

企业数据交易模式的构建

张 艳*

摘要:企业数据交易模式的构建可细分为交易对象、交易方式与交易互信3个方面。交易对象是数据使用权。以数据使用权作为交易对象能够助力数据发挥更大价值、契合数据法的社会本位理念并保障数据的可获取性与可使用性。数据使用权源于作为弱民事权利的数据持有者。交易方式是数据许可。数据许可属非典型许可,具有不同于典型许可的诸多特殊之处。数据许可合同的具体内容由双方当事人依据合同自由原则进行约定,格式条款效力审查机制与强制许可制度则用来确保合同自由不失边界。交易互信的技术保障是隐私计算技术。在对数据价值结构进行解剖的基础上,可通过隐私计算技术实现“原始数据不出域、数据可用不可见”。技术提供方与数据提供方、数据使用方之间形成技术服务法律关系。

关键词:数据交易 数据使用权 数据持有者 数据许可 交易互信

企业数据是企业生产、经营、管理过程中生成并控制的、不涉及个人信息和公共利益的业务数据。目前,社会数据资源分布格局已发生转变,从政府数据资源占80%转变为以互联网、金融、电信等企业数据资源为主的倒“二八”格局。海量企业数据具有巨大的商业价值,其交易与流通对于充分释放数据要素价值具有重要意义。

遗憾的是,企业数据交易领域的诸多基础性问题尚未厘清、数据价值链的各环节间障碍重重严重阻碍了数据要素价值在社会经济生活中的充分释放。具而言之:(1)交易对象亟须确定。鉴于数据具有诸多特殊性,故有别于传统商品交易,数据交易并非以支配权作为交易对象。交易对象究竟是何种数据权利,理论界与实务界尚未给出清晰的答案。(2)交易方式有待提炼。目前我国正在建设多层次的数据交易市场,包括场内集中交易与场外分散交易、数据资源一级市场与数据产品二级市场等内容。然而,普遍意义上的数据交易究竟以何种方式进行,对应何种法律关系,并没有得到深入探讨。(3)交易互信尚未构建。数据的特殊性使信赖成为数据交易的基石,

* 上海社会科学院法学研究所副研究员

基金项目:2022年度上海市科学技术委员会“科技创新行动计划”软科学研究项目(22692111400)

目前传统的交易互信机制已面临瓶颈,导致数据孤岛比比皆是,故亟须构建新型交易互信机制。

为充分释放数据要素价值,构建符合数字时代要求的企业数据交易模式已迫在眉睫。本文将从交易对象、交易方式以及交易互信 3 个方面对企业数据交易模式的构建进行深入探讨。

一、交易对象的确定:数据使用权

确定交易对象是构建数据交易模式的前提。一般来说,商品交易是商品买卖的同义词,多以商品支配权为交易对象,并以卖方丧失支配权、买方获得支配权为交易结果。若以传统交易视角来看待数据交易,则可称之为数据买卖。具体内容为:卖方将数据交付给买方后删除己方数据,从而完全丧失对数据的持有与控制,买方在支付一定对价后成为新的数据持有人。然而,数据买卖在实践中较为罕见,^①更主流的数据交易模式是数据使用权的让与。实际上,数据使用权不仅是数据交易对象,而且是数字时代的核心数据权利。

(一)数据使用权作为交易对象的正当性

1. 助力数据发挥更大的价值。数据是对信息以机器可读的方式进行的记录,可分解为语义、符号与结构 3 个层面。^② 以一张电子婚礼照片为例,语义层面的数据指照片的信息内容,需通过人的理解获得含义,即甲男与乙女举办了婚礼。符号层面的数据是由 0 和 1 的排列所呈现的计算机编码,是计算机计算的对象。结构层面的数据则是作为数据载体的物理存储设施,如硬盘、云等。其中,作为媒介的符号是枢纽,其通过存储于特定物理介质传递语义信息,故符号层面的数据是狭义的数据,亦是本文探讨的对象。相较于其他商品,数据彰显出截然不同的特点,因其无体且无需较多成本即可进行复制,故其具有使用上的非竞争性、非排他性与非消耗性。^③ 这意味着,数据可克服有体物以实际控制为前提方可使用的局限性,在无损使用效用的情形下同时被多个主体使用。

传统商品交易因立基于有体物的稀缺性与使用上的竞争性,故以商品支配权作为交易对象。对数据交易来说,应从数据特性出发构建与之相适应的交易模式。具体而言,应充分利用数据的非竞争性、非排他性与非消耗性等优点,将数据使用权确定为交易对象,使数据更充分地发挥价值。鉴于同一数据上可存在无数个并行不悖的使用权,可通过使用权让与创建一对多的交易模式。这意味着,在无损使用效用的前提下,同一数据可同时被数据提供方与多个数据使用方使用。数据是企业业绩增长不可或缺的重要资源,数据使用权让与将充分释放数据价值,从而促进整个国民经济水平的提升。

2. 契合数据法的社会本位理念。数据法可分为数据交易法与数据规制法。前者主要调整数据提供方与使用方两个平等主体之间因数据交易而产生的横向民事法律关系;后者则是数据规制主体对包含数据交易关系在内的所有与数据相关的法律关系的纵向规制与监管。总体来看,数据法具有浓厚的社会本位特征。社会本位是数据法的基本理念之一,具体含义为,以促进社会

^① See European Commission, Building a European Data Economy, COM 2017 (9) final, p. 10.

^② Vgl. Zech, Information als Schutzgegenstand, 2012, S. 37.

^③ 参见丁晓东:《论企业数据权益的法律保护——基于数据法律性质的分析》,《法律科学》(西北政法大学学报)2020年第2期。

整体利益为目标,数据规制主体、数据提供方、数据使用方以及数据价值链上的其他主体各司其职地推动数据资源的平等获取与数据福祉的公平分配,以可持续和可获得的方式使数据资源惠及社会公众。^① 当存在市场失灵或以私法自治为基础的数据交易法无法实现实质性的合同公平时,就需要数据规制法从公共利益出发予以介入,以保障数据提供方负责任的数据供给与数据使用方可持续的数据获取与使用。

在社会本位理念的指引下,数据规制旨在从公共利益出发使数据参与社会化大生产,充分释放数据价值从而促进整个国民经济的发展,最终使全体人民共享数字经济的发展红利。具体而言,应从国民经济整体效能的提升和社会整体发展的均衡出发,使数据被更多市场主体获取与使用。目前,社会本位理念已被融入多个国家和地区的数据立法中。^② 对数据交易来说,以使用权作为交易对象更加契合数据法的社会本位理念。一方面,使用权让与更能彰显数据法以公共利益为中心的价值取向。数据法以数据服务于最广泛的社会大众为目标,通过制度设计使数据切实促进经济与社会发展。在数据买卖的交易场景下,小微企业一般被排除于买方群体之外,因为其通常不具备雄厚的资金储备以及强大的数据建模、计算与挖掘能力。使用权让与能够使更多处于相对弱势地位的市场主体有机会获取与使用数据,享受数字经济的红利,进而保障数据福祉的公平分配。另一方面,以使用权为交易对象能更好地平衡个体利益与全局利益,从而实现社会整体利益的最大化。使用权让与能有效沟通彰显个体利益的数据交易法律关系与彰显全局利益的数据规制法律关系,通过保障个体利益最大化的普遍化和持续化来提高社会整体利益。^③

3.助力达成数据法规制目标。数字经济是由数据价值链上的各个主体组成的庞大生态系统,各主体各司其职,共同保障数据的流通、获取与使用,从而在最大程度上激活数据要素潜能。与上述理想蓝图形成鲜明对比的是现实中无处不在的数据孤岛,企业将数据封闭于企业内部或仅允许其在集团内部使用,直接剥夺了数据在社会经济生活中创造更大价值的可能性。在此背景下,数据的规制需求突出体现在合理引导数据交易法层面的私法自治从而使更多企业有机会获取与使用数据。

使用权让与可助力达成数据法的规制目标,促进数据的流通、获取与使用。使用权让与是连接数据封闭与数据流通的桥梁,能够更好地平衡数据提供方与使用方的利益,使双方各取所需。对数据提供方来说,使用权让与能够打消其不愿提供数据的顾虑,并增强其交易动机。使用权让与也能够克服数据买卖的弊端,在达成数据交易的同时不妨碍提供方继续控制与使用数据。使用权让与还有望为提供方创造更多利润。在技术的助力下,双方可通过约定数据的具体用途与用量将交易对象特定化,即每次交易都是对特定数据的特定使用权的消费。因此,一份数据文件上基于使用权让与交易所产生的利润总和可能远高于数据买卖所带来的一次性收益。对数据使用方来说,使用权让与能更好地满足其交易需求。数据使用方致力于使用他方数据进行融合计算进而服务于企业决策,因此其通常不追求控制他方数据。此外,与数据买卖相比,使用权让与

^① 参见刘盛:《现代金融体系视野下的金融法:理念信守与制度表达》,《政治与法律》2022年第11期。

^② 例如,欧盟在2024年1月正式施行的《数据法案》(Data Act)中规定了大量向中小微企业和消费者利益倾斜的制度。

^③ 参见蒋悟真、李晟:《社会整体利益的法律维度——经济法基石范畴解读》,《法律科学》(西北政法学院学报)2005年第1期。

将使使用方以可负担的成本使用他方乃至多方数据,进而有效增进企业效益。

(二)数据使用权的来源:企业数据持有权

使用权让与型交易能够助力发挥数据价值、契合数据法社会本位理念以及保障数据的流通、获取与使用,因此是更适宜的数据交易模式。作为交易对象的数据使用权无疑来自企业对数据享有的权利,对于该项权利的名称与内容,现行法并未予以规定。《关于构建数据基础制度更好发挥数据要素作用的意见》(以下简称《数据二十条》)明确提出设立企业“数据资源持有权”(以下简称“数据持有权”)的主张,鉴于该项权利是数据使用权的来源且对数据交易方式的定性至关重要,故需对其属性、内容以及法律保护路径进行探讨。

1.权利属性:弱民事权利。从微观层面观察,企业数据确权是“企业数据保护”与“他人数据利用”这组相互冲突的利益进行博弈的结果。鉴于上述利益是处于相同利益位阶的私利,因此在利益衡量的过程中需考虑企业数据确权的制度利益。制度利益能够联结私人利益与公共利益,是利益衡量的核心。^①企业数据确权制度主要存在两大核心利益:一方面,企业数据确权旨在激励企业在数字经济中的投资动机与劳动投入,即激励数据生成。另一方面,也是更为重要的,企业数据确权旨在达成数据法的规制目标,即从公共利益出发促进数据的流通与使用,从而使数据为公众创造更大的价值。结合制度利益,从更宏观的视角观察,数据确权与数据流通密不可分,前者代表安全利益,后者代表效率利益,二者分别具有工具价值与目标价值。数据确权旨在通过搭建合理的权利框架满足数据流通的需求,而非强化数据的封闭性从而形成新的数据壁垒。因此,在探讨数据持有权的权利属性时,应时刻关照其背后隐含的制度利益,即有利于数据的流通、获取与使用。

结合企业数据确权的制度利益可知,数据持有权不是绝对权。原因在于,绝对权具有不利于数据价值公平分配、阻碍数据流通利用以及损害市场创新与竞争等诸多负面效果,绝对权在将数据的全部使用权限赋予企业的同时,亦为他人划定了绝对的行为禁区,即禁止第三人获取与使用数据。因此,企业数据持有权不是绝对权,不具有对抗任意第三人的法律效果。

企业数据持有权宜定位为弱民事权利,^②是企业基于持有数据这一事实状态而享有的权利。权利的保护范围、保护方式以及保护强度均呈现出较弱的样态,这种有意为之的“弱势”旨在实现数据的流通与利用。数据持有权就像一位作风严谨的切割大师,致力于在整体的数据利益空间中精准地找到企业数据保护与他人数据利用之间的黄金分割点,进而实现二者之间的微妙平衡。数据持有权以行为规制为工具,通过对他人行为的必要规制切割出企业的数据利益空间。^③必要规制意味着,在他人广泛的自由行为空间中,法律遵循最小干预原则,仅对不法获取与利用行为进行否定性评价。切割后的利益格局是:企业不享有如绝对权一般全面的法律保护,仅拥有适度的数据利益;他人亦不负有一般性的不作为义务,仅在法律明确列举的事项中负有不作为义务,其获取与利用数据的行为空间得以大幅提升。权利由“特定利益”与“法律上之力”构成,前者

^① 参见梁上上:《制度利益衡量的逻辑》,《中国法学》2012年第4期。

^② 参见孔祥俊:《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年第5期。

^③ 参见叶金强:《民法总则“民事权利章”的得与失》,《中外法学》2017年第3期;郑晓剑:《个人信息的民法定位及保护模式》,《法学》2021年第3期。

是权利内容,后者为权利外形。^① 数据持有权正是将切割后的数据利益确认为企业数据权利。

作为一项弱民事权利,企业数据持有权彰显的不是数据的法律归属,而是企业对自己生产或管理的数据所享有的有限控制力。该有限性突出体现为数据持有权对技术控制措施的依赖。数据持有权有以下构成要件:(1)持有工具。企业一般通过认证技术、专用传输线路等技术措施实现对数据的控制。若企业未对数据采取技术控制措施,则其不享有数据持有权,此时他人可自由获取与使用数据。因此,现代企业都高度重视数据隐私技术。(2)主观要件。企业具有控制数据的内心意思,即希望通过设置数据访问控制机制向外界传递其欲控制数据的信号。(3)客观效果。技术措施将在客观层面阻止未获授权的他人获取与使用数据,或者极大增加获取难度。

2.权利内容与保护路径。基于技术控制措施,作为弱权利的企业数据持有权具有有限的处分与排他权能。处分权能指企业基于数据持有可实施的处分行为。具体而言,企业不仅可自行使用、编辑数据,而且可将数据使用权让与他人。处分权能是数据交易得以实现的基础,企业可通过合同详细设置使用权让与细节。排他权能指企业基于数据的持有所享有的防御能力,主要包括两个内容:(1)数据的获取保护,即阻止未获授权的他人获取与使用数据;(2)数据的完整性保护,即阻止他人通过编辑等操作改变数据的完整性。

法律通过最低限度的行为规制对企业数据持有权进行保护。我国主要通过民法、竞争法与刑法规范对其加以保护,具体包括:(1)《中华人民共和国民法典》(以下简称《民法典》)中的侵权法规定;(2)《中华人民共和国反不正当竞争法》第2条和第12条的相关规定;(3)《中华人民共和国刑法》第285条第2款中的数据获取保护规定和第286条第2款中的数据完整性保护规定。需注意的是,被禁止的不是他人使用数据的行为,而是侵害企业数据持有权的特定行为,具体行为类型有待立法者予以明确,如未被授权的强行突破技术措施的非法获取与使用数据行为、超出约定范围的使用数据行为等。

二、交易方式的厘清:数据许可

数据使用权是数据交易对象,使用权让与是主流的数据交易方式。民法上的使用权让与合同主要有两种类型,即有体物租赁合同与无形财产许可合同。从数据属于无形财产这一角度观察,数据使用权让与合同似乎应归为许可合同,然而学界对此并未达成共识。^② 对数据交易而言,厘清数据使用权让与合同的类型、内容以及合同自由的边界是必要且迫切的。

(一)数据许可:非典型许可

对于数据使用权让与合同是否属于许可合同这一问题,学界观点的模棱两可实属情有可原。一方面,作为无名合同的许可合同并非一个封闭、静止、有着清晰边界的合同类型,许可合同的边界与许可合同法理论一直处在不断的发展过程中,主要由法律实务、司法和学说形塑。另一方面,根据许可合同法理论,传统知识产权许可包含负担行为与处分行为,负担行为指许可合同,处分行为中被处分的使用权通常来自基于绝对权的设权让与或受负性权利转让。^③ 然而,由于作

^① 参见熊请龙:《权利抑或法益?——一般人格权本质的再讨论》,《比较法研究》2005年第2期。

^② Vgl. Patzak/Beyerlein, Adressdatenhandel zu Telefonmarketingzwecken, MMR 2007, 687, 690.

^③ Vgl. Forkel, Gebundene Rechtsübertragung, Bd.1, 1977, S. 44 ff.

为数据使用权来源的数据所有权不是绝对权,因此无法根据传统的处分行为创设数据使用权。

判断数据使用权让与合同是否属于许可合同,首先要对许可合同的特征予以明确,下面将以知识产权许可为例展开探讨。许可合同处于民法与知识产权法的交叉地带,学界对许可合同特征的认识历经从消极性许可向积极性许可的转变。消极性许可理论聚焦于许可人享有的绝对权,由于绝对权具有消极的排他性,因此该理论主张,许可人没有能力赋予被许可人任何权利,只能放弃向其主张部分或全部防御权。^① 积极性许可理论则更加关注许可人的支配权,认为许可人通过许可合同为被许可人创设积极的使用权,使后者得以按照约定的方式使用无形财产。^② 随着积极性许可理论于1937年获得德国法院判例的支持,其已成为欧陆法系的主流学说。实际上,如同支配权与绝对权是物权的一体之两面,消极性许可理论与积极性许可理论亦共同构成对许可的全面理解。一言以蔽之,许可合同通过创设积极的使用权来消解许可内生的消极性。具而言之,由于作为许可基础的绝对权具有对抗所有人的排他效果,因此许可合同蕴含了积极性与消极性两大内容,前者指许可合同通过创设积极的使用权赋予被许可人使用无形财产的机会,后者指许可人承诺放弃主张基于消极绝对权的防御权。

数据使用权让与合同完全符合许可合同的上述特征。虽然企业数据所有权不具有绝对的排他性,但是有限的排他性足以产生阻止他人获取与使用数据的效果。在积极层面上,数据许可通过创设积极的使用权突破企业的数据所有权,使被许可人得以获取与使用数据。在消极层面上,许可人放弃针对被许可人实施技术控制等防御性措施。在许可合同法中,相较于被称为典型许可的知识产权许可,立基于数据所有权这一弱民事权利的数据许可被称为非典型许可。^③

相较于典型许可,作为非典型许可的数据许可具有诸多特殊性,具体表现如下:(1)数据许可是纯粹的债权性许可。典型许可的法律性质较为复杂,学界对其的认知历经由“(类)物权”向“债权物权化”的转变,^④数据许可的法律性质则较为明晰。由于数据上不存在绝对权,因此数据许可合同具有纯债权属性,不产生物权法律效果。数据许可中只包含负担行为,不存在处分行为。基于数据许可所创设的数据使用权是纯债权性权利,不具备物权属性。(2)数据许可法中没有必要设置继受保护规定。继受保护被通俗地称为“转让不破许可”,是典型许可的核心特征之一,被视为使许可具有“债权物权化”属性的关键。^⑤ 在我国、德国、日本等国,继受保护规定普遍存在于知识产权法中。继受保护制度以无形财产上存在绝对权为基础,旨在处理被许可人在先的使用权与新手权利人继受取得的绝对权之间的冲突。然而,既受保护与数据许可并不匹配。由于数据所有权不是绝对权,不具有对世的排他性,因此数据交易中不存在上述权利冲突。当被许可人通过合法有效的许可合同获取并使用数据后,新手数据所有权人不享有针对被许可人的排他性权利。当然,为避免被许可人在一次性许可交易后享有永久的数据使用权,需要通过相应技术与法律措施设计具体使用权让与方式。(3)被许可人不享有针对第三人的独立诉权。在典型许可中,独占与排他性许可的被许可人享有独立诉权,即当第三人侵害其权益时,其可作为原告提

① Vgl. Klöppel, Der Lizenzvertrag, 2010, S. 24.

② Vgl. Kohler, Handbuch des deutschen Patentrechts in Rechtsvergleichender Darstellung, 2013, Rn. 508.

③ Vgl. Schur, Die Lizenzierung von Daten, GRUR 2020, 1142, 1145.

④ Vgl. McGuire, Die Lizenz, 2012, S. 537.

⑤ Vgl. Schur, Die Lizenzierung von Daten, 2020, S. 125.

起侵权之诉。由于数据许可具有纯债权属性,因此被许可人不享有针对第三人的独立诉权。诚然,当许可协议中存在相关授权约定时,被许可人可作为诉讼担当人为许可人的利益提起诉讼。^① (4)与知识产权排他性许可中的被许可人不同,数据许可中的被许可人不享有抵御破产与强制执行的能力。可见,数据许可所彰显的一系列特殊性都与数据上不存在绝对权继而不具有物权属性息息相关。

(二)数据许可合同的内容

数据许可合同是合同双方依据私法自治自主形成的调整双方利益关系的法律行为,其本质是为数据交易当事人提供行为规范。当事人遵循合同自由原则,依私法自治约定合同内容,以达成双方利益的平衡。以下试将对数据许可合同的重要条款进行分析。

1.数据持有与结果归属。数据交易旨在使用数据进行计算,因此输入数据的持有与输出数据的归属是数据许可合同的重要内容。对输入数据来说,双方首先会对数据进行特定化,即对数据的种类、范围、内容等因素进行非常细致的约定,这一内容对交易安全与交易对象的明确性具有重要的意义。双方将在合同中详细约定,何方是数据的持有人及其对数据享有何种权益。这一约定一般被包含在较为靠前的合同条款中,是许可人得以进行使用权许可的前提。对作为计算结果的输出数据来说,双方亦需对其归属做出明确的约定。一般来说,输出数据归被许可人使用。若在许可人事先拟定的合同中包含了许可人亦对计算结果享有权利的条款,则该条款很有可能被视为无效的格式条款。^② 此外,双方可以对被许可人能否将输出数据转让给第三人进行细致的约定。

2.数据质量。在计算机科学中,数据质量指在指定条件下使用时数据的特性满足明确与隐含要求的程度。在数据许可合同中,数据质量高低与是否具有合目的性息息相关,即数据能否满足被许可人的使用需求以达成合同目的。由于数据质量对于数据计算速度与计算结果的精确性具有重要意义,且可导致合同责任,因此双方会在合同中对数据质量作出细致的约定。我国2018年出台的《信息技术——数据质量评价指标》提出6大数据质量评价指标,分别是数据的规范性、完整性、准确性、一致性、时效性以及可访问性,每个指标都有较为细化的确定标准。在判断数据是否满足约定的质量标准时,有两个需要考量的因素:(1)是否满足质量标准需一事一议地进行判断,有时需在数据质量评估服务商的助力下完成;(2)合同中可约定双方可容忍的误差值,误差值之内的质量差距可以免责。^③ 在实践中,为了验证数据质量,双方一般会在签订数据许可合同之前签订前置评估协议,许可人会将数据样品提前提供给被许可人供其进行质量评估。^④

3.数据使用权让与。在数据许可合同中,许可人的主要义务是向被许可人提供数据使用权。具体而言,许可人须尽到一切必要努力使被许可人得以依约定方式获取与使用数据。如果数据获取需要借助特定技术,那么双方应通过单独技术保障条款加以详细约定。若相关技术措施由

^① 参见上海市第一中级人民法院课题组:《知识产权被许可人的诉权研究》,《东方法学》2011年第6期。

^② Vgl. Hennemann, Datenlizenzverträge, RD 2021, 61, 66.

^③ Vgl. Rosenkranz/Scheufen, Die Lizenzierung von nicht – personenbezogenen Daten – Eine rechtliche und ökonomische Analyse, ZfDR 2022, 159, 177.

^④ Vgl. Hennemann, Datenlizenzverträge, RD 2021, 61, 64.

许可人提供,则其亦应承担相应责任。此时,如果数据获取行为能够成为一个独立的技术服务合同或者承揽合同的对象,那么就可能存在混合合同。至于许可法律关系与其他法律关系的融合应适用吸收方法还是结合方法,需具体问题具体分析。

4.数据使用权行使。使用权行使条款是数据许可合同中最为核心的条款,在该条款中双方将对被许可人行使数据使用权的目的、方式、期限、权利限制等内容进行极为细致的约定。^① 上述约定为被许可人创设了清晰的行为指南,其有权使用数据,但是必须在合同约定的框架内行为。具体而言,使用权条款主要包含以下内容:(1)被许可人的数据权利:除了使用之外,其可否复制、转许可抑或编辑数据。(2)使用方式:是否需要将数据存储于本地设备、云抑或指定计算机网络,是否需要借助隐私保护技术,是否涉及与本地数据融合计算。(3)使用目的:数据许可合同中一般存在“目的限制条款”,一次许可仅限定于合同约定的特定目的。(4)权利限制:使用权在期限、地域等方面的限制。(5)许可类型:普通许可抑或排他性许可。由于数据具有使用上的非竞争性,因此除非双方对排他性许可作出明确的约定,否则都将视为普通许可。

5.数据隐私与安全。除支付相应对价之外,被许可人还负有数据安全保障义务。一方面,在获取数据后,被许可人负有保护数据免受丢失、盗窃、未获授权的获取与编辑的义务。必要时被许可人须在企业内部任命数据保护官承担相关职责。另一方面,被许可人在遭遇黑客攻击、征用、破产等可能危及数据安全的事件时,应立即将相关情况及其采取的措施告知许可人。如果合同约定此时许可人可要求被许可人销毁或归还相关数据,那么被许可人须履行相应义务。^②

可见,数据许可合同的诸多内容有赖于合同双方进行细致且明确的约定。而在约定不够明确的情况下,就涉及合同解释问题。相较于传统知识产权许可合同,数据许可合同须遵循不同的解释方法。在传统知识产权法中,许可合同的解释主要适用著作权许可合同中的经典理论:让与目的理论。其主要内容为,在双方就使用权让与的相关内容约定不明时,应尽可能限缩使用权的范围,将其限缩至达成合同目的所必需的程度。^③ 该理论旨在保护著作权人,使著作权人能够尽可能多地享有其作品产生的经济收益,故在约定不明时将权利保留于著作权人处。^④ 可见,让与目的理论是一种较为倾向许可人利益的解释方法,然而其无法适用于具有不同利益格局的数据许可合同。一方面,与作为数据持有人的许可人相比,被许可人通常处于更加弱势的合同地位,在其是中小微企业时更是如此。另一方面,数据法的规制理念与目的更具社会性,旨在使数据能够被更多人获取和使用,进而增进整个社会利益。因此,在解释数据许可合同时,宜回归民法中的一般合同解释规则,即根据许可行为的性质、目的、交易习惯以及诚信原则更加中立地解释争议条款。同时,确属必要时,在个案中可向被许可人的利益适当倾斜。

(三)格式条款效力审查机制

数据许可合同为数据交易提供了灵活、便捷、高效的私法工具,合同双方享有缔约自由、选择相对人自由以及合同内容自由等广泛的合同自由。然而,上述自由并非不受约束。如果一方滥

^① Vgl. Czychowski/Winzek, Rechtliche Struktur und Inhalt von Datennutzungsverträgen, ZD 2022, 81, 86.

^② See COPA & COGECA, EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement, 2002, p. 11.

^③ Vgl. Wandtke, in: Wandtke/Bullinger, Urheberrecht, 6. Aufl., 2022, § 31 UrhG, Rn. 41

^④ Vgl. Schulze, in: Dreier/Schulze, Urheberrechtsgesetz, 7. Aufl., 2022, § 31 UrhG, Rn. 110.

用不对等的协商地位,采用单方面预先拟定的不公平条款作为合同条款,那么相关条款就会落入格式条款的范畴,将接受效力审查且可能归于无效。如果将数据许可合同视为企业被授权形成的调整企业之间数据利益关系的规则,那么格式条款效力审查机制则是立法者通过指定的程序性、框架性规范对“私人立法”行为进行把控的手段。^①

通过对《民法典》第496条第1款进行文义解释、体系解释以及目的解释可知,格式条款可适用于商事合同。^②然而,由于商事交易与民事交易存在差异,而数据交易行为又是较为特殊的商事交易行为,因此需立基于数据交易的特点合理解释与适用规则。

格式条款的订入是进行效力审查的前提。相较于民事主体,法律对商事主体的谨慎程度与注意义务有更高的期待,故企业数据许可合同中格式条款的订入门槛更高,双方享有更程度的合同自由。首先,在合同主体方面,接受格式条款的一方须为中小微企业。鉴于大型企业不存在突出的受保护需求,大型企业之间的数据许可合同不存在适用格式条款制度的空间。相反,中小微企业之间签订的许可合同中则可能存在格式条款,中型企业对小微企业滥用协商地位即属此例。其次,在订入条件方面,“未与对方协商”被严格解释为“不容协商”。只有当中小微企业只能对条款表示同意或不同意但无法改变条款内容时,才触发格式条款的订入。若其未提异议直接接受对方预先拟定的条款,则属于合同自由范畴。最后,在条款内容方面,只有与数据获取与使用、数据提供义务的违反与终止等内容相关的条款才被认定为格式条款。除此之外,包括价款条款在内的其他条款都不受格式条款制度的约束,由合同自由原则统领。综上,企业数据许可合同中格式条款的定义是:由一方预先拟定的,向中小微企业提供且不容协商的,以数据获取与使用、数据提供义务的违反与终止为内容的合同条款。

格式条款效力审查机制的构建是法律确定性与灵活性的博弈。《民法典》第497条包含两项审查工具,一是第1款中的一般性规则,二是第2、3款中的黑名单制度。作为引致条款,一般性规则的主要内容是,违反强制性规定与违背公序良俗的民事法律行为无效。由于抽象的原则性规定具有广泛的适用性,可辐射未知的新兴不公平交易实践,因此一般性规则极具灵活性。在企业数据交易中,公序良俗突出体现为对遵循诚信公平的交易理念与良好商业惯例的数据交易行为的肯定与引导,有违诚信公平且严重背离良好商业惯例的合同条款将被判定为无效。《民法典》第497条第2、3款以黑名单的方式列举了合同条款无效的具体情形,与一般性规则相反,黑名单制度极具确定性,但因适用范围过窄而灵活性不足。对数据交易合同来说,包含下列内容且将导致双方利益严重失衡的合同条款无效:(1)限制或排除数据获取与使用权。(2)免除或减轻因违反数据提供义务、数据质量不达标而导致的违约责任。(3)免除或减轻因故意或重大过失给相对方造成损失而导致的侵权责任。

可见,一般性规则与黑名单制度分居法律灵活性与确定性天平的两端。在实践中,若格式条款仅导致双方利益的一般失衡,则无法落入黑名单的调整范围,此时法官只能根据一般性规则对相关条款进行审查,然而这并不高效。为提升审查效率,可考虑引入灰名单制度。不同于黑名单所蕴含的确定无效的法律后果,灰名单中所列举的条款被归为推定无效,即条款是否确定无效取

^① 参见董安生:《民事法律行为——合同、遗嘱和婚姻行为的一般规则》,中国人民大学出版社1994年版,第31页。

^② 参见殷秋实:《民法典第496条(格式条款的定义与订入控制)评注》,《中国应用法学》2022年第4期。

决于当事人是否有证据予以反驳。灰名单兼具确定性与灵活性,赋予当事人与法院在个案中更多的解释空间。实证研究表明,与黑名单相比,灰名单被视为更加不可或缺,众多国家将灰名单与一般性规则的搭配视为规制数据交易合同格式条款的首要选项。^①在数据交易情形中,灰名单中涵盖的合同条款主要包括如下内容:(1)允许一方以严重损害另一方合法利益的方式获取与使用数据,(2)允许一方以其他来源与质量标准的数据取代合同中约定的数据,(3)允许一方没有任何理由即可解除数据许可合同。在个案中,法官将按照黑名单、灰名单、一般性规则的顺序对格式条款进行审查。

(四)强制数据许可

如果说格式条款效力审查机制是对当事人合同内容自由的介入,那么强制性数据许可制度则是对缔约自由的强力干预。法律制度是利益平衡的产物,旨在将经过平衡的利益凝固于具体法律制度之中。各项法律制度皆由彰显其核心价值的制度利益所形塑,从而表现出不同于其他制度的性格与特征。^②在数据交易情境中,自愿许可与强制许可具有截然不同的制度利益,并基于此展现出差异化的制度构造。对于自愿许可来说,其制度利益在于促进数据的流通与使用,故双方当事人享有广泛的合同自由。而就强制许可而言,其制度利益是对超越了许可人私人利益的公共利益的保护。如果许可人在特定情形下的拒绝交易行为有损公共利益,那么就可以突破许可人的意愿,实施强制缔约。

数据强制许可是反垄断法对拒绝交易行为的规制结果。拒绝交易属于典型的滥用市场支配地位行为,被规定于《中华人民共和国反垄断法》第22条第3款。我国学者在研究数据强制许可时多在必要设施原则的框架下进行讨论。^③实际上,起源于美国判例法的必要设施原则只是拒绝交易反垄断法规制的一种特殊类型,^④其无法涵盖反垄断法中数据强制许可的全部情形。鉴于我国反垄断法未引入必要设施原则,本文将在拒绝交易规制的范畴内探讨数据强制许可。在数据交易场景下,如果具有市场支配地位的许可人无正当理由拒绝与被许可人进行交易,且被拒绝许可的数据对于后者在相邻市场的竞争来说不可或缺,加之拒绝交易行为很可能导致相邻市场中的有效竞争被排除,那么拒绝交易行为就可能因许可人滥用市场支配地位而被禁止,从而触发数据强制许可。强制许可制度主要解决许可人的缔约意愿问题,许可合同的具体内容仍有赖双方依私法自治加以约定。

一般情况下即便许可人具有市场支配地位,其也有权从自身利益出发决定是否与其他企业进行数据交易,拒绝交易行为不会招致反垄断法责任。然而,在满足特定条件时,拒绝交易行为将导致反垄断法的否定性评价进而触发强制缔约。数据强制许可是立法者对企业投资动机保护与相邻市场有效竞争这组相互冲突的利益进行利益衡量的结果。一方面,若放任许可人随意实施拒绝交易行为,则将导致相邻市场的竞争受损。另一方面,若对拒绝交易行为进行一刀切式的

^① See European Commission, Study on Model Contract Terms and Fairness Control in Data Sharing and in Cloud Contracts and on Data Access Rights (Executive Summary), 2002, p.8.

^② 参见梁上上:《制度利益衡量的逻辑》,《中国法学》2012年第4期。

^③ 参见周辉平:《大数据时代企业数据权益保护论》,《法学》2022年第5期;王健、吴宗泽:《论数据作为反垄断法中的必要设施》,《法治研究》2021年第2期。

^④ Vgl. Fuchs, in: Immenga/Mestmäcker, Wettbewerbsrecht, Band 1, 6. Aufl., 2019, Art. 102 AEUV, Rn. 331.

禁止,则将抑制企业的投资动机,进而损害整个数字经济的发展。最终,立法者将数据强制许可确定为拒绝交易行为不承担反垄断法责任这一一般规则的有限例外。^① 许可人须履行强制缔约义务的理由在于,鉴于其所具有的市场支配地位导致了数字市场结构的恶化,故其应为保障自由竞争体系承担相应的反垄断法责任。^② 由于数据强制许可具有不可小觑的负面效应,因此应严格限制其适用范围。不同于滥用市场支配地位对数字经济产生的直接性、毁灭性破坏,滥用相对优势地位往往更为直接地侵害微观个体利益,仅间接作用于市场秩序,且上述波浪式的能量传递更易被市场的自我调节消除,^③在具有相对优势地位的企业拒绝与他人进行数据交易的情形下,其无须承担反不正当竞争法上的强制缔约义务。

在世界范围内,数据巨头通过纵向一体化战略进入上下游市场,利用在相关市场的垄断地位,在杠杆效应的助力下获取相邻市场上的竞争优势已经屡见不鲜。^④ 在此背景下,数据巨头往往具有较强的拒绝交易动机。从是否存在既往交易的角度观察,拒绝交易可分为初次拒绝交易与中断既存交易两类。前者指在拒绝交易之前双方从未有过数据交易,后者指许可人以直接或间接拒绝的方式中断了双方持续进行的数据交易。这一分类对拒绝交易行为的认定具有重要意义,与初次拒绝交易相比,中断既存交易的认定门槛更低,实践中更容易被认定为拒绝交易行为。原因在于,既存交易使被许可人对作为交易对象的数据形成依赖,而许可人对依赖的形成负有责任。^⑤ 尤其在被许可人基于对本次交易的信赖已布局投资的情形下,中断既存交易极有可能被认定为滥用市场支配地位的拒绝交易行为。

执法机构对拒绝交易行为的认定是启动数据强制许可的前提。在个案中,执法机构在认定时通常考虑客观必要性、竞争排除性以及“无正当理由”这3个因素。^⑥ 首先,客观必要性意味着被拒绝交易的数据是被许可人在相邻市场进行有效竞争所必需的,其可进一步分解为3个递进式的标准:(1)无法在别处获取同类数据,(2)不存在可实现同一经营目的的其他数据,(3)拒绝交易将导致被许可人无法在相邻市场提供相关产品或服务。^⑦ 其次,竞争排除性指拒绝交易可能导致相邻市场的有效竞争被排除。在长期执法实践中,执法部门总结出了若干与竞争排除性相关的要素。具体而言,许可人在相邻市场的市场份额越高,拒绝交易涉及的相邻市场上的竞争者数量越多,在相邻市场上竞争者的产品或服务被许可人替代的可能性就越大,相邻市场上的客户

① 参见王健、吴宗泽:《论数据作为反垄断法中的必要设施》,《法治研究》2021年第2期。

② Vgl. Fuchs, in: Immenga/Mestmäcker, Wettbewerbsrecht, Band 1, 6. Aufl., 2019, Art. 102 AEUV, Rn. 305.

③ 参见龙俊:《滥用相对优势地位的反不正当竞争法规制原理》,《法律科学》(西北政法大学学报)2017年第5期。

④ 参见曾彩霞、朱雪忠:《数字经济背景下构建数据强制许可制度的合理性、基本原则和监管思路——基于数据作为关键设施视角》,《电子政务》2022年第2期。

⑤ See European Commission, Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009, para. 84.

⑥ Vgl. Paal, BeckOK InfoMedienR, 2017, Art. 102 AEUV, Rn. 42a.

⑦ Vgl. Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018, S. 133.

由竞争者转向许可人的盖然性越高,就认为拒绝交易行为的竞争排除性越高。^①最后,拒绝交易须不具有正当性理由,典型的正当性理由主要指个人信息保护、商业秘密保护等原因。

在数据交易实践中,拒绝许可行为很难同时满足上述3个条件。一方面,数据的特性使“客观必要性”的证明标准极高。另一方面,个人信息保护、商业秘密保护等正当理由为许可人提供了低门槛的免责路径。此外,具有谦抑性的反垄断法在面对我国方兴未艾的数字经济时,对强制性数据交易保持克制是执法部门更可能采取的态度。以上或许是迄今世界范围内尚未出现反垄断法适用下数据强制许可案例的原因之所在。毕竟,因公共利益而牺牲缔约自由的强制缔约制度已处于反垄断法规制的边界。

三、交易互信机制的建构:数据可用不可见

承上所述,数据交易以数据使用权为交易对象,以数据许可为交易方式。尽管数据交易模式已初见雏形,然而环顾全球,目前数据交易的规模远远未达预期。究其原因,交易互信的欠缺在相当程度上削弱了企业提供数据的动力。许可人的主要顾虑有两个方面:(1)数据是信息的载体,提供数据意味着被许可人将知晓数据所蕴含的信息内容,这将损害许可人的数据隐私与竞争力。(2)提供数据意味着,被许可人在获得数据使用权的同时亦获得了在事实层面控制数据的可能性,其可随意复制数据,甚至将数据提供给他人使用,这将导致许可人丧失对数据的控制。虽然双方可以通过契约方案约束被许可人的不当使用行为,但鉴于违约行为具有隐蔽性且蕴含着巨大的利润空间,合同的约束效果一般较为有限。

在数据交易中,能够增进交易互信的技术措施是法律制度的必要补充。目前,物理封闭、脱敏授权、可信第三方等传统互信方案已无法满足企业的需求。为切实打消许可人不敢提供数据的顾虑,探索符合数字时代要求的新型交易互信机制已势在必行。

(一)数据价值分割

使用权让与型交易的底层逻辑在于使用权的可控性。然而,数据许可则截然不同。鉴于数据易于复制且具有使用上的非竞争性,在实践中数据一经交付就意味着许可人在事实上丧失了对数据的控制。在许可关系存续期间,许可人无法控制被许可人是否依约使用数据,是否将数据提供给他人使用。在许可期间届满后,许可人亦无从确认,被许可人是否通过私下复制行为仍在继续使用数据。在此情况下,使用权失控的数据许可无异于数据买卖,数据使用权定价更是无法确定。为增进交易互信,打破数据交易的安全壁垒,实现使用权可控的数据许可,有必要首先对数据价值结构进行解剖。

数据具有双重价值:(1)信息价值,数据是对信息的记录,透过数据可以获知信息的具体内容,故信息价值是数据“可见”的价值。(2)计算价值。数据通过计算来实现其核心价值,企业将不同的数据组合代入特定算法函数,服务于具体结果的计算与预测,计算价值是数据“可用”的价值。在大数据时代,数据要素的核心价值体现为计算价值。

对数据交易而言,不应无视数据的特殊性,惯性地适用传统的商品交易理念。数据许可中使

^① See European Commission, Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009, para. 85.

用权失控的根本原因在于,交易者将蕴含着信息价值与计算价值的数据当然地视为一个不可分割的整体,且将“可见”视为“可用”的前提。秉持着上述思路,许可人须将明文或密文数据“交付”给被许可人使用,数据许可的结果是数据可用又可见。实际上,数据不是用来看(“见”)的,而是用来计算(“用”)的,数据交易的目的是不是使被许可人了解数据所蕴含的信息内容,而是使被许可人得以利用数据进行价值挖掘与计算,从而获得需要的计算结果。因此,若能将数据的信息价值与计算价值分割开来,切断“可见”与“可用”之间的必然联系,使数据“可用不可见”,则可在相当程度上打消许可人的顾虑,实现使用权可控的数据许可。具体而言,在数据交易中,数据仍保留于许可人处,数据可见的信息价值不出域,交易流通的只是数据不可见的计算价值,被许可人无法看到明文或密文数据本身,只能得到使用数据进行计算后的结果且无法倒推出原始数据。

(二)交易互信的技术保障:隐私计算

为使数据计算结果更有针对性地服务于企业的经营实践,数据使用方通常会将本地数据与提供方数据进行融合计算。隐私计算致力于解决多方数据融合应用中的交易互信问题,以实现数据在交易过程中的“可用不可见”,是目前实现数据交易互信的最现实的技术解决方案。隐私计算是在保证数据提供方不泄漏原始数据的前提下对数据进行分析计算的一系列信息技术,是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。^① 隐私计算可在技术层面实现数据信息价值与计算价值的分割,保证流通交易的仅为可用的计算价值,使用方只获悉计算结果,而对数据提供方的原始数据一无所知。隐私计算主要有3大技术方向,分别是多方安全计算、联邦学习和可信执行环境。由于可信执行环境高度依赖硬件环境,因此多方安全计算与联邦学习是目前国内更为主流的隐私计算技术。

在数据交易中,隐私计算服务由技术提供方提供。技术提供方是为数据交易双方提供隐私计算服务的主体。隐私计算技术是数据交易的计算控制站和算力调配中心,是机密计算和高效算力的结合体,能够助力多方数据在融合计算的基础上产生新的数据。^② 技术差异使技术提供方的服务方式存在区别。在以多方安全计算为主的应用场景中,技术提供方根据数据提供方与数据使用方之间的具体约定,设计算法并调配算力执行相关隐私计算,且将计算结果传输给数据使用方。多方安全计算技术可在有效区隔数据信息价值与计算价值的基础上,实现对数据定性、定量的计算,即“数据可用不可见,用途可控可计量”。

在以联邦学习为主的应用场景中则遵循不同的交易互信保障思路,技术服务方首先根据数据使用方的需求设计相关模型并将模型发送给数据提供方与数据使用方,各方在本地使用约定范围的数据按照约定的方法训练相关模型,并于训练结束后将不涉及原始数据的中间结果发送到技术提供方的服务器,如梯度、模型参数等。技术服务方在收到各方的中间结果后对全局模型进行更新,并将优化后的模型再次发送至各方,各方继续用本地数据对模型进行训练,周而复始,直至模型收敛为止。可见,在联邦学习技术的适用场景中,数据提供方在本地对模型进行训练,传输的对象是模型的中间结果而非原始数据本身,即“数据可用不可见,数据不动模型动”。

^① 参见中国信息通信研究院安全研究所、阿里巴巴集团安全部、北京数核科技有限公司:《隐私保护计算技术研究报告(2020年)》, <https://www.vzkoo.com/document/3fbee591fc7f6027ff5e2769e785085f.html>, 2023-07-26。

^② 参见《华控清交 CEO 张旭东:数据“可用不可见”和“规定用途用量”,让数据真正成为生产要素》, https://www.sohu.com/a/403847307_114778, 2023-07-26。

综上,隐私计算技术致力于实现“原始数据不出域、数据可用不可见”,是实现数据交易互信的重要技术保障。数据提供方在保留数据信息价值的前提下,将特定数据的特定使用权出让给数据使用方。双方可以就数据的具体用途与用量作出约定,指定算法并约定数据的使用次数或频率,每次运算结果的获取都是对数据特定使用权的消费。

(三)技术服务法律关系

在适用隐私计算技术的交易场景中存在两个法律关系:(1)数据许可法律关系,(2)技术服务方、数据提供方与数据使用方三方通过签订协议创建的技术服务法律关系。在技术服务法律关系中,数据提供方的数量不唯一,因为数据使用方可能同时需要多方数据进行联合计算。在特定场景中,一个主体可能身兼双重或多重角色。例如,大型互联网公司若同时拥有隐私计算技术并持有数据,则在其需要外部数据进行联合计算时其既是数据使用方又是技术提供方。由于此时数据许可法律关系与技术服务法律关系的主体完全一致,因此双方可通过签订一份协议创建综合性的数据安全交易法律关系。

在技术服务法律关系中,数据使用方为委托人,技术提供方为受托人。受托人有义务在充分了解委托人需求的基础上,设计相关隐私计算方案,按照约定完成隐私计算服务,保证计算质量,并传授解决技术问题的相关知识。委托人有义务按照约定完成配合事项,接受计算结果并支付报酬。数据提供方亦在技术服务法律关系中负有相应配合义务,如将数据导入多方安全计算平台加密转换为计算因子或者在本地训练并上传相关模型。在商业实践中,技术方往往不仅提供技术服务,而且需要为数据使用方提供一套完整的问题解决方案,尤其是为其找到合适的数据来源。在此情况下,技术服务方还扮演着居间人的角色,与其他两方之间形成居间法律关系。实际上,实践中技术服务方存在销售模式、服务模式、调用模式、分润模式等多种服务模式,^①各服务模式存在差异化的法律关系,可通过个案分析加以确定。

各方对数据安全的重视使数据安全保护条款成为技术服务合同的重要内容。一方面,技术提供方有义务保证技术的安全性,具体包括客户端与融合端两个地点。在客户端,技术提供方须保证,无论是多方安全计算中的安全计算节点,还是联邦学习中训练数据所用的模型,都不得访问及存储客户端的数据。在融合端,技术服务方有义务确保,无论是安全多方计算中的合作节点,还是联邦学习中的全局模型,也都无法对计算结果进行解密并倒推出原始数据。另一方面,数据使用方与数据提供方亦负有相应安全保障义务。双方不得通过中间或最终计算结果倒推对方的原始数据。诚然,法律上设置的安全保障义务与违约条款只能在一定程度上使合同当事人不敢违约,若想实现更为完善的保护效果,则必须配合使当事人不能违约的各项技术保障,如多方安全计算中的不经意传输协议^②。

四、结 语

企业数据交易模式的构建涉及民法、知识产权法以及反垄断法等多个部门法。本文旨在构

^① 参见微众银行、金融科技微洞察、毕马威:《深潜数据蓝海——隐私计算行业研究报告(2021年)》, <https://max.book118.com/html/2021/0410/7101004112003113.shtm>, 2023-07-06。

^② 不经意传输协议是一种广泛应用于多方安全计算的密码学协议,能够在技术上保证数据传输双方的隐私,使发送方与接收方无从知晓对方的完整数据。

建以数据使用权为核心的交易模式,即以数据使用权为交易对象,以数据许可为交易方式,并依托隐私计算技术实现交易互信。首先,数据交易对象是数据使用权。以使用权作为交易对象能够使数据发挥更大价值,契合数据法社会本位理念并助力实现数据法的规制目标,即保障数据的流通、获取与使用。数据使用权源于企业数据持有权,是基于技术控制产生的弱民事权利,具有有限的处分与排他权能。其次,数据交易方式为数据许可。由于数据上不存在绝对权,因此数据许可具有诸多特殊性。许可人与被许可人在设定合同内容时享有广泛的合同自由,格式条款效力审查机制与强制许可制度则用来确保合同自由不失边界。最后,隐私计算技术可构建交易互信,实现“数据可用不可见”。隐私计算可在技术层面实现数据信息价值与计算价值的分割,保证流通交易的仅为可用的计算价值,使用方只获悉计算结果。技术服务方、数据使用方与数据提供方通过签订协议创建技术服务法律关系,数据安全保护条款是技术服务合同中的重要内容。

Abstract: The construction of enterprise data transaction mode can be subdivided into three aspects: transaction objects, transaction methods and mutual trust in transactions. First of all, the transaction object is the data usage right. Using the data usage right as the transaction object can help data to exert greater values, conform to the “society as the standard” conception of data regulation law, and ensure the accessibility and usability of data. The source of the data usage right is the data holding right as a weak civil right. Secondly, the transaction method is data licenses. Data licenses are atypical licenses, which have many special features different from typical licenses. The specific content of the data license contract is agreed upon by both parties in accordance with the principle of contract freedom, and the review mechanism for the effectiveness of standard clauses and the compulsory licensing system is used to ensure the freedom of contract without losing boundaries. Finally, the mutual trust guarantee of transactions is privacy computing technology. On the basis of dissecting the value structure of data, privacy computing technology can be used to realize “the original data does not go out of the domain, and the data is usable but not visible”. A technical service legal relationship is formed between the technology provider, the data provider, and the data user.

Key Words: data transaction, data usage right, data holding right, data license, the mutual trust guarantee of transactions

责任编辑 张家勇