

从创设型机制到支撑型机制： 数字时代信息财产法律保护的范式转型

张浩然

摘要 与有体财产不同,信息财产的法律保护机制遵循着秘密—公开信息的二分,仅秘密信息可通过保护对客体的事实控制来保障利益实现,即支撑型机制;公开信息则主要依靠法律创设排他性权利加以保护,即创设型机制。受限于权利法定原则,创设型机制需因应技术进步不断作出调整。伴随着数据成为新生产要素,国内主流观点主张在数据之上设立新的排他性权利,美国、日本等国的数据保护实践却选择对支撑型机制进行扩张,基于企业对数据的事实控制建构保护制度,这为信息财产保护提供了新范式。在数字环境下,信息与其含义、主体及物理载体逐渐分离,企业对信息的私力控制范围进一步拓宽,支撑型机制适用范围扩张,且相对于创设型机制更具效率优势,传统秘密—公开信息的二分方式已不再适用。为弥补技术变革环境下法定知识产权僵化和滞后的缺陷,应构建更具包容性和现代性的支撑型机制,在商业秘密制度基础上建立合法控制信息保护制度,对向有限主体提供、采取相应控制措施并因此具有商业价值的信息,禁止他人未经许可的获取、利用、公开行为。

关键词 信息财产;知识产权保护;数据要素市场;数据财产权益;商业秘密;秘密—公开二分法;私力控制

中图分类号 D923.41 **文献标识码** A **文章编号** 1672-7320(2024)01-0078-12

基金项目 国家社会科学基金青年项目(23CFX025)

进入数字经济时代,数据成为新一类生产要素,关于数据财产权益的法律保护,已成为立法、司法以及法学理论界热议的话题之一,民法、刑法、经济法等不同学科的学者从各自视角进行了探讨,提出了一系列数据财产权利模型,却难以达成一致。从客体来看,数据是以电子或其他方式对信息的记录,信息是事物存在方式或运动状态的反映,与物质、能量并列为客观世界的三大组成元素,既包括表达人类可理解含义的语义信息,也包括特定符号代码组合的句法信息,数据本质上属于信息的范畴^[1](P114-116)。18 世纪后,伴随着信息独立于有体物成为一类独立的财产形态,知识产权制度即将信息作为保护对象并发展出了独特的调整范式,至今成为信息财产保护的专门制度。面对数据问题对既有立法形成的挑战,除考虑如何建立新的数据保护制度,在知识产权学科内部更为重要的是检讨传统信息财产保护范式对数据保护存在的局限及原因,从而面向数字时代的信息财产保护进行体系性制度完善。因此,本文将数据保护问题为切入点,首先厘清信息财产保护中支撑型机制和创设型机制两种范式及区分适用规则,进而考察比较法实践突破传统区分适用规则,扩张支撑型机制保护数据的制度趋势,厘清其理论基础和效率优势,最后对支撑型机制和创设型机制的区分适用规则进行重构,为数字时代的信息财产保护制度完善提供建议。

一、传统信息财产保护的二重范式及适用规则

在调整民事主体对物之控制、开发、利用的法律关系中,法律一般通过授予某人优先地位而排除他人干涉,主要依两类标准界定权利:一是建立在人与物之间事实关系的基础上给予保护;二是不考虑人与物之间的事实关系,而基于法律认可的原因授予一种“资格”进行保护^[2](P3-4)。在有体财产保护中,前者为占有保护,后者为所有权制度。信息财产保护同样遵循这两种路径。具体而言,在经济学意义上,信息财产的法律保护立基于经典市场失灵理论,即由于信息的公共物品特性而容易被“搭便车”利用,有必要保护市场主体对信息成果的产权而恢复市场竞争过程。产权指的是个人通过交易直接或间接地实现资产价值的能力,既包括通过私人力量建构的产权,又包括法律承认和保护的权利^[3](P3-4)。当私力建构的产权不足以发挥作用时,则需要法律介入,依照前两种路径划分,存在两种介入方式:其一,在私力建构产权基础上提供补充保护,从而恢复市场的自律性作用,典型如商业秘密制度;其二,当私力建构的产权无法发挥作用时(如信息利用存在隐匿困难),有必要人为地创设一种对于成果开发具有激励作用的制度设计,典型如版权、商标、专利等知识产权。按照日本学者田村善之教授“市场指向型知识产权法”理论的划分,前者为支撑型机制,后者为创设型机制^[4](P10-16)。

此两种路径在信息财产保护中的作用方式相较于有体财产存在较大差异:第一,有体财产保护存在两种路径的混合,即同时存在占有和所有权保护,信息财产保护则因秘密—公开信息不同而存在适用的二分,即由于信息具有无形性、传播性和共享性特点,一经公开传播便会成为社会共识,很难通过物理控制来保护其不被盗用,因此立法较少地适用支撑型机制,只有秘密信息可通过商业秘密制度保护,大多数可被公开的信息只能通过建立排他性的知识产权加以保护(以下简称“秘密—公开二分法”)。第二,有体物之上利益实现的基础在于对物的排他性控制,故而适用两种路径导向的权利构造相似,均体现为对物的排他性支配的权利,信息财产保护则产生了两种截然不同的保护范式。一方面,商业秘密制度与有体财产占有保护类似,均保护对信息事实上的排他性控制及利用,同时并不妨碍其他主体开发相同信息,制度设计相对简单而保持稳定;另一方面,信息之上创设排他性权利与物权所有权存在显著不同,由于信息的传播性和共享性特点,无法通过普遍地保护对客体的排他性控制来确保利益实现,不得不采用“客体共享,利益排他”的复杂制度设计:首先,将客体占有与收益、使用、处分相分离,允许信息在全社会共享,并根据信息的商业化利用方式设定排他性权能,形成组合的“权利束”^[5](P139);其次,由于在信息之上对世性地设定排他权利,必将排除其他所有人对信息的获取而威胁公共利益,这要求财产权授予客体必然要以一定创新性高度为阈值条件,权利保护设定特定期限,以及因公共利益设定权利限制和例外平衡。同时,创设型机制不可避免地存在其僵化性和时代局限,科技进步不断催生新的信息客体形式和利用方式,立法创设的知识产权受权利法定原则限制,保护周延性、有效性不断面临着冲击,需遵循着“技术革新—法律变革”的历史周期率不断进行调整。

进入数字时代,伴随着数据价值的凸显,这一经典命题再次出现,传统知识产权制度无法为数据集提供恰当保护,其保护制度构建同样面临着支撑型或创设型机制的二元抉择。国内学界提出了一系列排他性权利模型,但在全球实践中,除1996年欧盟确立了对传统数据库的财产权保护,并没有国家创设新的排他性权利保护数据,美国、日本、韩国等国家均选择采用支撑型机制,基于企业对数据的事实控制建构保护制度。然而,相关实践未在国内理论探讨中产生广泛影响,少数学者从完善数据保护制度的角度介绍了相关立法^[6](P69-80),侧重于规则本身的研究借鉴,并未关注其背后理论基础及保护范式的转变,导致依此建构的数据保护制度存在不同法律逻辑的杂糅。

事实上,数据保护由创设型机制向支撑型机制的转变对知识产权法整体都具有范式革新意义,因为过去一直遵循着秘密—公开二分法的共识,认为商业秘密只保护秘密信息而不延及公开信息,一般信息只能通过设定排他权加以保护,这决定了知识产权难以像传统物权那样提炼出相对抽象而普适的权能

制度,适应不同技术形态形成了杂乱无章、不断变换的权能体系。如果可以突破秘密—公开的二分,一般性地基于私力控制建立保护制度,而无论数据公开与否,将带来支撑型机制适用范围的实质扩张,为数字时代信息财产保护提供新的范式选择。因为与创设型机制的不同之处在于,支撑型机制采取的是类似于有体财产保护的 mode,以私力控制为基础辅之以法律保护,提供了私人力量与法律之力合作共治的空间。技术变革不断对国家立法的调整能力提出新的挑战,同时带来了私人力量的空前发展。面对技术进步带来的挑战,支撑型机制将首先交由企业私力措施应对,在此基础上构建法律补充保护。这有望为纷繁复杂的技术问题寻求简单通用的法律解答,避免创设型机制下法定知识产权不断过时的历史周期率。基于此,本文将进一步探索完善支撑型机制弥补知识产权法定缺陷的可能。

二、数字时代支撑型机制的扩张适用

面对数据保护的现实需求,在现有制度体系中,尽管版权、专利等知识产权制度难以为数据提供恰当的定位和保护,但数据生产、流通仅存在“有限市场失灵”,目前对数据产权主要有两方面的保护:其一,在事实层面,绝大多数数据集合生成后处于企业事实控制之下,企业可通过技术措施排除他人获取,对数据建立事实上的产权,不过仍面临着数据被不法入侵以及因公开、流转后失控的风险;其二,在法律层面,对处于事实控制之下的数据,商业秘密制度可为企业私力控制提供进一步法律保护,这也是目前数据集合保护的主要制度之一。同时,由于遵循着秘密—公开的二分,将商业秘密作为主要的数据保护制度存在较强局限性:一方面,数据不仅包括非公开数据,还包括公开数据,有的数据价值实现是以用户公开访问为前提,则无法获得保护;另一方面,对于非公开数据,数据价值最大化在于流通共享,如果数据持有者大规模共享数据,将可能导致数据丧失秘密性而无法获得保护,这会对数据流通共享形成较大限制。面对这“有限的市场失灵”,国内多数学者倾向于采取创设型机制,提出了一系列排他性权利模型,包括“数据资产权说”^[7](P63)、“数据用益权说”^[8](P116)、“数据公开传播权说”^[9](P20)、“数据块权利说”^[10](P92)等。

形成对比的是,在实践中,美国、日本等国家选择对商业秘密制度进行改造,构建一种“类商业秘密制度”保护数据集合:

在美国法上,虽然知识产权制度在理论上可为数据提供部分保护,实践中却并未被广泛主张和适用,而是主要适用规制计算机入侵制度。具体而言,1986年为规制黑客入侵行为,美国国会类比普通法的侵入土地制度制定了《计算机欺诈与滥用法》(CFAA),其中第1030(a)(2)条规定禁止计算机入侵行为,即未经授权、超出授权故意访问受保护计算机并获取内部信息的行为,计算机所有者对此有权要求禁令救济和损害赔偿,这赋予了其排除他人未经允许访问其计算机以及获取内部信息的权利。在网络环境下该制度逐渐发展成为商业秘密保护的替代和扩张性机制^[11](P289):相对于商业秘密制度,CFAA的保护要件更为宽松,仅要求所有者排除或者限制他人对其计算机系统的访问。比如,在hiQ诉领英案中,法院明确该要件要求对网络空间访问设置代码或技术措施限制(hiQ Labs, Inc. v. LinkedIn Corp, 938 F.3d 985 [9th Cir. 2019])。按照此要求,受保护信息并不需要满足严格的秘密性、保密性和价值性要件,公开数据通过施加技术手段限制访问也可获得保护,数据收集者不必担心数据因广泛交易利用而进入公有领域。在保护效果上,CFAA禁止一切未经授权、超出授权访问计算机并获取信息的行为,类似于商业秘密制度排除他人未经许可获取、利用、披露商业秘密信息的宽泛效力。伴随着信息存储的数字化,大多数商业秘密案件都涉及计算机访问从而可以适用CFAA,后者更具保护周延性和诉讼效率上的优势,因此CFAA成了网络环境下保护商业秘密的主要方式。对他人未经允许的数据获取行为,实践中也主要通过此“类商业秘密制度”加以规制。

日本是全球为数不多的通过专门立法保护大数据的国家之一,其在立法之初曾考虑客体保护和行为规制两种路径,前者着眼于在数据之上创设排他性权利,以欧盟《数据库保护指令》中的特别权利制度

为典型;后者侧重规制不当利用行为,以商业秘密制度为典型。由于赋权路径可能阻碍对数据的合理利用,日本最终选择了行为规制。同时,考虑到商业秘密保密性要求与数据分享利用存在冲突,2018年《日本不正当竞争防止法》对商业秘密制度加以改造,构建了专门的“限定提供数据”制度。所谓“限定提供数据”,是指作为营业向特定对象提供、累积到一定规模并通过电磁方式存储并且加以管理的与技术或经营相关的信息。对比商业秘密制度,二者的相同之处在于,保护对象都是与技术或经营信息,都禁止他人未经允许的获取、使用和披露行为。不同之处在于,“限定提供数据”的构成要件由商业秘密的保密性、保密性、价值性发展为有限提供性、相当累积性和电磁管理性:相当累积性要求客体为“相当大的数量”积累而产生价值的数据,这应当是价值性要件在数据领域的体现,二者并无本质不同;相应的保密性或电磁管理性要件均旨在为维持信息的秘密性或有限提供性状态;最为根本的改变是保护对象由不为公众所知悉的秘密信息扩张到了向有限对象提供的信息,将半公开乃至公开数据都纳入保护范围,弥补了秘密—公开二分法的局限。

尽管因循不同路径,美国、日本建立了基本相同的数据保护制度,二者都突破了商业秘密仅保护秘密而不保护公开信息的限制,对事实控制之下的信息提供保护,也为数字环境下商业秘密本身的完善提供了新的可能。那么,相关制度对我国数据保护实践是否具有可借鉴意义?笔者认为,有两方面问题尚待考察:第一,传统商业秘密保护受限于秘密—公开二分法,这也是其仅能够为部分数据提供保护而无法成为一般性机制的主要原因,鉴于美国、日本等国家的实践探索,需检验数字经济环境下秘密—公开二分法是否仍然适用;第二,如果存在完善支撑型机制为数据提供一般性保护可能,由于创设型机制同样具有纠正市场失灵的功能,需确定二者相对效率优势而作出最优立法选择。

三、数字时代秘密—公开二分法之检视

在商业秘密制度发展史上,伴随着其理论基础由合同转向财产理论,秘密—公开二分法即已产生并长期存在。19世纪后期,普通法法院主要类比财产权制度构建商业秘密制度,即由于占有是财产权取得的前提,要取得财产权,必须建立对物的排他性控制并体现其个人所有的意图;对信息建立财产权保护,权利人同样要占有该信息。由于信息难以像有体物进行物理上的控制,占有信息排除他人干涉的唯一方式就是保密,只要信息通过保密不为公众所知悉即可获得财产权保护,一旦公开所有权利均宣告终止(Bristol v. Equitable Life Assurance Soc., 132 N.Y. 264, 30 N.E. 506. [1892])。时至今日,一般仍然认为信息具有共识性特点,一经公开即不胫而走便成为社会共识,任何人都可以无限地复制和利用^[12](P91)。基于此,两方面原因导致公开信息无法成为受商业秘密保护的财产:一是可被无限复制利用的信息不具有稀缺性,不具备价值性而没有保护的必要;二是对已经作为社会共识进入公有领域的信息,很难将其从公有领域剥离作为私有财产,否则将产生过高的社会成本。

然而,历经百年之后秘密—公开信息的二分是否仍然有效尚值得检验。从传播学来看,信息传播包含信源、信息、信道、信宿四项基本要素,基本传播过程是信源将信息编码,经由信道传递给信宿,信宿将信息解码的过程^[13](P20-48)。自19世纪中期商业秘密制度产生至今,人类经历了第四次信息技术革命向第五次信息技术革命的跨越,信道即传播媒介经历了由书籍、报刊、广播、电视向信息技术以及数字技术的转变,信道变化带来了其他三项要素的改变。在传统环境下,信息传播往往是人与人之间语义信息的直接传递,依附于有形载体并以载体转移为基础,信息一经公开便不胫而走成为社会共识的描述无疑是恰当的;进入信息网络时代,传播主体(信源、信宿)、传播内容(信息)、传播媒介(信道)都经历了颠覆性改变,这也对法律规制的对象、手段提出了新的要求。德国学者蔡希(Zech)将此界定为信息剥离(Abstraktion von Information)现象^[14](P167),即信息逐渐与其物理载体、人类创造者、接收者以及特定含义相剥离,既有法律体系中以人为主体、以物理载体为对象的界定和规制方式已经失去作用,而应当寻求新的规制基础。秘密—公开二分法也应置于此视角下审视,具体而言,两方面改变对秘密性这一要件

提出了挑战:

第一,信息与之传播主体和含义的脱离,传播主体由人与人的传递转向机器之间的传递,传递内容由语义信息转向句法信息。自旧石器时代开始,语言文字的出现允许人类将其意识层面的信息进行记录并传递,之后印刷术、照相机、电报、电话、留声机、广播、电视等使得信息生产和传播的成本不断降低,但仍然一直是人与人之间语义信息的传递。进入信息网络时代,机器发挥着更重要的作用,人与人之间的信息传递开始以计算机传递为媒介。伴随着数字技术不断深化发展,信息的直接接收和处理主体已经不再是人,如软件、数据集合等要首先经过机器处理过滤之后甚至是再生产之后再传递给人。在传递内容上机器间的信息传播与人际的信息传播存在显著不同。按照符号学上的划分,信息可分为句法、语义、语用三个层面,句法指的是特定符号(如0和1)根据约定规则进行的组织和构造,语义指向的是符号排列背后的含义和意谓,往更高层次的语用则指向信息所追求的目标。人与人之间主要是内容含义即语义信息的传递;机器与机器之间主要是代码符号组合即句法信息的传递,是人与人之间信息交流的中间形态^[15](P97)。过去这种中间形态信息缺少独立价值而未被纳入法律调整的视野,但伴随着人工智能等技术的发展,机器可以直接处理这种中间形态的信息并进行再生产,使之具有了独立市场价值而产生了新的调整维度。对机器而言,数据文件的价值关键不在于是否具有可被人类理解的有用含义,而在于其是否存在可被计算机处理的代码,即信息含义不再重要。这种改变带来的结果是,需要将人与人之间以及机器与机器之间信息传播的一般理解和规制方式区分开来,在机器传播层面,含义公开与否不再是判断信息是否进入公有领域的绝对标准,如尽管所有用户可自由浏览某一网页内容,却绝不意味着用户已经自由获取了背后整个数据库的内容,而是要考察机器对代码信息的获取是否存在限制。

第二,信息传播与有形载体的脱离。与人与人之间信息传播依靠聆听、阅读等方式不同的是,机器之间信息传递依靠的是对数据文件的直接接触和访问。伴随着信息传播由商品范式向服务范式的转型,信息一经传播便可无限复制的特点发生了实质性转变。具体而言,过去信息传播主要依靠有形载体的移转加以实现,获取之后信息接受者便可以自由处置该载体而传播、利用其内部信息;伴随着互联网技术出现以及信息存储传递成本的降低,信息传播可以完全不依靠有形载体,内容提供者可在其网络空间内集中提供和传播信息,信息传播由商品交易转变为网络空间访问路径权限的交易,信息产品的购买者获得的是网络空间的访问权限或计算能力^[16](P116)。这一转变突出地体现于数据交易之中,当今数据交易并非是数据文件或产品的直接转让,而多采取“原始数据不出域、数据可用不可见”的方式,向交易对象提供一种访问权限或计算服务。在服务范式下,访问权限授予并不等于对数据控制的移转,在私人网络空间中,所有者可以通过设置网络空间基础架构即代码措施来精确地界定访问者行为规则,自主决定哪些主体有权访问哪些数据以及哪些数据能够与其他数据通信,建立起数据控制、利用、流转的“私人秩序”。除非他人的恶意破坏,网络空间所有者并不因数据广泛交易和共享失去其数据集合的事实控制。故而有学者称“代码即法律”,甚至是相对于法律保护更加精准和有效的保护^[17](P28)。

以上两点决定了秘密—公开二分法已无法适用于机器之间的信息传递,数字环境下“信息的剥离”使得句法信息即数据具有了独立价值,从而形成了一个数据生产、利用和交易的全新市场,其传播方式与人与人之间的信息传播存在实质不同,传统面向人的规制范式面临着调整乏力。句法信息是否进入公有领域,不在于含义是否被公开,而在于他人是否具有不受限制地访问该数据文件的能力。以代码空间为中心,企业可以采用技术措施而限制他人对数据的获取,只要处于计算机所有者的排他性控制之下数据或代码信息即具有稀缺性和市场价值,进而有法律保护之必要,并非只有秘密信息才能够成为值得保护的财产,美国、日本的数据保护制度即可见一斑。因此,支撑型机制的适用需从传统人与人信息传播的理解和规制方式中跳脱出来,构建更具普适性、包容性的适用标准。

四、数字时代支撑型机制的迭代升级

面对数据保护问题,支撑型机制提供了新的制度可能,但创设型机制同样具有纠正市场失灵的功能。相较于创设型机制,支撑型机制是否具有制度选择上的优先性,进而有必要作出制度扩张,决定了数据保护乃至其他信息财产保护制度建构的方向。因此,本文将具体分析支撑型机制与创设型机制的一般关系及效率优劣,进而明确支撑型机制的完善必要及制度设计。

(一) 支撑型机制扩张适用的必要性检讨

数字经济中数据等新客体的保护可存在支撑型机制和创设型机制两种路径,二者均服务于纠正市场失灵的共同目标,按照田村善之教授的“市场指向型知识产权法”理论,一般而言,市场力量主导的支撑型机制相对于法律主导的创设型机制应具有选择的优先性,即在市场自身能够发挥激励作用时,法律不必要介入;在法律规制成为必要时,也应该主要依赖市场既存的激励机制;只有在例外情况下,市场既存的激励机制不能发挥自律性功能时,才需要通过法律创设权利来恢复市场的自律性作用^[4](P15-16)。这种优先关系是由两种制度的作用方式决定的,因为支撑型机制的首要任务是恢复市场对创新成果开发的自律功能,主要调整方式是保护私力构建的产权、纠正不法行为,不排除他人对相同信息的研发利用,并不产生额外社会负担,故在一定程度上不关心受保护成果的创新程度,而是交由市场优胜劣汰选择。创设型机制是独立于社会事实之外重新建构的一套社会秩序,作为一种对世的排他性权利,需要通过登记等方式明确看不见、摸不着的信息范围,相对于支撑型机制缺乏确定性以及保护的有效性。排他性权利的本质在于禁止他人对信息客体未经许可的利用,这种排他性保护同时构成了对社会整体利益的直接克减。为避免对社会公众不必要的限制,排他性权利的授予应以客体具有一定创造性高度为前提(如专利创造性、作品独创性要求);为保障公共利益和公有领域,要求权利保护应以特定期限、限制例外为约束。这一系列都依靠国家权威进行设定和判断,相对于市场机制存在效率上的不足,并存在较高的制度运行和错误成本。基于支撑型机制在保护确定性、社会公共负担及制度成本方面的优势,在信息财产保护中一般应具有选择的优先性。

在数字经济时代,支撑型机制相对创设型机制的效率优势是否仍然成立有待验证,数据保护制度需在两种选项中作出选择,故本文将主要围绕此具体分析二者效率优劣。在制度模型选取上,支撑型机制主要以日本法、美国法上的数据保护制度为代表,但创设型机制的权利模型理论界尚未达成共识。由于欧盟数据库特别权利制度是现有制度实践中对数据赋予财产权利的最成熟制度,可参照此类排在数据之上排他性权利的理想模型,即如果市场主体在数据生成、收集、加工中付出实质性投资,获得了具有相当数量累积而具有商业价值的数据集合,可赋予投资者禁止他人获取和再利用数据集合的全部或实质部分内容的权利^[18](P152-170)。以下主要就此两种制度模型比较分析。在比较标准上,知识产权制度的总体目标在于提供一种产权激励而实现社会总体福利的最大化,即将促进信息创造、利用的价值与之带来社会成本的差值最大化,具体可细化为三方面判断标准^[19](P5-6):一是新的足够数量信息可否在恰当时被创造出来;二是创造新的信息可否用于生产,为服务生产者、消费者产生社会效益最大的流动;三是在新信息被创造的条件下,生产所需的社会成本是否会降至最低限度。这三个子目标也是知识产权制度设计需要不断回应的问题,可将之概括为有效生产激励、最大化信息流动、最小化社会成本三项标准。以此视角出发,现分别就支撑型机制与创设型机制的效率优劣对比如下:

1. 有效生产激励

创新激励是设立知识产权的最主要理由,有效生产激励标准的核心在于法律对生产者投资成果保护的有效性。当前实践中数据往往作为数字企业经营的副产品而存在,生产激励并非是当前面临的最突出问题,但产权保护对于数字市场运作仍具有不可或缺的意义:一方面,完整的产权保护可保障企业数据投资收益的内部化,从而吸引更多投资和创新;另一方面,某些业务模式完全以收集用户数据为基

础(如大众点评),市场中也存在专门收集和交易数据的数据中介模式,其有效地促进了数据共享,如果缺乏对于数据集合的产权保护,将导致此类投资激励的缺失。为保护数据产权,如前所述,企业一般首先通过技术措施自我建立对数据集合的事实产权,同时需要法律禁止未经允许的数据获取利用行为。创设型机制和支撑型机制遵循着不同的路径发挥作用:创设型机制在于通过法律界定受保护的客体、确定权利归属,并赋予权利人排除任何人获取、再利用其数据集合的权利;支撑型机制在于以法律保护强化技术控制措施的效力,排除他人未经允许的数据获取、利用、公开行为。

就两种保护模式产权保护的有效性对比:首先,在法定排他性范围层面,支撑型机制主要排除他人的不当数据获取、公开行为,禁止恶意第三人对非法获取数据的继受取得及进一步公开、利用行为,但不及于善意第三人的获取、利用、披露行为;创设型机制概括地禁止他人任何未经允许的数据复制及传播利用行为。理论上,创设型机制比支撑型机制保护范围更加宽泛。然而,产权保护效果不仅要看法律文本的承诺,同时应考量权利实施的有效性。在权利实施层面,与互联网出现伊始时的版权保护难题类似,如果仅赋予企业对数据集合的排他性权利而没有技术保护措施的法律支持,侵权者可以相对低成本地进入他人网络空间、获取数据。虽然权利人在理论上享有禁止他人获取和再利用数据的排他性去权利,但数据一旦脱离了权利人的实际控制将重归“无政府主义”的网络空间,在他人网络空间的“黑箱”内,权利人将难以及时发现侵权行为、确定侵权行为人、制止侵权行为和获得权利救济。基于此,权利人仍然会采取技术措施自我保护,由于缺乏对技术措施的保护,企业之间将可能陷入技术措施绕过与反绕过的“丛林法则”。支撑型机制的优势在于,其本质上是企业代码措施的“法律强化器”。代码措施本身作为网络空间的一种客观规律蕴含于人们的行为之中,在并非蓄意破坏的情况下,无需依赖外部力量即可实现访问者行为规制的效果,不会因访问者主观上是否知道代码规制存在而受影响,针对蓄意破坏行为则交由法律提供保护加持。总体而言,支撑型机制以一种事前的方式从根本上减少了未经允许不当获取数据的行为,相较于创设型机制将更加具有产权保护的确定性和有效性优势。

2. 最大化成果流动

创造的知识只有传播给他人进行消费或者直接间接用于生产服务时,才能真正产生经济福利。数据互惠分享是数字经济赖以生存的基础生态规则,由不同数据分析者根据不同用途对数据进行发掘,方能实现数据价值的最大化。最大化成果流动或促进数据的商业化利用是采取创设型机制的重要理由之一,其理论出发点在于阿罗(Arrow)所提出的“阿罗悖论”^[20](P609-626),即信息交易的前提是潜在的购买者能够评价信息价值,这要求潜在购买者对信息进行了解,但其一旦充分了解信息之后,就不必要再进行购买,这导致信息交易无法实现;同时,购买者购买之后可能对信息进行转售,进而对于原来销售者的利益产生实质影响。在数据保护中,虽然商业秘密制度可以解决前述生产激励的问题,在流通共享场景下会存在信息外漏和失去保护的风险。因此,有学者认为排他性权利可为数据交易提供更加稳定的法律预期。但如前所述,信息传播形式的变化已使得“阿罗悖论”的前提不再成立:第一,伴随着信息传递主体由人与人之间的传递转向机器之间的传递,信息传递内容由语义、语用信息转向句法信息,信息含义在信息传递中已不再重要。这意味着可以交易的潜在对象可以了解语义层面的信息内容范围,却无法获取数据代码即直接获取信息的价值。第二,信息传播形式由商品范式转向服务范式,信息传播过程与物理载体相脱离,内容提供者可以在其网络空间内集中提供和传播其信息,信息接收者仅获得的是对网络空间的访问权,数据交易并不意味着控制者对数据控制权的丧失。基于此,日本法及美国法只是将法律保护的标准由商业秘密的秘密性扩张到了有限提供信息,即可允许企业大规模地交易共享数据,而不必担心数据被泄露而无法获得保护,实现与法定权利同样的功能。同时,数据流动在很大程度上受到产权保护确定性的影响,如前所述,尽管创设型机制在排他性范围上大于支撑型机制,但无法确保执法的有效性,这种不确定性会抑制权利人数据共享的积极性;在受到支撑型机制保护的可靠空间内,权利人可自主设定数据获取权限、范围、内容,而不必担心此类问题。因此,在促进数据流动方面,支撑型

机制相对于创设型机制将更具优势。

3. 最小化社会成本

知识产权制度的根本目的在于通过授予权利人对信息产品的垄断权来激励创新,同时存在一定社会成本,包括三个方面^[21](P18-24):一是无谓损失,短期垄断将带来信息产品价格上涨而排除了部分人利用该信息的可能,使得短期内资源配置处于低效率;二是创新的累积性成本,由于知识创新具有累积性特点,难以存在绝对的无中生有,新的信息生产必然要以在先信息为基础,产权保护一方面会增加后续创新者的成本,另一方面可能会形成对某些公共信息的垄断而阻断创新动态竞争的过程;三是制度运行、产权交易所产生的制度成本。最优制度设计应寻求社会成本的最小化,创设型机制与支撑型机制带来的社会成本可对比如下:

第一,在减少无谓损失层面,现实中企业将首先通过技术措施辅之以合同约束的方式建立起数据保护、利用、交易的私人秩序,区别于国家立法,理性的市场主体通常能更加准确地把握自身定位及市场需求。在有一定界权成本的前提下,企业会谨慎地根据业务需要界定要保护的数据范围及限制访问的对象从而施加技术措施保护,其他的则贡献给公众自由获取,可以相对灵活地随时选择保护或者放弃产权。作为一种“法律强化器”,支撑型机制对企业建立的私人秩序提供补充保护,以一种侵入性较弱的方式强化而并非改变事实层面的交易秩序。创设型机制是一种独立于企业构建的私人秩序之外的调整模式,作为一种对世的排他性权利,其需要以“一刀切”的方式明确权利人对其投资数据集合的排他性权利。新的权利设置之后,可预见的是数据控制者一般仍会对其数据集合采取技术保护措施保护,不可避免地导致两种保护秩序的重叠和企业排他范围的扩大,原来放弃保护进入公有领域的数据将重新进入其排他性范围。因此,相对于创设型机制“一刀切”的保护,支撑型机制允许企业以私人定制的方式区分数据类型、交易主体等情形进行区别定价,可产生更少的无谓损失。

第二,在制度成本方面,主要涉及保护的确定性法律问题。作为对世性的财产权利,创设型机制必须清晰地界定其保护客体和范围,对外公示受保护数据集合的全部或实质部分。这却存在着现实困难,因为与版权保护一部著作、歌曲所不同的是,数据集合是一堆零散数据的堆积,且具有动态性和不断变化的特点,一般公众很难获知何为其全部或实质部分,难以界定合理利用其非实质部分与侵权的边界。尤其在网络空间由爬虫机器人爬取数据的情形下,爬虫机器人更加无法确定何为受到法律保护的数据内容以及何为侵权,导致原本自由访问的网络空间动辄得咎。由于缺乏权利保护范围的确定性,类似于“专利蟑螂”利用问题专利进行策略性维权的现象同样可能出现在数据领域,从而压缩社会创新空间、增加创新成本。相对于此,支撑型机制具有更强的确定性优势,其保护前提在于受保护数据区别于公众可获取数据,并通过代码控制彰显保护意愿、公示保护范围。这种代码控制不仅是一种观念上的规制,更是一种客观技术环境的约束,不因相对方主观上是否知道代码规制存在而受影响,其产生的制度运行成本比法定权利模式要更小。

第三,创新累积性成本方面是反对支撑型机制而主张采取创设型机制的最主要理由。有学者认为,权利人过度依赖技术措施保护,会显著降低数据的流动性和可及性,使原本不受法律保护的数据获得保护,增加了企业的运营成本,也使得互联网朝更加封闭的纵向一体化方向发展^[9](P8)。现实情况却是,即使在数据之上创设排他性权利,完全自由的网络空间下也面临着执法困难,尤其是企业对企业(B2B)的数据交易一般会采取端到端的最低限度加密,数据控制者很难发现侵权行为存在,其往往仍然会选择直接有效的技术措施保护,将法律救济作为最后的措施。以版权技术措施保护为例,尽管对于计算机软件和音乐作品作者可以通过版权保护,权利人仍然广泛地采用技术措施。可以说,代码限制或互联网走向封闭是企业追逐私利而产生的不可避免的结果,但信息传播中语义信息与句法信息的分离,使得企业将限制措施集中于代码信息而开放语义信息,因而至今这种封闭对于一般用户的影响并不明显。支撑型机制的积极意义在于为企业私力措施提供了一种“法律强化器”,通过法律保护避免陷入无休止的技

术措施绕过及反绕过的丛林法则,以一种对现实交易秩序侵入性更弱的方式为数据控制者提供保护,且避免了对于数据流动造成进一步的限制,在公共信息获取方面并没有让情况变得更坏,同时,这也减少而非增加了企业在设置、维护技术措施等方面的成本。

总体而言,支撑型机制在有效生产激励、最大化信息流动、最小化社会成本三个方面都优于创设型机制。在企业私力措施基本上能够恢复市场自律性作用的前提下,在数据之上建立一种新的排他性权利并不会产生显著的效率,支撑型机制仍具有制度选择上的优先性,因此有必要突破现有商业秘密制度对于秘密—公开的二分,适应数字环境特点进行制度完善。

(二) 支撑型机制扩张适用的制度构造

尽管支撑型机制在数据保护理论探讨中较少受到关注,却已经得到了立法机关的接纳。在新一轮《中华人民共和国反不正当竞争法》(以下简称“《反不正当竞争法》”)修改中,2022年11月市场监管总局公布的《中华人民共和国反不正当竞争法(修订草案征求意见稿)》(以下简称“《征求意见稿》”)第18条建立了商业数据保护制度,规定经营者对“依法收集、具有商业价值并采取相应技术管理措施的数据”,有权排除他人的不当获取和使用。《征求意见稿》体现了立法机关对支撑型机制的接纳,试图在商业秘密制度之外承认并保护经营者对数据的事实控制。然而,现有制度设计却体现出了一定要素缺失和逻辑混乱:首先,就商业数据保护条件,《征求意见稿》规定了依法收集、具有商业价值、采取相应技术管理措施三项要件,依法收集、具有商业价值内涵相对明确,但“采取相应技术管理措施”内涵却具有不确定性。例如,商业秘密合理保密措施要件的目的在于保持信息秘密性即不为公众所知悉的状态,日本限定提供数据制度的电磁管理性要件要求权利人采取电磁管理措施确保数据仅向有限主体提供。《征求意见稿》商业数据制度却并未对“相应技术管理措施”作出限定,明确其应达到什么程度或实现何种功能,导致实践中将难以认定。其次,针对不法侵害行为,商业秘密制度主要禁止他人不正当获取、利用、披露信息三类行为,比如日本“限定提供数据”制度也继续沿用了此界定方式,《征求意见稿》分别为各类不正当行为的认定进一步增加了限定条件:第一,以不正当手段获取商业数据的行为,应以“不合理地增加其他经营者的运营成本、影响其他经营者的正常经营”为限;第二,违反约定获取数据以及进一步使用、披露数据,应以“实质性替代其他经营者提供的相关产品或者服务”为限。该规定体现了不同法律逻辑的杂糅,除借鉴商业秘密制度外,其还吸收了美国法上动产侵占之诉、信息盗用侵权等不同的制度逻辑。然而,这却与支撑型机制的基本逻辑并不相容,因为支撑型机制旨在保护权利人对信息控制的圆满状态,一旦不正当获取、披露、使用行为发生后即会导致信息失控的风险,破坏技术措施并盗用有价值数据本身应当具有不正当性,不问其是否对权利人业务构成实质性替代或不合理地增加运营成本。

从征求意见稿到正式立法仍然存在较大的完善空间。事实上,由于数字经济中秘密—公开二分法的失灵,不仅针对数据保护,面向未来各种新领域新业态的信息财产形态,都需要回归商业秘密理论基础对现有制度作出重构。传统商业秘密保护的理论基础包括规范分析和效用分析两个层面,伴随着秘密—公开二分法的失灵,其制度的现代化重构也应当结合技术发展从此两个层面进行检讨:

在规范分析层面,商业秘密保护限于对具有秘密性、价值性并采取保密措施的信息加以保护,秘密性以及保密性要件确立的基础是,财产权的取得必须以占有为前提,占有指的是对物事实上的控制与支配,要求占有人在主观上具有占有的自然意思,在客观上形成对物事实上的管领力,将信息作为私人财产保护也必须对其建立事实上的排他性控制并体现个人所有的意图。如前所述,伴随着技术进步,对信息的排他性控制已不限于严格保密,经营者完全可以通过施加技术措施确保特定信息仅向有限主体或者仅按照特定方式提供。无论含义公开与否,该信息都处于相关主体的控制或支配范围,在事实上具有稀缺性而存在交易价值,任何违背他人占有意思而获取该有价值信息的行为即具有不法性。基于此,有必要将商业秘密保护的客体范围由秘密性信息扩张至有限提供信息,对保护要件作以下调整:第一,将秘密性要件调整为有限提供性要件。即将保护客体由不为公众所知悉的秘密信息扩大到仅向有限主体

提供的信息,但公众可不受限制地自由获取的信息不在此列。第二,将保密性要件调整为控制性要件。商业秘密制度中的保密性要求采取合理措施维持信息的秘密性,有限提供信息保护中对应地应当调整为采取相应控制措施维持信息仅向有限主体提供。第三,调整价值性要件的内涵。价值性是一切财产受保护的前提,传统商业秘密要求相关信息应因秘密而具有价值,有限提供信息保护对应性地则应调整为相关信息应当因有限提供性而具有价值。在保护范围上,商业秘密与有限提供信息都旨在维持权利人对信息控制的圆满状态,均有必要限制他人的获取、利用和披露行为,对此可继续沿用对此三类行为的禁止。

在效用分析层面,将保护客体从秘密信息扩张至有限提供信息的合理性也可以得到检验。从经济学的角度分析,商业秘密保护的原因在于,对创新性信息,企业在可能的情况下将采取私力措施加以保护,避免其在利用流通中外溢而产生负外部性,但这种私力措施本身容易遭到破坏。提供法律保护,一方面可以实现对未知信息创造的制度激励,另一方面可以减少企业的保密成本,避免企业间“丛林法则”以及为预防盗窃(商业秘密)开展“军备竞赛”,促进企业间更大范围的信息共享^[22](P329-337)。保密性要件的功能在于确保保护客体不同于公有领域已有信息,即具有通常所谓的“新颖性”,要求信息不为一般公众知悉或容易获得而具有市场交易的稀缺性价值,核心在于保护客体具有创新性并具有交易价值。对公有领域之外的信息,如果企业采取代码措施限制有限主体获取,无论其含义是否被公开,都具有这种稀缺性和交易价值,从而存在法律保护和激励创新的必要性,从降低私力保护成本的角度也有必要将法律保护延及此类信息。如在数据保护实践中,企业收集获得数据之后,往往采取一定措施限制他人爬取(如Robot协议、人机识别系统、用户密码认证等),这仅能使诚信的人保持诚信却无法提供完美保护,他人仍然可能绕过或破坏限制措施而获取数据。现有数据保护纠纷,大多都是他人绕过企业限制措施而获取数据的情形,如果没有法律干预,数据收集者和竞争对手很容易陷入绕开与反绕开无休无止的消耗战,对这种有限提供信息的保护则可以有效降低私人保护的成本。

因此,法律对信息私力控制的保护不仅应包括秘密信息,还应包含有限提供信息。由于二者保护基础的同质性,在具体立法中可选择对现行《反不正当竞争法》第9条商业秘密条款进行扩张,因为“合法控制”而非“秘密”才是立法保护的核心。这也可以从国际条约中得到印证,WTO组织订立的《与贸易有关的知识产权协定》(TRIPs)作为商业秘密保护最主要的多边条约,也是我国商业秘密保护的重要基础,其第39条第2款并未将保护对象限定于商业秘密,而是“合法控制信息”,规定“自然人和法人应有可能防止其合法控制信息在未经其同意的情况下以违反诚实商业行为的方式向他人披露,或被他人取得或使用”。换言之,只要通过合法的途径控制相关信息即可得到保护。该条款后半部分规定的秘密性、价值性、保密性要件应当是在当时技术条件下对“控制”成立条件的具体界定。基于此,我国在内的各国立法一般将TRIPs第39条第2款规定直接理解为对商业秘密的保护,但该款却为此后扩大保护客体范围保留了空间。伴随着技术不断革新演进,该条款的实施应当突出阐明法律保护信息“控制”的核心目标,将《反不正当竞争法》第9条商业秘密保护修改为对合法控制信息的保护,根据现实技术条件将合法控制的要件由秘密性、价值性、保密性扩张至有限提供性、价值性以及控制性要件,这包含了对传统商业秘密的保护,也并不构成对国际条约最低保护义务的违反。

将商业秘密制度扩张至对合法控制信息保护,可解决绝大多数情境下的数据保护问题:对平台内部数据,数据控制者在其网络空间建立了访问控制措施,并通过设置用户认证和访问权限限制他人访问,应构成有限提供和合法控制;对互联网公开数据,有的通过用户访问政策、爬虫协议或者人机识别措施限制他人对其网站数据的爬取,从降低保护成本的角度应当认为保护条件成立^[23](P25-26);对未施加任何限制措施的原则上不予保护,严格影响市场竞争秩序的则可交由《反不正当竞争法》一般条款补充调整。在此制度下,他人未经允许破坏、绕开控制措施获取、利用、公开数据的行为将被禁止,因为相关信息一旦被他人不正当获取而失去控制将面临着完全丧失价值的风险,而不应问相关行为是否对权利人

的业务构成实质性替代或不合理地增加运营成本。

基于此,笔者建议《反不正当竞争法》修改不必设立专门的“商业数据”保护制度,应将第9条商业秘密保护制度修改为对“合法控制信息”的保护:

“任何自然人、法人、非法人组织不得实施下列侵犯他人合法控制信息的行为:

(一)通过窃取、欺诈、强迫等不正当手段,获取合法控制信息的行为,以及使用、公开通过不当获取行为所取得的合法控制信息的行为;

(二)违反合同或者法律规定的义务,使用、披露其所掌握的合法控制信息;

(三)明知或应知他人以不正当手段获取合法控制信息,或者他人违反合同或法定义务使用、披露有限提供信息,仍然继续获取、使用、披露合法控制信息的行为。

本法所称的合法控制信息,是指仅向有限主体或仅以特定方式提供、采取相应控制措施并因此具有商业价值的技术信息、经营信息等商业信息。”

由于信息具有无形性特点而难于被控制,故不同于有体财产,信息财产法律保护一直遵循着秘密—公开的二分,仅秘密信息可通过保护对其事实控制来保障客体之上的利益实现,公开信息则依靠设立知识产权加以保护。受限于权利法定原则,知识产权需因应技术进步不断作出调整,数据保护等新问题的出现不断对传统知识产权体系提出挑战,由于对权利范式的依赖,新的排他性权利模型不断被提出。然而,在数字时代,信息逐渐与物理载体、人类创造者、人类接收者及特定含义相剥离,信息并不因含义公开而失控,企业对信息私力控制能力范围进一步拓宽,支撑型机制具有了更宽的适用范围,依照秘密—公开二分法来划定支撑型机制与创设型机制的功能分担关系已不合时宜。面对数据保护等新问题,支撑型机制相对于创设型机制在权利保护确定性、社会公共负担以及制度运行成本方面更加具有效率优势,有必要从过去对人与人信息传播的理解和规制方式中跳脱出来,面向机器之间的信息传播重构支撑型机制。本文建议在商业秘密制度基础上建立合法控制信息保护制度,禁止对向有限主体提供、采取相应控制措施并因此具有商业价值的信息的不正当获取、利用和公开行为。通过支撑型机制的现代化完善,建立私人力量与法律之力合作共治的良性循环,弥补传统知识产权体系僵化和滞后性问题,适应新一轮科技革命中不断发展变化的信息财产保护需求。

参考文献

- [1] 郑开琪. 关于信息的定义及其分类. 上海社会科学院学术季刊, 1989, (3).
- [2] 鲁道夫·萨科, 拉法埃莱·卡泰丽娜. 占有论. 贾婉婷译. 北京: 中国政法大学出版社, 2014.
- [3] 约拉姆·巴泽尔. 产权的经济分析. 费方域、段毅才、钱敏译. 上海: 格致出版社、上海三联书店、上海人民出版社, 2017.
- [4] 田村善之. 日本知识产权法. 周超、李雨峰、李希同译. 北京: 知识产权出版社, 2011.
- [5] 朱谢群. 信息共享与知识产权专有. 中国社会科学, 2003, (4).
- [6] 李扬. 日本保护数据的不正当竞争法模式及其检视. 政法论丛, 2021, (4).
- [7] 龙卫球. 数据新型财产权构建及其体系研究. 政法论坛, 2017, (4).
- [8] 申卫星. 论数据用益权. 中国社会科学, 2020, (11).
- [9] 崔国斌. 大数据有限排他权的基础理论. 法学研究, 2019, (5).
- [10] 许可. 数据权利: 范式统合与规范分殊. 政法论坛, 2021, (4).
- [11] Patrick J. Manion. Two Steps Forward, One Step Back: The Defend Trade Secrets Act of 2016 and Why the Computer Fraud and Abuse Act of 1984 Still Matters for Trade Secret Misappropriation. *Journal of Legislation*, 2017, 43(2).
- [12] 彭诚信. 智力成果、知识产权与占有制度. 法商研究, 2002, (6).
- [13] David K. Berlo. *The Process of Communication: An Introduction to Theory and Practice*. New York: Holt, Rinehart and Winston, 1960.
- [14] Herbert Zech. *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, 2012.

- [15] Denis Pombriant. Data, Information and Knowledge: Transformation of Data Is Key. *Computer Law Review International*, 2013, 14(4).
- [16] 吴伟光. 构建网络经济中的民事新权利：代码空间权. *政治与法律*, 2018, (4).
- [17] 劳伦斯·莱斯格. 代码2.0：网络空间中的法律. 李旭、沈伟译. 北京：清华大学出版社，2009.
- [18] 张浩然. 由传统数据库保护反思新型“数据财产权”. *法学杂志*, 2022, (6).
- [19] Stanley M. Besen, Leo J. Raskind. An Introduction to the Law and Economics of Intellectual Property. *Journal of Economic Perspectives*, 1991, 5(1).
- [20] Kenneth J. Arrow. Economic Welfare and the Allocation of Resources for Invention//National Bureau of Economic Research. *The Rate and Direction of Inventive Activity: Economic and Social Factors*. Princeton: Princeton University Press, 1962.
- [21] 威廉·M. 兰德斯, 理查德·A. 波斯纳. 知识产权法与经济结构. 金海军译. 北京：北京大学出版社，2016.
- [22] Mark A. Lemley. The Surprising Virtues of Treating Trade Secrets as IP Rights. *Stanford Law Review*, 2008, 61(2).
- [23] 孔祥俊. 论反不正当竞争法“商业数据专条”的建构——落实中央关于数据产权制度顶层设计的一种方案. *东方法学*, 2022, (5).

From Constructive Mechanism to Auxiliary Mechanism: The Paradigm Shift of Information Assets Protection In Digital Age

Zhang Haoran (Chinese Academy of Social Sciences)

Abstract Different from physical property, the legal protection of information follows the secrecy-publicity dichotomy, only secret information can be protected based on the exclusive control over the object to fulfill the interests (auxiliary mechanism), while other information should be protected through establishment of exclusive rights (constructive mechanism). Restricted by the numerus clausus principle, the constructive mechanism needs to be constantly adjusted with technology development. With data becoming the new production factor, the majority view advocates a new exclusive property right on data. However, the data protection practices in such countries as the United States and Japan have chosen to expand the auxiliary mechanism, which provides a new paradigm for the information assets protection in digital age. In digital environment, information is gradually abstracted from its meaning, creator, receiver and carrier. The ability of enterprises to control information has been largely expanded, and the secrecy-publicity dichotomy is no longer applicable. It's necessary to build a more inclusive and modern auxiliary mechanism, a protection system for information within lawful control based on trade secret system, to prohibit acquiring, utilizing, or disclosing the information, which can only be accessed by limited subjects, thus generates commercial value, and has been taken control with measures correspondingly.

Key words information property; IPR protection; data element market; property interests in data; trade secrets; secrecy-publicity dichotomy; private control

■ 作者简介 张浩然, 中国社会科学院法学研究所助理研究员; 北京 100720。

■ 责任编辑 李 媛