

共有数据隐私保护的法律困境及其多维治理机制

李棠洁¹, 池悦²

(1. 广州医科大学 卫生管理学院, 广东 广州 510182; 2. 吉林大学 理论法学研究中心, 吉林 长春 130000)

摘要: 共有数据作为多主体共同参与形成的数据形态, 具有权利叠加与价值复合等特征, 其隐私保护面临保护与利用失衡、权利配置冲突以及规范适用分散等多重困境。在界定共有数据内涵及其法律关系的基础上, 引入类型化与场景化相结合的分析框架, 从主体结构、数据形态与权利内容等维度区分隐私风险, 结合数据生命周期中的具体场景, 构建差异化的数据权利配置与隐私保护规则。提出共有数据隐私保护应通过多维度治理机制实现隐私保护与数据利用之间的动态平衡, 以提升共有数据治理的针对性与制度适配性。

关键词: 共有数据; 隐私保护; 数据共享; 类型化; 场景化

中图分类号: D922.16

文献标志码: A

文章编号: 1009-2013(2026)02-0069-09

The legal dilemma of shared data privacy protection and its multi-dimensional governance mechanism

LI Tangjie¹, CHI Yue²

(1. School of Health Management, Guangzhou Medical University, Guangzhou 510182, China;

2. Theoretical Law Research Center, Jilin University, Changchun 130000, China)

Abstract: As a form of data generated through the participation of multiple stakeholders, shared data is characterized by the superimposition of rights and the compounding of value. Its privacy protection faces multiple dilemmas, including imbalances between protection and utilization, conflicts in the allocation of rights, and the fragmented application of legal norms. On the basis of defining the connotation and legal relationships of shared data, this study introduces an analytical framework that integrates typology and contextualization. It differentiates privacy risks across dimensions such as subject structure, data form, and rights content, and develops differentiated rules for data rights allocation and privacy protection in conjunction with specific scenarios throughout the data lifecycle. The study proposes that privacy protection for shared data should be achieved through a multi-dimensional governance mechanism to strike a dynamic balance between privacy protection and data utilization, thereby enhancing the specificity and institutional adaptability of shared data governance.

Keywords: shared data; privacy protection; data sharing; typification; contextualization

一、问题的提出

当前, 数据已成为新型的生产要素, 数据的产生速度和数量达到了前所未有的水平, 大数据的广泛应用促进了各行各业的创新和发展, 但同时也带来了诸多隐私安全问题。共有数据作为一种重要的

数据类型, 成为数据隐私保护的重点领域。共有数据由多个数据主体共同所有, 属于涉及多个个体或群体的数据, 具有共享性、复杂性和多样性等特点, 在隐私保护层面面临着多主体权利冲突、责任界定模糊以及利用与保护平衡难度倍增等挑战。共有数据与公共数据、共享数据之间存在区别, 共有数据的“共有”强调的是数据的所有权, 由两个及以上主体所有; 而公共数据则是指由公共部门收集、存储并进行分析利用的数据; 共享数据强调的是数据在使用权上的多主体共同享有, 换言之, 共享数据的所有权可能仅归属于某一单一主体, 但该主体将

收稿日期: 2025-12-06

基金项目: 教育部人文社会科学研究青年基金资助项目(20YJC820023)

作者简介: 李棠洁(1981—), 女, 湖北赤壁人, 副教授, 主要研究方向为卫生法学。

数据共享给他人使用。在承认数据具有一定财产属性的理论框架下,可以将多个主体对同一数据的权利关系理解为一种“共有”结构。即使基于“数据去产权化”立场,不将数据纳入传统财产权范畴,多主体之间围绕同一数据所形成的利益关联与控制关系,仍然呈现出“共有特征”,因而有必要加以专门分析。

国内外关于数据共有的研究主要围绕两个方面展开:第一,共有数据的法律监管;第二,共有数据的具体治理路径^[1]。针对共有数据的法律监管问题,国外学者普遍认为数据共有长期缺乏有效监管与公众监督,会导致隐私保障义务履行不充分^[2]。如,G.Birckan等^[3]指出,行业监管的缺失与快速技术进步之间的矛盾,加剧了共有数据环境下的隐私风险;Amo Daniel等^[4]则强调,现有法律框架与隐私协议对数据控制者的约束力与威慑力不足,难以有效遏制共有数据被泄露与滥用的行为。就国内研究而言,王利明等^[5]在探讨个人信息共同处理者的责任分配时指出,在共有数据场景中,如何具体界定各主体的权利义务缺乏细化规则;张新宝^[6]则从数据权利体系构建的角度提出,共有数据的“共同所有权”属性使得传统知情同意机制难以有效运作,亟需引入动态同意或分层同意机制以适应其特殊性。针对共有数据具体治理路径的讨论,学者们从多学科和多角度提出了对现有共有数据治理的方案^[7]。如,Chih-Liang等^[8]通过比较共有数据治理的美欧模式,指出欧盟通过严格的同意机制与目的限制原则,为规范数据运营者行为提供了更具约束力的制度范式。在技术治理方面,有学者^[9]提出构建隐私计算框架,以实现不暴露原始数据前提下的协同计算与价值挖掘;还有人^[10]则尝试引入经济激励机制,探讨如何通过参数化模型平衡隐私披露与经济利益回报。Daniel Neyland等^[11]进一步强调了市场干预与多方协调在应对新兴数据产品监管中的重要性,呼吁构建包含多利益相关方的协同治理体系。国内学者李海英、马民虎^[12]提出应当建立中国特色社会主义数据所有权制度——共有制,从而推进数据基础制度体系构建,进一步激发数据要素潜能和价值,不断提高我国的数字化建设能力,创造新的国际竞争优势。齐延平等^[13]从数据治理的公共性角度提出,我国应建立“政府—平台—用户”三

方协同的治理结构,以应对共有数据中公私利益交织的复杂局面。

总体来看,现有研究为理解数据治理问题提供了有益的理论参照与问题切口,但在此基础上,仍存在以下有待深化的缺陷。第一,现有研究多将共有数据与共享数据混同讨论,对“共有数据”这一特殊形态的聚焦深度不足。第二,缺乏对共有数据隐私保护研究的系统类型化梳理。第三,现有研究未能充分回应共有数据隐私保护在实践中的复杂性与动态性,缺乏深入探讨与体系化构建。鉴于此,本文针对“共有数据隐私保护”这一核心问题,致力于弥补现有研究的上述不足。

二、共有数据的内涵及所涉法律关系

数据作为“信息的载体”,其中可能包含隐私信息,从而凸显了数据隐私保护的重要性。与传统单一主体数据不同,共有数据的隐私保护面临更为复杂的理论挑战。其一,从权利属性看,隐私权属于人格权范畴,而传统民法关于共有物的规范主要围绕财产属性展开,对其所承载的精神利益关注不足;其二,从客体属性看,数据具有可复制性与非损耗性,突破了传统民法对“物”的物理形态假设,使其难以完全适用既有物权规则。正因如此,共有数据隐私的界定与保护,有必要在现有民法框架下进行适度调适,以回应数据这一新型客体所带来的制度挑战。

(一) 共有数据的内涵与主要特点

共有数据的隐私就是指两个或两个以上的主体所共有的数据当中所蕴含的隐私信息,这些隐私信息既包括来源于数据提供者的个人隐私信息,也包括作为整体的蕴含企业商业秘密的信息。共有数据隐私与个人数据隐私存在以下几点区别:

首先,相比于个人数据的主体,共有数据主体具有多元性和综合性,涉及企业、组织或个人等多个数据持有主体共同拥有数据的情形。此类数据可能涵盖个人隐私、商业秘密等多种信息类型,其处理、交易与使用需兼顾多方主体的权益与隐私保护。其次,共有数据隐私因包含商业秘密信息而具有更强的排他性。在共有数据场景下,数据经过处理分析后往往形成独特的商业价值,从而具备了商业秘密的属性,这种属性进一步强化了共有数据隐

私的排他特征。最后,共有数据隐私的保护呈现出非固定性特质。这类数据的特殊性在于,其既包含作为自然人隐私权内容的信息,也包含作为法人财产权内容的商业秘密。当自然人信息数据经汇集、分析后转化为以商业秘密形态存在的隐私时,便同时兼具了上述两种法律属性。

综上,由于共有数据涉及数据提供者、法人及其他组织等多方主体,其隐私保护不仅涵盖人格权项下的隐私权,还涉及法人人格理念影响下数据所蕴含的商业秘密。

(二) 人身价值与财产价值的兼具

传统观点认为隐私是“人的延伸”,对隐私的判定也注重从主体的主观角度展开。例如,《中华人民共和国民法典》(以下简称《民法典》)所规定的私密空间、私密信息、私密活动,均指向特定情境下的单个主体。以往关于隐私法律保护的讨论侧重于人身价值,但在数字化时代,数据作为信息载体承载了多重价值,既包含传统的个人私密空间、私密信息、私密活动,也涵盖企业的商业秘密。由此,共有数据的隐私价值得以延伸,除人身价值外,还体现出财产价值与企业信誉价值。相应地,在对其实实施法律保护时,既需注重第一层面对个人人格权益的保障,也需关注第二层面对企业财产权益的维护。

(三) 不同情形下的共有关系内容

数据的可复制性及复制的非损耗性,决定了同一数据可在同一时间内被不同主体所占有,这使得“共有”超出了民法上的原初含义。数据作为一种“物”,其核心在于数据信息本身。法人对个人数据进行汇集、分析等行为并未改变数据信息的本质,因此即便法人与自然人所拥有的数据在表现形式上存在差异,二者所享有的仍是同一数据。若不借助“共有”来解释这一现象,则难以说明为何在自然人未丧失数据权利的前提下,法人亦能主张对数据的相同权利。在此意义上,共有数据的“共有”并不要求主体在物理意义上共有某一特定的有体物,而仅要求事实上特定自然人与法人都能对同一数据主张权利即可。同时,各共有主体对数据享有的均为完整权利,这与普通物的共有存在重要区别。对应于共有数据隐私保护的两个层次,数据共有的情形可分为以下两种:

第一种情形为所有原始数据提供者共有—一个数据集。此时聚合后的数据集可拆分为若干份额,每一份额对应原始数据提供者所提供的数据。对于此类数据集产生的经济效益,各原始数据提供者可依其数据份额主张分配。因此,此种情形可按按份共有的方式处理。

第二种情形为经过处理后的数据的共有,具体表现为数据收集者与数据分析者的共有。在实践中,数据收集与分析形成大数据产品的过程常涉及多个主体,出于收益共享与风险共担的目的,数据收集者与处理者通常约定二者共有某一数据集。

(四) 双重价值引致多方规则适用

共有数据隐私保护既需关照人格权的维护,又需在财产权保障层面通过所有权能的扩展延伸促进数据财产价值的发挥。

一方面,在人格权益维护上,共有数据隐私保护涉及《民法典》隐私权保护及《中华人民共和国反不正当竞争法》等相关法律规范。由于共有数据包含了原始提供者被收集的各类隐私信息,因此共有权能发挥的首要前提是不得侵犯个人隐私权利。

另一方面,在发挥共有数据的财产价值上,需运用《民法典》关于共有物的相关规范以及与数据处理相关的政策法规。《民法典》第二分编“所有权”第八章“共有”规定了共有的类别、共有人的权利义务、共有物的分割等内容。此外,关于数据处理的相关政策法规亦是促进共有数据发挥经济价值的重要依据,如《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》(《数据二十条》)以及行业规范、地方性法规等。

此外,由于共有数据在现实中多体现为企业之间对某一数据产品的共有,因此商业秘密保护相关的法律规范也成为共有数据隐私保护的重要依据。

三、共有数据隐私保护的多维度难题

(一) 保护与利用的价值张力

几乎所有数据都面临着保护与利用之间的权衡问题。一方面,数据关联着个人隐私、国家安全等重要权益,在利用过程中极易造成侵害。另一方面,数据作为一种具有极大潜力和价值的“沉睡的资源”,应当得到充分利用,以顺应数据产业发展的浪潮,确保我国在数据发展中保持领先地位。有

学者指出,数据资源的最大价值就在于重复利用,数据价值的释放与叠加也依赖数据流通共享^[13]。从这个意义上来看,保护与利用之间的平衡难题并非共有数据所特有的问题,而是所有数据利用均需考量的共性问题。

就性质而言,共有数据的所有权分别归属于数据所有者与数据使用者,二者处于相互重叠或交缠的状态,难以直接认定哪一方享有最终处分权。如果数据所有者与数据使用者就保护与利用何者优先达成一致,则两种价值的排序便具有确定性。问题在于,不同主体对共有数据的态度往往是不可预知的。通常情况下,数据所有者更倾向于保护个人信息,而数据使用者更倾向于发掘数据经济价值;但也不排除数据所有者更希望以个人信息换取经济价值,而数据使用者基于不同理由不愿实现数据的经济价值、倾向于对数据进行保密保护的情形。

由于在共有数据中数据所有者与使用者的权利处于叠加状态,难以对二者的权利进行清晰分配与优先性判断,因此不能简单地以“对数据所有者的数据权利以保护为主,而对数据使用者的数据权利以鼓励应用为主”的方式处理。这导致在共有数据的保护与利用之间,不仅要做事先的价值判断,还须听取当事方意见,在个案中具体衡量,从而增加了价值判断的难度。

(二) 独占与共享的权力冲突

数据作为一种特殊的“物”,既具有一般物的特征,又与传统的物存在区别,其中最典型的是其具有可复制性。对于传统物而言,同一物上仅能存在一个物权。物的共有,本质上是不同主体共享同一物的所有权,因而各主体均无法享有完整的所有权。但由于数据具有可复制性,共有数据的本质在于不同主体能够完整享有对数据信息的所有权。从这个意义上说,尽管本文遵从学界一般称谓,将自然人称为“数据所有者”,将法人称为“数据使用者”,但实际上这两类主体在某种意义上都是“数据所有者”,只不过其所有数据的表现形式不尽相同。

更复杂的是,由于数据所有者与数据使用者均在完整意义上共享数据的所有权,二者的权利相互叠加与纠缠,因此从理论上来说,双方均可主张对数据的控制权。在共有数据框架下,由于双方都对数据的产生做出贡献,难以判断哪类主体享有控制

权。实践中,数据所有者与数据使用者往往同时主张对数据的控制权,甚至进一步提出排他性主张,从而引发权利冲突。

由此可见,共有数据的权利结构具有内在张力:一方面,不同主体基于各自的投入与利益诉求,强化其对于数据的控制,在实践中表现为对数据支配权的强化主张;另一方面,由于数据本身具有可复制性与非排他性,传统意义上的“排他性支配”在现行制度下难以完全成立。这种“控制强化”与“排他受限”之间的张力,构成了共有数据在“独占”与“共享”之间的制度性难题。

(三) 多元规范的适用失序

个人信息保护规范与数据隐私规范在目的上存在差异。前者强调数据收集和处理的合法性、必要性与最小化原则,侧重于对个体信息权益的保障;后者则在保障隐私的前提下,更注重数据的流通与利用,旨在促进信息共享和技术创新,推动社会经济发展与科技进步。

在共有数据背景下,上述两类规范的适用冲突更加凸显。共有数据既可能包含受个人信息保护规范约束的个体信息,又承载着促进数据流通利用的价值追求,因而时常同时受到两类规范的调整。当共有数据涉及多个个体或群体的信息时,如何平衡个体权益保护与数据流通利用之间的关系,成为法律适用中的核心难题。

四、共有数据隐私保护的可适用理论

(一) 系统分析视角下的类型化理论

在共有数据隐私保护问题中,单一规则难以应对多主体参与、权利交叠以及数据形态多样所形成的复杂结构,因此有必要引入类型化理论作为分析工具。所谓类型化,并非对数据进行一般的经验分类,而是基于法律评价的需要,对具有不同权能分布与风险特征的数据和使用情形进行规范意义上的区分,从而为隐私保护下差异化规则的适用提供理论基础。本文所采用的“系统分析视角”,是指将共有数据隐私保护视为一个由权利主体、数据形态与权利内容共同构成的复合系统,而非孤立地对某一要素进行考察。在这一视角下,类型化的功能不在于描述数据本身,而在于识别不同法律关系结构下数据隐私相关风险和法律问题的差异,并据此确

定相应的保护路径,从而实现差异化规则的适用。

具体而言,共有数据隐私保护至少涉及三类需要加以类型化区分的核心要素:其一,权利主体的类型化,即区分数据提供者、数据处理者与数据使用者等不同主体,以明确在相关权利配置与义务承担上的差异。其二,数据形态的类型化,即区分原始数据与加工数据,或将数据基于组织形式与结构化程度分为结构化/半结构化/非结构化数据^[14],以揭示不同数据形态在可识别性、处理方式及再识别风险等方面的差异。其三,权利内容的类型化,即区分控制权、使用权与收益权等不同权能在共有结构中的配置状态,以明确各类权能在隐私保护与数据利用中的边界及其行使条件。

基于此,系统分析视角下类型化的意义在于,它并非提供一般性的数据分类框架,而是作为一种规范分析工具,在避免对共有数据隐私保护适用“一刀切”的统一化规则的同时,根据不同情形下的利益结构与风险程度,分别配置差异化的隐私保护标准。在此基础上,还可结合数据的共享程度与安全敏感程度,对共有数据适用差异化的保护强度。例如,已进入公共流通领域的数据,其隐私保护强度相对较低;而涉及个人隐私或商业秘密的高敏感数据,则应适用更严格的访问控制、使用限制与责任规则。

(二) 动态观察视角下的场景化理论

场景理论强调在特定的情境或环境中理解和解释行为、事件或现象,将“场景”作为认识研究对象的重要外部环境,由此构成该理论的重心。这一理论与类型化既存在联系也存在区别。二者都强调在不同应用情境中对隐私保护强度进行差异化调整,在价值指向上均反对“一刀切”的形式化适用,在规范结论上均导向差异化治理,因此整体功能具有相似性。但二者的侧重点有所不同:类型化理论强调对数据本身的层级化、类型化处理,其功能在于对数据作出更细致的区分;场景化理论则强调在具体个案中结合场景、行为条件与主体诉求等个性化因素进行考量,其功能在于形成更具针对性的处理方案。若以数学上的坐标轴作比,类型化可视为纵轴,场景化则构成横轴。换言之,不同的数据类型可能出现在同一场景中,不同场景中的数据也可能归属于同一类型。

在数据隐私保护的领域中,场景理论的应用尤为重要。共有数据隐私保护糅杂诸多法律问题,主体客体纷繁,需要置于具体场景中加以细化分析。不同主体在不同场景中有不同的利益、诉求和期望,法律不能简单一刀切,而需结合类型化理论,在具体情景、环境和条件中规制和保护共有数据隐私^[15]。应根据不同场景的需求、利益状况与风险,综合制定针对性的政策、规范与行为准则,通过对数据流转、处理、存储及共享等环节的细致剖析,评估隐私泄露的可能性、影响范围及潜在后果,从而明确哪些数据在哪些场景下需要更高保护级别,以合理分配资源,实施更为严密的保护措施。

场景理论为共有数据的合法、合规使用提供了明确指南。数据控制者与处理者可依据具体场景中的指引规范自身行为,从而提升数据使用的合法性、合规性与安全性。同时,可基于不同环节制定相应的监管要求:在传输过程中采用先进加密技术,维护数据的安全传输;在存储环节运用匿名化处理或差分隐私技术,降低个人隐私泄露风险;在共享过程中实施细粒度的访问控制与审计追踪机制,防止数据滥用与泄露。由此,构建起全方位、多层次的共有数据隐私保护体系。

五、共有数据隐私保护的多方面展开

(一) 类型化保护路径

对共有数据隐私进行类型化保护,意味着根据数据的不同属性和应用场景,采取不同的保护策略。具体而言,可以从价值类型化、权利类型化和规范类型化三个维度展开。从现行法律规范来看,相关规定虽各有侧重、自成体系,但均可为类型化保护提供解释空间,需借助法律解释等方法论技术将其串联,形成系统性的规范解释框架。例如《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第1条即明确其制定目的是“规范个人信息处理活动,促进个人信息合理利用”,也就是说,它并未只强调个人信息的隐私价值或财产价值,而是强调对这两种价值的合理调和。《国家安全法》在第四章和第五章分别规定了一般的数据安全保护义务与政务数据的安全与开放制度,尤其是在政务数据部分,进一步确定了数据所有人、数据收集人与可能的数据使用受托人等不同主体在

不同阶段的权利与义务。此外,根据《中华人民共和国数据安全法》第19条,国务院相关部门还出台了《关于加强数据资产管理的指导意见》,各个地方政府也制定了大量关于数据交易的地方性法规或规章,如《广西数据交易管理暂行办法》《深圳市数据交易管理暂行办法》等,对此需在具体案例中进行系统性解释。

1. 隐私价值与财产价值平衡下的类型化

作为平衡数据共有与隐私保护的关键策略,共有数据价值类型化保护的核心理念在于精准识别并差异化应对数据中蕴含的隐私价值与财产价值。

对于原始共有数据的保护,首要的任务是构筑起坚固的隐私防线。为此,技术层面可采用更为先进的数据加密技术,确保数据传输与存储过程中的安全;同时利用数据脱敏处理技术,对敏感信息进行模糊处理,降低数据泄露的风险。管理层面则需建立健全的访问控制机制,明确数据访问权限,并建立审计跟踪制度,以便在发生安全事件时快速溯源并采取补救措施。

另一方面,对于经过处理后的共有数据,应侧重于维护数据持有者的财产权益。具体而言,可通过知识产权法、合同法等法律手段,为数据持有者提供坚实的法律保障^[16]。同时,应建立完善的数据资产评估与定价机制,为数据交易提供科学合理的依据,激发数据市场的活力与潜力。

2. 数据持有者具体权利配置下的类型化

权利类型化保护是共有数据隐私与财产权益维护的核心,具体体现为对数据持有者在数据处理全流程中各项权利的配置与实现路径的细致划分。

首先,数据所有权作为数据持有者的基本权利,即使在共有数据的复杂背景下也需得到清晰界定与尊重。每位数据持有者对其所贡献的原始数据均享有不容置疑的所有权。这种所有权不仅赋予了数据持有者对数据的直接控制与使用权,还涵盖了他们参与数据处理决策并监督处理过程的权利^[17]。同时,这种所有权还隐含着对数据处理活动潜在风险的知情与评估权,使数据持有者能在充分知情的基础上作出理性决策。

其次,数据处理权是数据持有者在数据处理流程中的核心权利。它涵盖了从数据收集、整理、分析到挖掘与利用的全过程。为确保数据处理活动的

合法性与正当性,数据持有者必须明确界定数据处理的目标、方法、范围,并采取一切必要的安全措施来维护数据的完整性与隐私性^[18]。

最后,数据收益权作为数据持有者参与数据处理活动的经济动力,其重要性不言而喻。数据持有者不仅有权就其提供的原始数据获得相应的经济回报,还有权在数据产品交易、许可使用及数据服务等领域分享收益。

3. 数据处理生命周期分阶段下的类型化

规范类型化保护是确保共有数据隐私在不同阶段和场景中得到全面有效保障的重要策略,其核心在于精准对接数据生命周期的各个关键环节,综合运用现行法律法规、政策文件及行业标准,以制定并实施具体、细致的保护规范。

数据收集阶段的首要任务是确保数据来源的合法性与数据质量的可靠性。数据持有者必须严格遵守相关法律法规以及行业标准。此阶段应建立健全数据质量控制机制,确保所收集数据的真实性、准确性和完整性。对于涉及个人隐私或商业秘密的敏感数据,应采用加密、脱敏等先进技术手段进行处理,以防止数据泄露或被非法利用。同时,建立数据收集活动的审计与监督机制,确保收集过程的透明与合规。

数据处理阶段需将合规性与安全性置于首位。应明确数据处理的目的、方式和范围,制定详尽的数据处理计划并严格执行。此阶段还需严格遵守相关法律法规与行业标准,确保数据处理活动的合法性与正当性。对于涉及个人隐私或商业秘密的数据处理行为,务必征得数据主体的明确同意,并充分告知数据处理的目的、方式和潜在风险,确保数据处理的透明度与合规性。

数据使用阶段则侧重于确保数据使用的合理性与规范性。数据持有者应根据数据使用的目的和范围,制定科学合理的数据使用策略,确保数据使用的合法性与正当性。此阶段应建立健全的数据使用审计机制,定期对数据使用活动进行审查与评估。同时,完善数据泄露应急响应机制,确保在发生数据泄露等安全风险时能够迅速响应、有效应对,最大限度减少损失。

数据交易阶段应保障数据交易的合法性与公平性。应建立健全的数据交易市场规则与监管机

制,确保数据交易的合法合规。对于涉及个人隐私或商业秘密的数据交易行为,必须严格遵循相关法律法规与行业标准。在交易过程中,应征得数据主体的明确同意,并明确告知数据交易的具体细节与潜在风险。此外,建立完善的数据资产评估与定价机制,确保数据交易的公正性与合理性,促进数据市场的健康发展。

(二) 场景化规制方案

根据尼森鲍姆的学说,对信息进行规范时需加以权衡的参数包括:具体化的情景场域、行为主体、信息类型及其本质特征、传输原则^[19]。综合考虑共有数据隐私的特征及其实践场域,可将共有数据的价值周期分为三个具体场景:一是权利分享或共有权生成的场景,二是共有数据加工场景,三是市场机制下共有数据的流转场景。

1. 原始数据共有化的场景化隐私保护

原始数据共有化是所有共有数据共同的生命周期起点,此过程中隐私保护的担忧若不卸除,共有数据的价值将难以进一步释放。但此种状态下的共有实际上仅为潜在共有,实质上的共有规则并未生效。因为此时个人信息仅表现为碎片化的、具有明显个人特征的数据信息,还未经由他人汇聚、分析和处理而转换为其他形式的共有数据。因此,在这里既要保护数据所有者的权利予以充分保护,也不能因此完全切断后续利用和发展相关数据的可能性。

如果站在原始数据来源者的立场,基于个人信息自主的观念,个人资料的所有权应归属个体本人,而非由数据控制权派生的占有者。但如果站在数据处理中生产要素提供者的立场,则可能倾向于认为,孤立的个体信息呈碎片化特征且缺乏独立价值,唯有通过特定方式、基于特定目的加以集中与处理,所形成的数据库或数据集合方能体现经济价值。而且,《民法典》人格权编和《个人信息保护法》并未试图网罗和保护所有物理意义上的个人信息数据,仅当某一数据与受保护的权益或法益相关联时,才会进入法律的评价范围。在此背景下,基于共有客体的可复制特性,一旦共有共同体中的其他成员滥用其特权^[20],或该共同体的范围不当扩张^[21],共有人难以援引物上请求权寻求救济。因此,欧盟等立法对数据的实际控制方课以更重的义务,以强化对原始数据隐私的预防性保护^[22]。这一做法对我国

立法与实践亦有启示。

2. 共有数据加工中的场景化隐私保护

共有数据的加工处理是其价值实现的关键环节,因为数据的商业价值主要在该环节中被开发与实现^[20]。数据使用者在对数据所有者的个人信息进行处理并形成新的表现形式后,亦成为该数据的所有权人。

数据处理主要关注对原始数据的收集、整理、转换和分析,旨在通过清洗、格式转换、挖掘等操作,提升数据的质量和增值。在域外立法中,欧盟的数据库指令重视数据处理者的劳动价值增值,因而承认处理后数据的自身利益^[23]。我国有观点认为,数据处理不仅涉及处理前后两组数据之间的关联,处理后数据本身亦成为新的权利客体^[24]。也有学者指出,有必要区分数据信息与数据载体(如存储器、硬盘等),二者的权利归属应分别判断^[25]。国家发展和改革委员会发布的《数据基础制度若干观点》承认数据持有者的自主管理权,将排他性数据支配的附加利益赋予数据持有者,一定程度上认可了其基于私益管理数据的权利^[26]。

基于这一基础价值判断,结合处理后数据在客体形态和价值分配上与原始数据的区别,可借助《民法典》第322条物之添附的规定,构建共有数据在加工情景下的权利保护范式。数据加工后价值明显超出原始数据价值的,应将其完整的所有权赋予数据处理者^[27]。在隐私保护方面,通过处理过程充分消除个人隐私,从而实现隐私保护规范的自然豁免,是数据处理者的普遍追求,亦应受到法律的尊重^[28]。当然,处理后数据本身若具有商业秘密或知识产权上的法益,法律应予保护,应无疑义。

3. 数据交易流转中的场景化隐私保护

相比于数据处理,数据交易强调的是将数据作为商品进行买卖,其目的在于实现数据的财产价值。共有数据交易场景的隐私保护可以划分为原始数据交易中的隐私保护和加工数据交易中的隐私保护。原始数据交易发生在数据所有者与数据使用者之间。此时不仅需要保障数据所有者的信息安全,还需要保障数据所有者与数据使用者在数据交易中的权利。而加工数据交易通常是数据使用方与第三方的交易,此时对数据所有者隐私的保护义务主体就从数据使用方扩展到数据使用与购买双方。

学界对原始数据交易中的隐私保护多有讨论,但是结合法律规范及实施周期来看,无论是引入行政监管责任强化控制主体保护意识^[29]、重构权衡机制以协调多方利益^[30]、建构多元主体共治责任体系^[31],亦或是借鉴域外统一立法模式^[32],都难以有效纾解实践困境。对交易客体作出二元划分之后,以“转介性条款”和“引致条文”为核心内容进行保护体系的立法指引,再辅以执法程序和司法制度进行实践衔接^[33],或许是一条可行性较高的路径。首先,对共有人中数据处理者的行为约束应当以我国《个人信息安全规范》的内容为规范指引^①。其次,以比例原则为基准对共有人处理数据的行为进行考察。企业数据合规监管部门应当进行“定性”和“定量”的双重审查,判断数据处理行为是否满足“最小范围”的要件^[34]。

加工数据交易中的隐私保护不仅涉及共有人中数据处理者的行为规制,更涉及交易环境的安全保护。在数据交易前会产生新的内部争议,即共有数据转变所有权人后,产生的加工数据这一新型客体是否会损害其他共有人的隐私。前文已述,法律对此种情况应当保留一定空间,但同时要进行必要干预^[35]。因此,本文提出以内部治理为主的方式进行隐私保护。首先,数据处理者应当自觉履行隐私保护义务,进行合规审计。而数据购买者应当遵守相关法律设置的隐私保护规范。其次,通过外部监督机构对相关活动进行引导和监督,确保数据处理和交易在法律框架内运行,有效平衡数据利用与隐私保护之间的关系。最后,通过公权力介入的方式,以企业信用评价机制为基础要求数据处理者定期公开数据交易中的隐私保护履行情况。

注释:

① 参见《信息安全技术个人信息安全规范》(GB/T 35273-2020)第11.1-11.7条。

参考文献:

- [1] 倪千森. 政府数据开放共享的法治难题与化解之策[J]. 西南民族大学学报(人文社会科学版), 2021, 42(1): 82-87.
- [2] 李卓卓, 张楚辉. 数据伦理框架: 国际对话与中国化的构建路径[J]. 情报学报, 2024, 43(2): 154-166.
- [3] Birckan G, Dutra M, De MACEDO D, et al. Effects of data protection laws on data brokerage businesses[J].

ICST transactions on scalable information systems, 2020, 27(20): 12-29.

- [4] Amo D, Fonseca D, Alier M, et al. Personal data broker: A solution to assure data privacy in EdTech [C]// Learning and collaboration technologies: Designing learning experiences, Orlando, FL, USA, 2019: 3-14.
- [5] 王利明, 丁晓东. 论《个人信息保护法》的亮点、特色与适用[J]. 法学家, 2021(6): 1-16, 191.
- [6] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
- [7] Rouvroy A, Poullet Y. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy[M]//Gutwirth S, Poullet Y, De Hert P, et al, Reinventing Data Protection, Springer, 2009: 45-76.
- [8] Yeh C L. Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers[J]. Telecommunications policy, 2018, 42(4): 282-292.
- [9] Al- Neyadi F, Abawajy J. A privacy preserving service broker architecture for data sharing[C]//Kim T. Lee Y H, Kang, et al. Future generation information technology (FGIT 2010), Jeju Island, Korea, 2010: 450-458.
- [10] Parra-Arnau J. Optimized, direct sale of privacy in personal data marketplaces[J]. Information sciences, 2018, 424: 354-384.
- [11] Neyland D, Milyaeva S. The entangling of problems, solutions and markets: On building a market for privacy[J]. Science as culture, 2016, 25(3): 305-326.
- [12] 李海英, 马民虎. 我国数据跨境流动的治理框架与实践方案[J]. 图书与情报, 2022, 42(6): 50-57.
- [13] 齐延平, 李旭. 个人数据保护论争中的隐私权: 反思、还原与再定位[J]. 山东大学学报(哲学社会科学版), 2021(4): 95-106.
- [14] 封海波. 迈向“数据治理”: 数据确权方案的本土争论与理论调和[J]. 法理——法哲学、法学方法论与人工智能, 2024(2): 180-199, 371-372.
- [15] 黄尹旭. 和合共生: 公共数据治理的“传统-现代”互融式建构[J]. 法治社会, 2024(3): 116-126.
- [16] 尹西明, 陈劲, 王冠. 场景驱动: 面向新质生产力的数据要素市场化配置新机制[J]. 社会科学辑刊, 2024(3): 178-188.
- [17] 齐爱民. 区块链环境中个人信息保护的法律障碍与应对[J]. 现代法学, 2022, 44(5): 180-193.
- [18] 罗有成. 数字权利论: 理论阐释与体系建构[J]. 电子政务, 2023(5): 50-62.
- [19] Nissenbaum H. Privacy as contextual integrity[J]. Washington law review, 2004, 79: 119-158.
- [20] 徐玖玖. 从“数据”到“可交易数据”: 数据交易法律治理范式的转向及其实现[J]. 电子政务, 2022(12):

- 80-89.
- [21] 王融. 关于大数据交易核心法律问题——数据所有权的探讨[J]. 大数据, 2015(2): 49-55.
- [22] 全国信标委大数据标准工作组. 数据要素流通标准化白皮书[M]. 北京: 中国标准出版社, 2022: 53.
- [23] 刘再春. 我国政府数据开放存在的主要问题与对策研究[J]. 理论月刊, 2018(10): 110-118.
- [24] 刘武朝, 温春辉. 过度收集用户隐私数据行为的竞争损害及反垄断法规制[J]. 价格理论与实践, 2021(7): 65-70.
- [25] 李延舜. 位置何以成为隐私?——大数据时代位置信息的法律保护[J]. 法律科学(西北政法大学学报), 2021, 39(2): 107-118.
- [26] 唐要家. 中国个人隐私数据保护的 mode 选择与监管体制[J]. 理论学刊, 2021(1): 69-77.
- [27] 孙晋, 马姗姗. 反垄断视野下数据开放与隐私保护的冲突与协调[J]. 武汉大学学报(哲学社会科学版), 2024, 77(6): 154-166.
- [28] 袁静, 周欣丽, 臧国全, 等. 政府开放数据隐私风险研究: 现状、特征及展望[J]. 图书情报知识, 2024, 41(4): 67-81.
- [29] 杨张博, 王新雷. 大数据交易中的数据所有权研究[J]. 情报理论与实践, 2018, 41(6): 52-57.
- [30] 尹博文. 个人数据交易中知情同意规则的破局与重构[J]. 科技与法律(中英文), 2022(5): 85-94.
- [31] 焦俊峰, 李晓东. 大数据时代个人信息保护的治理体系研究——基于技术信任和专家系统的二分框架[J]. 电子政务, 2022(12): 35-45.
- [32] 张帆, 李春光. 数据流通交易平台的全生命周期治理路径研究[J]. 学习与实践, 2022(5): 78-84.
- [33] 徐梦瑶. 大数据中的隐私流动与个人信息保护研究[J]. 东南大学学报(哲学社会科学版), 2022, 24(S1): 46-49.
- [34] 刘雪婷. 数字经济时代个人信息保护的法治规范及机制构建[J]. 吉首大学学报(社会科学版), 2022, 43(4): 137-147.
- [35] 武腾. 最小必要原则在平台处理个人信息实践中的适用[J]. 法学研究, 2021(6): 71-89.

责任编辑: 黄燕妮

(上接第 49 页)

- [25] 林忠, 刘亦飞. 组织变革理论变迁[J]. 产业组织评论, 2013, 7(3): 129-145.
- [26] 张陶然. 结构耦合、过程闭环与功能实现: 矛盾纠纷数字化治理的警务实践逻辑[J]. 中国人民公安大学学报(社会科学版), 2025, 41(4): 145-156.
- [27] 杨柳, 唐学兵. 矛盾纠纷预防化解法治化的时代意蕴与实践向度[J]. 理论视野, 2024(11): 54-60.
- [28] 薛澜, 赵静. 走向敏捷治理: 新兴产业发展与监管模式探究[J]. 中国行政管理, 2019(8): 28-34.
- [29] 任勇. 重视新时代“枫桥经验”的数字治理面向[J]. 探索与争鸣, 2023(8): 21-23.
- [30] 张静. 案例分析的目标: 从故事到知识[J]. 中国社会科学, 2018(8): 126-142+207.
- [31] 罗伯特·K. 殷. 案例研究: 设计与方法[M]. 重庆: 重庆大学出版社, 2017: 63.
- [32] 范逢春. 基层治理“小马拉大车”问题的成因及破解[J]. 人民论坛, 2024(11): 23-26.
- [33] 王思斌. 社会工作机构在社会治理创新中的网络型服务治理[J]. 学海, 2015(3): 47-52.
- [34] 蓝宇蕴. 经济强镇社会治理探索与“社会性”培育——以佛山市南海区狮山镇为例[J]. 学术研究, 2024(8): 61-69, 177.
- [35] 何阳, 王俊. 农村人民调解效能变化机理及增效策略——基于“三治”环境的分析框架[J]. 湖南农业大学学报(社会科学版), 2022, 23(1): 55-62.
- [36] 于显洋. 组织社会学[M]. 北京: 中国人民大学出版社, 2002: 272.
- [37] 周雪光. 组织社会学[M]. 北京: 社会科学文献出版社, 2003: 166.
- [38] 林彬, 刘红波. 逆向压力型体制与农村基层政府空转执行的形成逻辑——基于粤西 L 镇数字资源下沉的考察[J]. 经济社会体制比较, 2023(3): 151-161.
- [39] 顾丽梅, 宋晔琴. 超大城市敏捷治理的路径及其优化研究——基于上海市“一网统管”回应社情民意实践的分析[J]. 中国行政管理, 2023(6): 6-14.
- [40] 王小华, 吴双虹. 化“数字”为“数治”: 数字素养与村民社会治理参与[J]. 湖南农业大学学报(社会科学版), 2025, 26(1): 62-71.
- [41] 刘瑞平, 王建新. 居民矛盾纠纷化解模式的选择偏好及其影响因素——基于平安北京调查数据的分析[J]. 中国人民公安大学学报(社会科学版), 2024, 40(5): 100-111.
- [42] 于洁阳. 行政吸纳社会: 过渡型乡村人民调解实践及其功能困境分析——以苏南 A 村为例[J]. 湖南农业大学学报(社会科学版), 2023, 24(5): 83-94.
- [43] 马作宽. 组织变革[M]. 北京: 中国经济出版社, 2009: 175.

责任编辑: 黄燕妮