伯纳斯·李(Tim Berners-Lee)直陈互联网的垄断已经使“长尾效应”失效,大公司形成数据孤岛,个人和社会失去了对数据的控制权,他提出了一个“Solid”技术解决方案,以强化用户对个人数据的控制。^[29]同样,目前网络业界也在尝试建立基于区块链技术的去中心化大数据开放社区,使用户可以上传共享自己的数据来获得收益,通过用户自己控制个人数据,可以打破数据垄断,使个人或普通企业通过极低的成本就能获得大数据应用价值。

上述对于企业数据控制利益的分析 and 理解,贯穿着一条矛盾主线,即企业数据的控制和分享之间的矛盾。就企业自身利益而言,数据的价值需要通过交易或互享来实现,但同时数据的控制就会被动摇;数据的控制是企业数据利益的基础保障,但同时数据的流动就会受到抑制。这种矛盾映射到社会层面也会体现为企业和公众之间的利益冲突,即强调企业对数据的控制利益,会减少社会参与分享数据的机会,形成数据壁垒甚至“垄断”;采用政府监管和干预来强制他人访问或强制数据公开,又会导致数据基本占有秩序的破坏。总体而言,企业对数据的控制享有的只是一种有限的自我控制利益,它追求企业在控制数据上的自身利益的平衡,以及企业和社会之间的利益平衡,随着网络行业的发展,这种平衡一直处于动态调整中。

四、企业数据的法律保护模式

企业数据的利益源于对数据的事实控制,决定了企业数据的保护主要依赖于自我防护,即强化对自身数据的有效控制,这也是传统信息控制的基本方式。在此基础上,法律将这种控制状态作为一种新型的“法益”予以适度保护。在此基础上,由于企业数据缺少传统信息私权或财产权等绝对权的利益外衣,不再适用传统绝对权请求权中回复性的保护方式,这种保护方式

[28] Inge Graef, Thomas Tombal, and Alexandre de Streel, *Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law* (November 27, 2019), TILEC Discussion Paper No. DP 2019-024, Available at SSRN: <https://ssrn.com/abstract=3494212> or <http://dx.doi.org/10.2139/ssrn.3494212>, last visited on 20 August 2021.

[29] 参见 Deep Tech:“互联网要推倒重来!长尾已死,数据垄断”,载搜狐网,http://www.sohu.com/a/290315855_354973,最后访问日期:2021年7月3日。“Solid”技术解决方案即将用户数据储存在自己的 Solid POD上,而非互联网公司的服务器上,个人数据可以通过新的标准化协议,并且使用相同的全球通用的 Solid API,在不同的 APP 连接使用。

对于以事实控制为利益表征的企业数据利益来说,并没有实质意义。因为企业数据利益并没有固定的客体或以信息内容为支撑的利益支点,数据一经扩散,传统财产法上的恢复原状或返还财产方式已无适用的可能。对于预防性的绝对权请求权如停止侵害、排除妨害、消除危险等方式,尚有适用空间,但在网络特有的虚拟环境下,上述请求的适法判断并不易实施,其判断因素内化在企业数据风险预防和控制措施体系中,且大部分为网络或数据安全规则所吸收。依上文所述,由于数据控制状态并不必然体现为实际利益的类型,只是为企业各种实际利益的实现提供一个基础或可能性,故在保护企业数据时将依实际利益被侵害的类型,存在不同的保护方式。具体可分为侵权法、合同法和竞争法保护模式,以下分述之。

(一)侵权法保护

侵权法保护模式是企业数据保护的基本方式。在企业数据没有法律权利外衣的情形下,侵权法通过“法益保护”模式可以有效实现数据保护的目。私法上“法益保护”与“权利保护”的区别首要在于被侵害的对象是否属于法定的、类型化的权利,此外这种区别还在于适用法律的不同和损失性质的差别上。^[30] 企业数据属于非权利化的法益,依大陆法系法益保护原理,应适用相应的“保护性法律”,即以保护他人为目的的法律,同时应将法益被侵害所致损失作为纯粹经济损失来认定,由受害人向侵权人主张赔偿。对企业数据侵权法保护所适用的“保护性法律”,包括以保护企业和用户安全控制数据的相关法律,如《网络安全法》《数据安全法》《个人信息保护法》当中有关企业数据安全的规则,还包括我国《刑法》第 285 条、《电子商务法》和《电子签名法》当中的有关企业数据安全的规定等。这些法律以公法为主,私法一般不直接涉及,除非数据之上存在隐私或知识产权这些特定信息。随着网络行业的发展,行政监管机构也会对企业数据的访问或公开做出规定,相关规定也将构成侵权法适用的对象。实际上,跟企业数据保护直接相关的应该是数据访问规则,因为目前大多数企业数据纠纷都与他人的不当访问相关,但目前关于数据的访问并没有统一的立法或制度来保障,而是由平台企业自身制定规约来指引,基于访问规则在企业数据保护上的重要地位,数据访问规则日益引起社会和立法界的重视,未来有可能通过立法建立数据访问的基本规则,或通过监管机构对企业的访问规约进行指引。

通过访问规则保护企业数据目前仍处于探索阶段,对于访问人的不当访问行为是否构成侵权行为,包括最具代表性的爬虫技术是否构成侵权,一直存在争议,^[31]其中以美国在适用《1986 年计算机欺诈与滥用法》(CFAA)上体现最为充分。CFAA 对未经授权或超过权限访问计算机早期的认定标准是,网站发表“限制访问”的明确声明或网站在使用条款中明确禁止网络爬虫。^[32] 但其后在 *Craigslist Inc. v. 3Taps Inc.* 和 *Facebook, Inc. v. Power Ventures* 案

[30] 参见朱虎:“侵权法中的法益区分保护:思想与技术”,《比较法研究》2015 年第 5 期,第 44—59 页。

[31] 对该问题的体系性研究,参见许可:“数据爬取的正当性及其边界”,《中国法学》2021 年第 2 期,第 166—188 页。

[32] 《1986 年计算机欺诈与滥用法》(CFAA)第 1030(a)(5)(A)(2008)条是美国规制数据爬取的主要条款。根据该条,“未经授权”故意访问计算机或超过授权访问权限,从任何受保护的计算机获取信息或者“故意造成程序传输,并且对未经授权且受保护的计算机造成损害”均构成违法行为。

中,法院又否定了“使用条款”可以触发 CFAA,同时明确了在有禁令信或技术手段(cease-and-desist letter and IP blocking measures)情形下,才构成“未经授权”。2017年的 hiQ Labs, Inc. v. LinkedIn Corp 案又有大幅反转,法院认为爬虫公开信息不构成 CFAA 意义上的“未经授权”或“超出授权”行为,事前的“使用条款”、事后的禁令通知、实施 IP 封锁技术都不再有效。^[33] 这种对爬虫行为性质认定的转变反映出企业数据保护的复杂性和微妙性,即企业数据虽然由企业暂时控制,却关涉到公共利益和信息自由,美国法院甚至认为数据的分享与言论自由相关。侵权法对数据的保护不能忽视这一背景,但在我国现有的爬虫抓取数据的案件中,法院多认定为爬取行为为不法行为,以不正当竞争规则对其进行责任追究,甚至追究当事人的刑事责任。除了爬虫行为外,在其他不当访问行为的认定中,除了坚持获取的是非公开信息外,还应将企业是否采取了足够的安全防护措施作为侵权行为认定的必要条件。

(二)合同法保护

合同法对于企业数据的保护主要体现在两个场景:一是数据分享合意;一是数据交易。数据分享合意的典型形式即是通过“开放应用端口”(API)进行的数据共享,数据交易则是企业之间通过约定或通过数据交易所进行的数据交易行为。API 数据共享是双方约定相互开放应用端口进行的数据分享形式,双方基于合意就互享的形式和权限达成了一致。合意分享方式在实际中的纠纷大多来自于共享方超越权限获取对方信息的行为,如 2016 年“新浪微博诉脉脉不正当竞争案”,以及 2019 年腾讯就“微信昵称、头像、好友关系链数据”诉抖音、多闪不正当竞争案等。^[34] 对于超越约定权限获取共享方数据给对方造成的不利,上述案例中当事人均选择通过不正当竞争规则来主张救济,并没有选择合同保护方式。数据交易形式目前处在探索和发展过程中,自 2015 年贵阳数据交易所建立以来,通过各类交易所成交的数据量并未如预期般形成爆发之势,其中针对数据的易于流传性和及时分享特征所做的交易安排,应当有别于传统存量资产的交易方式,并构成交易所设计的交易构架的重要部分,作为交易关系法定形式的合同也应纳入交易保障的体系。

从合同当事人的角度客观分析,合同法保护方式并非首选项,其原因在于:一是违约损害很难确定和计算。如上述案例中的越权分享行为即使被认定为违约,也无法确定损害(包括直接损失和间接损失),因为简单的数据分享行为并不一定导致现实确定的损害,并形成直接因果关系;二是违法责任的追究并不能阻止数据的分享或再流通,尤其对于数据交易市场而言,防止交易相对人获得数据后再传递给第三人是当事人关注的重点。对于违约损害难以确定的问题,合同法提供了相关途径比如违约金制度来解决。至于如何制约数据受让方不再与第三人分享的问题,其蕴含的立场是值得怀疑的。除了带有信息“原权”的数据(如隐私和作品等),其他数据一经分享即脱离原有控制人进入流通领域,这是由信息流动的“元规则”决定的,在法

[33] See *Craigslist Inc. v. 3Taps Inc.*, 942 F.Supp. 2d 962 (N.D. Cal. 2013); *Facebook, Inc. v. Power Ventures Inc.*, 844 F.3d 1058 (9th Cir. 2016); *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985(9th Cir.2019).

[34] 参见深圳市腾讯计算机系统有限公司、腾讯科技(深圳)有限公司商业贿赂不正当竞争纠纷,天津市滨海新区人民法院民事裁定书,(2019)津 0116 民初 2091 号。

律上企图强制性地要求经过交易已由相对人掌握的数据不再流动,在法律上并不具有可行性,原因在于:一是在数据交易后相对人获得了对数据的完全控制状态,这种状态与原控制人并无两样,也不可能形成某种从属的权利关系,受让方享有信息传播自由;二是数据交易并非排他性的财产交易,它本质上是一种信息服务,且可同时与多方交易,另外交易达成后原数据控制方的信息控制并不受影响。合同法可以通过保密条款来设定交易双方的利益分配,这属于意思自治范畴,理应受到法律承认和保护。至于如何避免数据分享人擅自将数据再行交易,除非原数据控制人能够通过现实技术阻止数据再次分享,否则数据将进入公共市场流通,并形成涟漪效应,原数据控制人处在与分享人同样的地位,通过改进信息服务、提升数据质量和研发数据产品等来实现企业数据的价值。

(三) 竞争法的保护

通过竞争法保护企业数据目前成为企业首选项,原因如上文所分析,这种方式可以有效地确定法律依据和损害的范围。竞争法保护分别体现为反垄断和反不正当竞争两种方式。数据“垄断”是由2019年“菜鸟—顺丰”事件引发的现实话题,近来又有公众提出对知网“垄断”的质疑。^[35]但数据垄断的概念并不清晰,通常可以在多个意义上被使用。比如它可以从数据由单个主体独占而拒绝共享的角度使用,也可以从企业自行控制数据而不受用户制约角度理解,还可以从企业独占数据收益角度来阐述等。但从反垄断法角度理解就复杂得多,因为一般意义上的数据独占并不构成竞争法意义上的垄断,数据的独占是否带来市场支配地位,不宜一概而论,应结合市场占有率、市场进入壁垒等相关因素进行综合考量。^[36]除非在替代性较弱的产品和服务上,存在一方所获取数据为另一方进入相关市场的基本前提情形,此时数据控制者的数据因符合“必要设施原则”基本要求,必须承担开放使用该设施的义务。另外,在企业拒绝开放数据时也应当区分是否因数据本身导致垄断,即使在由数据拥有导致的垄断情形,还须判断其行为是否构成滥用市场支配地位,或者是否还存在其他正当理由。^[37]由此,通过反垄断法强制公开数据的适用条件非常严格,一般情形下对于数据的公开贡献甚微,现实生活中存在更多的则是因企业对于数据独占使用而无法为社会分享的困难。

现实中反不正当竞争的运用频率要明显高于反垄断法。但现有的《反不正当竞争法》对于数据行业的规定并没有多少针对性的规则,只在第12条和第6条有一定的涉及,且集中在网络应用合法状态的维护上,几乎不涉及数据的无序竞争问题。^[38]基于此,司法裁判主要聚

[35] 参见孙晋、钟原:“大数据时代下数据构成必要设施的反垄断法分析”,《电子知识产权》2018年第5期,第38—49页。

[36] 参见丁晓东:“论数据垄断:大数据视野下反垄断的法理思考”,《东方法学》2021年第3期,第108—123页。

[37] 比如,在反垄断法领域,证成反垄断干预的主要方式就是以竞争损害作为认定垄断行为的效果要件。参见兰磊:“论垄断行为分析模式的配置逻辑”,《经贸法律评论》2021年第2期,第47页;叶明、张洁:“数据垄断案件的几个焦点问题”,载《人民法院报》2018年12月6日。

[38] 参见张建文:“网络大数据产品的法律本质及其法律保护——兼评美景公司与淘宝公司不正当竞争纠纷案”,《苏州大学学报(哲学社会科学版)》2020年第1期,第44页。

焦在《反不正当竞争法》第2条的适用上,并通过个案逐渐发展出了一些实际的适用标准。如通过“山东食品进出口公司诉青岛圣克达诚贸易公司”不正当竞争案,最高院确立了适用第2条的三要件:即法律对该种竞争行为未做出特别规定;其他经营者因该行为受到实际损害;该竞争行为违反诚实信用原则和公认的商业道德而具有不正当性。^[39]此三要件也适用互联网领域,并在其后的360公司和腾讯的“扣扣保镖案”以及奇虎公司和百度的“百度插标案”中,法院分别提出了“正当商业模式”观点和“非公益必要不干涉”原则。^[40]对于数据的不当利用的判断,在“汉涛诉爱帮”案中,法院认定爱帮网对于特定网站信息的利用造成了市场替代的后果,故构成不正当竞争。^[41]在“新浪微博诉脉脉案”中,法官对判断是否构成反不正当竞争的行为的标准又进行了细化。^[42]上述通过个案在运用《反不正当竞争法》第2条时发展了一些适用标准和方法,总体上遵循“道德标准”和“客观效果”并重的考量方式,对行为的违法性认定有着积极的意义。总体来看,采用竞争法来保护企业数据缺乏普通性,竞争法不太关注企业行为的适法问题和不法行为的责任追究,而是着重判断企业的竞争利益是否受到损害,故在竞争利益受到侵害时,竞争法具有不可替代的作用。

五、结 语

上文关于企业数据权益的基本理论分析和判断,是对企业数据利益问题在法律上所做的一个系统的、整体的理论尝试,这只是问题讨论的开始,随着网络行业实践的深入和数据纠纷的充分展现,学界对于该问题在法律上的理解将会更为全面和丰富。目前人类处在大数据时代的开始和人工智能的前夜阶段,数据的分享并没有过剩,而是正当其时。数据的汇聚释放了数据的威力,并对更高的数据分享提出了要求,这个过程节奏会逐步加快,促使人类向全息社会迈进。尽管在理论上数据的分享是前提性的,在现实生活中基于数据收集和处理的相对区隔,数据的分享仍然存在各种现实因素的制约,尤其是当政府或网络企业的利益与数据开放形成冲突时,数据分享就不再是自然而然的了,它需要法律予以促进和保障。与此同时,出于数据集中在少数人手中并被可能用来操纵公共生活的担忧,国外互联网领域的学者对数据的公有化提出相关设想,呼吁应当通过立法要求社交媒体平台捐赠数据以用于公益事业,对于私

[39] 参见山东省食品进出口公司、山东山孚集团有限公司、山东山孚日水有限公司与马达庆、青岛圣克达诚贸易有限公司不正当竞争纠纷案,《最高人民法院公报》2009年第9期。

[40] 参见百度在线网络技术(北京)有限公司等与北京奇虎科技有限公司等不正当竞争纠纷,北京市高级人民法院民事判决书,(2013)高民终字第2352号。

[41] 参见上海汉涛信息咨询有限公司与爱帮聚信(北京)科技有限公司、爱帮聚信(北京)信息技术有限公司不正当竞争纠纷,北京市海淀区人民法院民事判决书,(2010)海民初字第24463号;上海汉涛信息咨询有限公司与爱帮聚信(北京)信息技术有限公司不正当竞争纠纷,北京市第一中级人民法院民事判决书,(2011)一中民终字第7512号。

[42] 参见北京微梦创科网络技术有限公司与北京淘友天下技术有限公司等不正当竞争纠纷,北京市海淀区人民法院民事判决书,(2015)海民(知)初字第12602号。

人平台控制的公共数据,可以将其传递给公共机构,扩大数据在社会的非营利用范围。如英国学者尼克·斯尔尼切克(Nick Srnick)基于平台资本主义正在形成不可撼动的垄断,激进地呼吁将谷歌、脸谱网和亚马逊“国有化”的必要性,认为在人工智能已经贪得无厌地吞食社会数据时,提早对这些数据基础设施进行控制,是控制未来社会风险的必要举措。^[43] 数据最终社会化并不是一个不可能发生的结果,因为公司有其生存寿命,数据则有永续性,未来的数据归属无疑会向社会化迈进,这只是时间问题。基于数据的社会公共品属性,探索未来数据社会化控制和分享的具体方式,将成为日后的现实课题。

Abstract: How to allocate and protect the enterprise data rights and interests in law is a theoretical problem in the current Internet law. The existing theory protects them according to the traditional private law rules, mainly by incorporating them into the legal framework of statutory rights from the perspective of information private rights and property rights. The “database protection” and “trade secret protection” rules in information private rights are similar in form to enterprise data protection, but they are fundamentally different in substantive interest and coverage, which leads to the failure of “information content protection” orientation. The problem of enterprise data protection arises from the popularization of the Internet and is only meaningful in the context of digital technology. Therefore, it must be considered against the background of distinguishing information problems and data problems, and enterprise data rights and interests should be conceptualized as a pure data problem as a whole, enterprise data property theory is difficult to be constructed for the uncertainty or non-existence of its object. In terms of interest form, enterprise data is the limited self-control of data. The legal interests contained in this factual control are essentially embodied as freedom of information. For this reason, the protection of enterprise data should be granted through the maintenance of data control, and the various practical interests that may be involved in the competition for data control can be protected through tort law, contract law and competition law.

Key Words: Data Rights and Interests; Database; Information Private Rights; Data Control; Pure Data Problem

(责任编辑:贺 剑)

[43] See Nick Srnicek, “We need to nationalise Google, Facebook and Amazon. Here’s why”, <https://www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest>, last visited on 30 August 2021.