SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

LEGAL RESEARCH
法律研究中心
Alibaba Group

领羊

数字经济生产关系构建

数据要素“三权分置”理论范式及其实践路径研究

COPYRIGHT STATEMENT

版权声明

出品方

上海社科院互联网研究中心

上海赛博网络安全产业创新研究院

阿里巴巴法律研究中心

瓴羊智能科技有限公司

编写组成员

惠志斌　上海社会科学院互联网研究中心主任

　　上海赛博网络安全产业创新研究院首席研究员

李　宁　上海赛博网络安全产业创新研究院高级研究员

周雪静　上海赛博网络安全产业创新研究院高级研究员

王　莹　阿里巴巴集团法务总监

顾　伟　阿里巴巴集团法律研究中心副主任

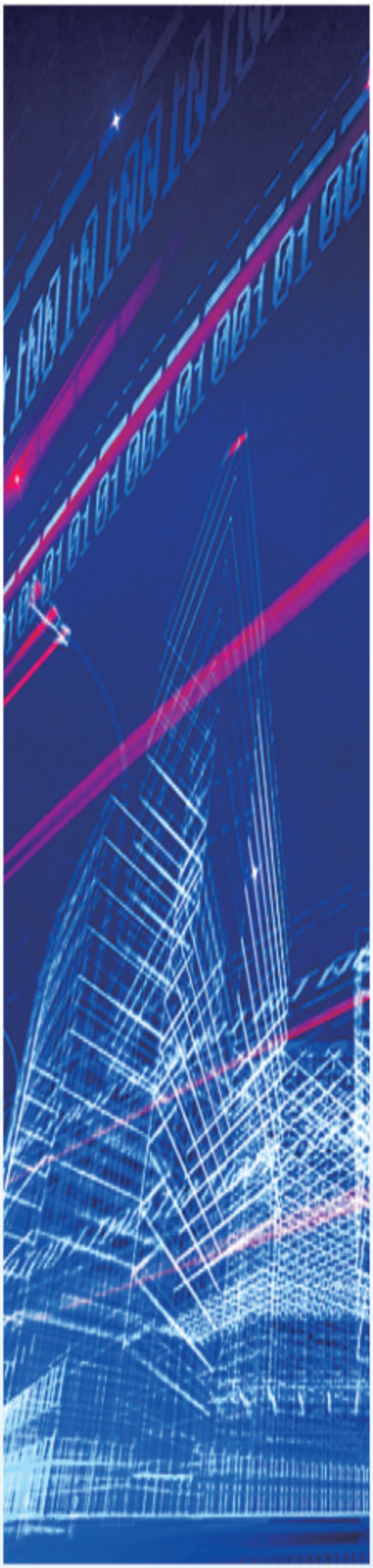
姚　栋　瓴羊智能总法律顾问

田喜清　阿里巴巴集团法律研究中心高级研究员

徐彩曦　阿里巴巴集团高级法律专家

目录

contents



前　言

随着数字经济的快速发展，数据作为生产要素的重要性日益凸显。我国近年来大力推进数据要素市场建设，促进数据要素流通和价值充分释放。但一直以来，数据确权、交易定价、流通规则等问题使得我国数据交易和数据流通并不活跃。2022年12月，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，成为我国数字中国和数据要素市场建设的纲领性文件，对释放数据要素的经济和社会价值具有根本性的意义，也是为解放数字生产力，在生产关系层面进行的一场大的变革。该意见创设性地提出数据资源持有权、数据加工使用权、数据产品经营权“三权分置”的产权制度，为破解数据高效合规流通提供了理论指引，引发了社会各界的高度关注。“三权分置”的数据产权制度框架以解决市场主体遇到的实际问题为导向，淡化所有权、强调使用权，聚焦数据使用权流通，将大大激发数据要素市场活力。

当前，“三权分置”的数据产权制度框架如何在产业实践中落地成为广泛关注的问题，社会各界都在翘首以盼国家层面配套政策法规细则的出台。在此背景下，上海社科院互联网研究中心、赛博研究院联合阿里巴巴法律研究中心等开展了《数据要素“三权分置”理论范式及其实施路径》的课题研究。本报告作为课题研究成果，旨在基于目前我国数据流通发展现状和数据流通普遍存在的问题，聚焦不同数据流通参与主体的权利、责任和收益的分配机制，呈现我国“三权分置”数据产权制度框架在产业实践中的实施路径。

第一章 当前我国数据流通发展现状与挑战

1.1 数据流通相关概念界定

在对数据要素流通和数据产权分置进行分析之前，有必要对数据相关的多个不同术语进行明晰，包括当前经常提到的“数据资源”“数据资产”“数据产品”等术语。

数据资源：随着数字经济的快速发展，数据成为一种关键的国家战略资源。《数据要素流通标准化白皮书》[1]定义“数据资源”为“可供人类利用并产生效益的一切记录信息的总称，并属于一种社会资源”。《全国统一数据资产登记体系建设白皮书》[2]认为“原始数据积累到一定规模，且经过必要的加工清洗处理、被独立部署存储的、具有潜在使用价值，便形成了数据资源”。《数据价值化与数据要素市场发展报告（2021年）》[3]中对“数据资源”的定义为能够参与社会生产经营活动、可以为使用者或所有者带来经济效益、以电子方式记录的数据，区别数据与数据资源的依据主要在于数据是否具有使用价值。可见数据资源是具有使用价值的一类资源，这是被一致认可的。

在此基础上，**本报告认为，数据资源是对持有或使用主体的社会生产经营活动具有一定使用价值的数据的统称。**

数据资产：数据资产是从经济角度对数据的认知。《数据要素流通视角下数据安全保障研究报告》[4]认为“数据资产是数据的经济维度，并非所有的数据都构成数据资产，数据资产是能够为组织产生价值的数据资源”。在《信息技术服务 数据资产 管理要求》（GB/T 40685-2021）中，数据资产是指合法拥有或控制的，能进行计量的，为组织带来经济和社会价值的数据资源。中国电子技术标准化研究院编著的《数据资产评估指南》[5]将数据资产定义为组织合法拥有或控制的、能进行计量的、能为组织带来经济利益和社会价值的数据资源。中国资产评估协会发布的《资产评估专家指引第 9 号—数据资产评估》[6]对数据资产的定义是由特定主体合法拥有或者控制，能持续发挥作用并且能带来直接或者间接经济利益的数据资源。

本报告认为，数据资产必须是组织合法持有或控制的，这是形成资产的前提；其次数据资产的核心是经济利益，应能为组织带来直接或者间接经济利益；再次，数据资产

---

[1] 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，2022年11月

[2] 上海数据交易所有限公司：全国统一数据资产登记体系建设白皮书，2022年8月

[3] 中国信息通信研究院政策与经济研究所：数据价值化与数据要素市场发展报告（2021年），2021年5月

[4] 中国信息通信研究院安全研究所：数据要素流通视角下数据安全保障研究报告（2022年），2022年12月

[5] 中国电子技术标准化研究院：数据资产评估指南，2021年

[6] 中国资产评估协会：资产评估专家指引第9号——数据资产评估，2020年1月

的本质是组织可对其行使权利，但权利的范围应该是受限的，是建立在法律规定或合同约定范围内的受限权利。

数据产品：数据产品是商品化的数据资源形态。《数据要素流通标准化白皮书》将“数据产品”定义为“利用数据辅助做出决策的一种产品，数据产品包含了供应原始数据、数据加工过程、数据展示、数据结论、数据解决方案等服务和形式”。《全国统一数据资产登记体系建设白皮书》认为“数据产品是指作为产品的数据集，或者是从数据集中衍生出来的信息服务”。李晓珊在《数据产品的界定和法律保护》[7]中将“数据产品”定义为：网络运营者通过合法手段获取到原始数据，对原始数据采用一定的算法，经过深度的分析过滤、提炼整合及脱敏处理后而形成的具有交换价值和技术可行性的衍生数据。《深圳市数据产权登记管理暂行办法（征求意见稿）》将“数据产品”定义为“自然人、法人或非法人组织通过对数据资源投入实质性加工和创新性劳动形成的数据和数据衍生产品，包括但不限于数据集、数据分析报告、数据可视化产品、数据指数、API数据、加密数据等”。

本报告认为，数据产品是基于合法获取的原始数据和衍生数据，采用一定的加工处理手段，形成的具有经济价值的商品化的数据资源或数据服务。

1.2 当前我国数据流通发展情况

数据流通是指以数据资源或数据经计算加工后形成的数据产品为流通对象，以其中蕴含的价值为流通驱动力，按照一定规则机制和流通模式向数据需求方提供的过程。当前，随着国家政策明确数据为重要的生产要素，社会各界都在积极探索和参与数据流通，以期充分释放数据要素价值。

1. 各行各业对数据流通的需求呈现逐步增长或显现趋势。金融行业对外部数据的需求较为旺盛，主要集中在风控领域，近年来，金融机构成为外购数据（包括数据服务）的重要市场主体，数据来源包括各类银行、电信运营商、社交平台等，基于更大的数据规模和更多维度的数据类型，金融机构可以建立更精准的风控体系。互联网也是数据流通较为频繁的领域之一，互联网平台可能持有用户的基本资料、习惯偏好、网络环境等类型的数据，目前互联网领域的数据流通主要用于跨平台营销、为中小企业提供客户数据管理、商业决策参考等数据智能服务。此外，医疗、气象、交通、政务等领域的数据流通在逐步兴起。

2. 数据流通多数基于场外的“一对一”或“一对多”模式，场内交易模式尚处于发

[7] 李晓珊：数据产品的界定和法律保护[J].法学论坛,2022,37(03):122-131

展初期。目前，我国接近80%的数据流通发生在场外[8]，大多数通过一对一的直接流通模式开展数据流通活动，即数据提供方和数据需求方直接通过双方洽谈、签订协议及数据对接完成数据流通。另外一种较为普遍的场外交易模式（“一对多”模式）是数据提供方利用自身持有的数据，通过一定方式的数据加工或计算，如数据汇总、统计分析等，向多方市场主体提供数据产品或服务。对场内交易而言，虽然我国近几年多地都在积极建设数据交易所等数据交易平台型机构，但由于数据权属、定价等多方面瓶颈加之市场需求不旺盛，我国数据交易场内成交率不高，数据交易市场尚处于培育阶段。

3. 参与数据流通的主体更加多元。目前在数据流通场景中，除了数据供需双方以外，出现了数据技术服务商、数据加工服务商、数据服务提供商、数据中介、数据经纪人等多类型的第三方市场主体。有的大型企业也会成立专门的数据智能公司，基于自身数据在合法基础上开发数据产品或服务，或研发相关安全技术能力，旨在充分利用数据价值并更好地服务客户。另外，顺应市场需求，出现了一批专业从事数据采集、清洗、标注、预处理等业务的数据加工商，为数据需求企业提供专业化服务。但由于目前我国整体数据流通和数据交易仍处于培育阶段，因此数据服务生态尚处于发展初期。

4. 数据流通对安全技术的需求越来越大。当前数据安全保障成为数据流通的前提，如何建立可信和安全的数据流通方式成为迫切需要解决的挑战之一。当前，隐私计算、区块链、数据脱敏、安全沙箱等数据安全技术的应用在一定程度上解决了数据安全的部分问题。例如隐私计算已在广告营销、金融风控、医学研究等方面为数据跨主体融合应用提供了解决方案，在对原始数据加密的情况下对数据进行计算，使得数据流通过程中供需一方无法获取对方的原始数据，在此基础上实现数据的可用不可见、安全可控与最小必要，为数据供需两端主体提供更加安全可信的数据计算和流通环境，增加双方之间的信任。

1.3 当前我国数据流通存在的挑战

1. 数据持有方合规顾虑重，参与数据流通的意愿不强。近年来，我国对数据安全和个人信息保护监管趋严，先后出台了《数据安全法》《个人信息保护法》等多部法律法规，尤其是《个人信息保护法》出台以来，数据违规使用和数据泄露事件带来的合规成本越来越高，企业对处理个人用户数据更加审慎，普遍存在出于合规顾虑不愿对外提供数据的情况，甚至同一企业、同一集团公司内不同部门、不同子公司之间的数据流通均存在顾虑。

[8] 中国信息通信研究院安全研究所：数据要素流通视角下数据安全保障研究报告（2022年），2022年12月

此外，当前数据流通参与主体各方的数据安全保护能力参差不齐，导致整个数据流通链条的整体数据安全保障水平不足，进一步降低了数据提供方共享数据的意愿。不同数据流通参与主体之间数据安全责任的划分、界定和分担机制尚不明确，也导致数据提供方流通数据的意愿不强。

2. 数据产权制度尚未建立，缺乏数据流通的确权机制。数据不同于其他的传统生产要素，数据的产生可能涉及个人、企业等不同利益方，需要在数据流通过程中解决多方数据主体权益和安全方面的诉求。数据的权属问题一直是业界争论的焦点问题，但目前社会各界仍未就数据所有权或产权问题达成共识。而数据的流通亟需确定参与主体各方的权利，包括对数据进行加工、使用、分析和产生收益的权利。当前我国直接关于数据产权及相关财产权益分配的法律基本处于空白状态，对于数据财产性权益保护而言，除了在可适用的情况下通过商业秘密和著作权保护外，目前主要通过反不正当竞争法对数据权益提供一定程度的保护。但是，反不正当竞争法框架下的保护仍存在受保护的数据类型、不正当行为认定标准不明确等问题。数据流通参与主体缺乏权利与财产权益主张的法律依据，成为阻碍数据流通的关键瓶颈之一。

3. 数据流通配套的制度细则和标准尚未建立。当前我国数据交易市场在数据主体准入、数据交易规则、数据定价、数据安全标准、数据监管规则方面，尚缺乏统一的配套制度细则和标准，各地场内数据交易市场的规则也不尽相同。这一方面导致场内数据交易的优势不明显，市场主体参与场内交易的积极性不足，我国场内交易始终处于不活跃状态。另一方面，场外交易参与方之间信任的建立，也缺乏法律、宏观政策的有效支撑。

4. 数据安全技术尚处于发展初期，缺乏规模化应用和合规上的正向激励。当前，隐私计算成为数据安全流通的关键支撑技术，通过实现数据加工利用过程的可用不可见，达到保护数据隐私与数据安全的目的。隐私计算包括联邦学习、多方安全计算、加密计算、同态加密等多种技术，目前已在一些数据流通场景有所应用，但离大规模商用还有一定距离。一方面，隐私计算的技术标准尚未建立，目前市场上隐私计算的技术水平参差不齐，影响了其应用的实际效果。另一方面，不同隐私计算技术路径之间的差异性导致平台之间的适配性不足，也是阻碍其大范围推广的重要因素。

更为关键的是，隐私计算本身意味着较高的技术成本，但是法律及国家标准层面尚未直接且具体地认可隐私计算对个人信息保护、数据安全的价值，企业利用隐私计算缺乏合规上的正向激励，很多企业不愿意“过度”投入。

第二章 我国“三权分置”数据产权制度理论创新

当前规则完善的数据要素市场尚未建立，我国数据流通仍处于发展初期和市场培育阶段。在这一背景下，2022年12月19日，中共中央、国务院印发了《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》），成为我国数字中国和数据要素市场建设的纲领性文件。以下将从数据要素权利配置的特点和数据流通的复杂性来阐述创新数据产权观念和构建数据产权制度框架的必要性。

2.1 构建新型数据产权制度的必要性

新型数据产权制度是构建数据基础制度的基础和核心。数据作为新型生产要素，具有无形性、非消耗性、可复制等特点，对传统产权、流通、分配、治理等制度提出新挑战，亟需构建与数字生产力发展相适应的新型生产关系。在数据要素市场的培育期，核心任务是构建数据要素基础制度，这对于充分释放数据要素价值，激活数据要素潜能具有重大意义。而由于当前大量市场主体困惑于对持有数据可主张的权益范畴，因此新型数据产权制度是构建数据基础制度和真正释放数据潜能的基础和前提。

数据所有权思路阻碍数据要素真正高效流通。数据作为新型生产要素，具有无形性、非消耗性等特点，可以接近零成本无限复制，对传统产权、流通、分配、治理等制度提出新挑战。传统生产要素的权益配置建立在绝对排他的所有权基础之上，但是数据相比于土地、劳动力等生产要素更加复杂，无法通过排他性占有来划分类似的产权配置体系。就数据要素生产过程而言，无论是来自消费互联网还是来自工业互联网的数据，数据要素常常从一开始就是多方主体围绕网络平台共同参与、协作生产的结果[9]，其中不仅包含了原始数据主体的信息内容，更是融合了平台企业主体在其中所投入的资本和技术等因素。数据之上承载了多方主体的不同合法权益，呈现出典型的“权利束”状态。这就决定了，数据产权制度的构建无法以基于传统要素特点的“所有权”制度为基础。基于科斯产权理论，产权体现的不是人与物的关系，而是人与人之间的关系[10]。因此，数据产权制度的构建应搁置数据权属争议，其核心任务应在于确认各个参与主体在数据价值链上分别主张且相容的数据权益。

讨论数据权益的配置应在剖析数据标的特征及应用场景的前提下进行。在实际的数据价值开发利用过程中，真正参与整个利用环节的数据形态往往已经不是原始数据，而

[9] 熊丙万：数据产权制度的理论挑战与现代回应，2022年12月

[10] 庞晓提，潘玥：解析数据产权制 构建数据基础制度意义重大，2022年12月

是经过加工后的衍生数据，其个人可识别性或企业敏感性已相对弱化，对侵害个人或企业主体权益的风险已经非常低或可通过建立机制被有效管理。抛开数据的形态、敏感程度属性及具体应用场景而单纯谈论数据的权属关系是无意义的，应就具体的数据种类、数据的风险级别，在具体的场景中，进行细粒度的数据权利关系配置。这对数据资源持有方能否就数据开发利用等权利进行授权至关重要，而只有权利流通起来才能实现数据要素的真正流通。

2.2 “三权分置”产权制度的理论创新

《数据二十条》构建了数据产权、数据流通和交易、数据要素收益分配和数据要素治理等四个方面的制度框架，提出了20条政策举措，可以说为推动数据在更大范围内有序流动和合理集聚、进一步促进数据价值转化应用指明了方向。其中《数据二十条》提出数据资源持有权、数据加工使用权、数据产品经营权“三权分置”的产权制度，是一种极具创新性的制度安排，是对数字经济时代围绕数据要素应有的生产关系进行的一次体系重构。

“三权分置”产权制度是促进数据要素流通的现实路径。《数据二十条》创新性地提出构建“数据产权结构性分置制度”，即在关于数据权属的建构上淡化甚至放弃了“所有权”概念。具体而言，《数据十二条》初步提出了数据资源持有权、数据加工使用权和数据产品经营权。值得注意的是，《数据二十条》并没有穷尽列举所有的权利，数据的产权还可以在这三种权利以外进行扩展。其中“数据资源持有权”是对应“所有权”而提出的一项新型权利，数据处理者可以有权依照法律规定或合同约定自主管控所取得的数据资源，如不存在法定正当事由，且未经持有人同意，他人不得侵扰权利人对数据资源的稳定持有状态[11]。数据加工使用权和数据产品经营权则是在数据资源持有权基础上衍生出的可对外授权的价值链后端的权利种类。结构化分置的数据产权制度将大大解放数字生产力，促进数据真正释放其价值。

“三权分置”产权制度将促成数据产业领域的专业化分工。一方面，社会越是向前发展，就越是要求社会分工的进一步深化和细化，“三权分置”鼓励数据的加工挖掘和产品经营交由更专业的机构来开展，保护参与主体对数据的合法持有、加工和经营状态，促进数据精细化加工，推动数据产品专业化经营，这将加速数据价值的充分释放和数据要素市场的建立。《数据二十条》明确提出，培育一批数据商和第三方专业服务机构，通过数据商，为数据交易双方提供数据产品开发、发布、承销和数据资产的合规

[11] 熊丙万：数据产权制度的理论挑战与现代回应，2022年12月

化、标准化、增值化服务。“三权分置”的制度设计为催生出数据流通环节中的专业第三方服务机构创造了良好的环境，包括数据加工服务商、数据技术提供商、数据中介、数据经纪人、数据产品和服务提供商等角色，从而营造更完善的数据交易服务生态。

数据分类分级管理机制及场景化的负面清单是落实“三权分置”产权制度的关键前提。《数据二十条》提出，要加强数据分类分级管理，把该管的管住、该放的放开，推进数据分类分级确权授权使用和市场化流通交易。当前，“一刀切”的数据治理方式已不能满足市场对数据生产要素的需求。无论公共数据、企业数据还是个人数据，推行分类分级管理的机制，形成梯度化的管控力度，才是促进数据高效流通和释放数字生产力的科学路径。当前，我国在国家层面、企业层面，都在加快推进数据分类分级制度，已基本形成一般数据、重要数据、个人信息等分类分级机制。法律法规已对个人信息、重要数据的流通设定了一些基本原则要求，未来，国家应制定数据流通和交易的负面清单，进一步明晰数据流通的监管红线。

第三章 “三权分置”在产业实践中的实施路径

《数据二十条》将数据大致分为公共数据、企业数据、个人数据，不同类型的数据其所承载和涉及的主体权益不尽相同。其中企业数据可能含有个人信息，也可能不含有个人信息。对于不承载个人信息的企业数据的流通，应交由商业决策和市场供需来决定。而对于承载个人信息的企业数据的流通，由于叠加了个人信息权益保护的要求和限制，因此是目前业界比较关注的场景之一。**本报告将主要关注承载个人信息的企业数据的流通问题，并从公共数据流通利用的角度观察其与企业数据流通场景在模式上存在的异同。**此外，由于当前各地数据交易所仍在建设过程中，国家对于数据交易所的管理机制尚不明确，**因此本报告主要聚焦企业数据的场外流通。**

3.1 建立权责利分配机制的必要性

《数据二十条》作为顶层规划创新性地提出数据流通“三权分置”的产权制度设计，具体如何在产业实践中实施和落地尚无法规和政策细则的支撑和规范依据。结合产业实践，我们认为，**科学合理的权责利分配机制是“三权分置”在产业实践中落地和数据高效合规流通的前提。**权利不授权无法实现数据流通链条中的专业化分工，责任不转移无法消除数据资源持有方的安全风险顾虑，收益不分配无法调动数据流通链条中各方的积极性。

首先，权利分配是数据高效流通和价值创造的前提，权利不释放则无法激活整个数

据要素市场的活力。《数据二十条》明确提出，根据数据来源和数据生成特征，分别界定数据生产、流通、使用过程中各参与方享有的合法权利，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制。支持数据处理者依法依规行使数据应用相关权利，促进数据使用价值复用与充分利用，促进数据使用权交换和市场化流通。因此，应尽快明晰各种权利的边界和内涵，使数据产权真正流通和释放。

其次，责任分配应与权利分配紧密偶联，市场主体在享有权利的同时应承担相应的责任，只有合理的责任分担机制建立起来，才能逐渐消除数据安全风险方面的顾虑并建立各方主体之间的信任关系。《数据二十条》明确提出，要强化市场主体数据全流程合规治理，确保流通数据来源合法、隐私保护到位、流通和交易规范。严格落实相关法律规定，在数据采集汇聚、加工处理、流通交易、共享利用等各环节，推动企业依法依规承担相应责任。因此，要在数据流通各方主体之间明晰各方应承担的数据安全和隐私保护责任，按照“谁处理谁负责”的原则，厘清责任边界，强化安全责任落实。

再次，收益的合理分配是除安全合规风险因素以外，数据持有者决策时考虑的另一重要因素。《数据二十条》明确提出，要按照“谁投入、谁贡献、谁受益”原则，着重保护数据要素各参与方的投入产出收益，依法依规维护数据资源资产权益，探索个人、企业、公共数据分享价值收益的方式，推动数据要素收益向数据价值和使用价值的创造者合理倾斜，确保在开发挖掘数据价值各环节的投入有相应回报。通过多种收益共享方式，平衡兼顾数据内容采集、加工、流通、应用等不同环节相关主体之间的利益分配。此外，2023年8月21日，财政部印发的《企业数据资源相关会计处理暂行规定》（简称《暂行规定》）则解决了此前企业数据资产和投入无法计量和核算的问题。通过“数据资源入表”的方式，进一步显化数据资源价值，将企业在日常活动中持有、最终用于出售的数据资源定义为存货，而出售未确认为资产的数据资源则按照收入准则等规定确认相关收入，从而为企业数据资产定价及收益分配奠定基础。

因此，权责利分配机制是目前“三权分置”落地实施的重中之重，对于促进数据流通、保障数据安全都有极其重要的意义。**在本报告中，我们试图结合产业实践剖析数据产权如何合理分配，才能最大程度地激发数据流通的活力，并落实到合同协议层面的具体约束条款，以期为行业各界提供实践思路。**

3.2 数据流通准入安全要求

3.2.1 设置数据流通准入安全要求的必要性

在数据流通利用过程中，考虑到个人信息主体的合法隐私权益，应针对参与数据流通的主体以及进入市场流通的数据，设置数据流通准入安全要求。

一是保障数据主体个人信息权益的必要。《数据十二条》提出，“审慎对待原始数据的流转交易行为”。对于个人数据而言，虽然《数据二十条》赋予了企业一定的数据资源持有权，但由于个人数据涉及个人数据主体的合法权益，因此，数据持有者必须合法合规使用数据，即在用户知情同意的范围内处理和使用个人数据。对于数据流通而言，如果流通的是原始个人数据，除法律法规另有规定，应以个人授权同意为基本前提。但由于数据流通的链条可能很长，数据授权机制将与数据高效流通不匹配，会严重降低数据流通的效率，另外，在数据流通链条中数据处理和加工的方式将不能完全提前预知，数据的前置授权机制存在实施方面的困难。因此，原始数据流通不仅会带来数据安全及隐私保护方面的风险，也会由于合规问题导致数据流通的效率大大降低。

综上，出于对个人信息权益的保护，对流通的数据应当进行去标识或匿名化等脱敏处理，并采取足够稳健的技术和管理措施，实现重标识个人信息主体的风险可控。这就有必要针对流通中的数据形态以及数据流通的全过程，设定安全标准，保障数据的合规高效流通。在此前提下，数据流通利用才能在释放数据价值的同时，不损害个人信息主体的合法权益，做到风险可控。

二是建立市场主体对法律责任判断稳定预期的必要。如前所述，当前数据持有者对共享数据的顾虑较大，对于一些衍生数据的流通所带来的法律责任风险，尚处于法律法规的模糊地带，导致数据持有者对法律责任的判定没有稳定预期[12]。《数据二十条》也明确提出，要结合数据流通范围、影响程度、潜在风险，区分使用场景和用途用量，建立数据分类分级授权使用规范。在法律和标准制定方面，也应当尽快明确数据流通的安全基线要求，稳定数据流通参与主体的法律责任预期。

3.2.2 数据流通形态安全要求

我国《个人信息保护法》规定，“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”，“匿名化是指个人信息经过处理无法识别特定自然人且不能复原的过程”。《数据二十条》在第（六）条中针对个人数据流通利用，提出要“创新技术手段，推动个人信息匿名化处理，保障使用个人信息数据时的信息安全和个人隐私”。虽然目前很多数据要素交易广泛使用数据匿名化技术，但目前实践中缺乏清晰的个人信息匿名化的合规判断标准。目前产业界迫切需要对法律上的“匿名化”给出具体的技术保护和组织管理的标准，指导企业在不侵害自然人个人信息权益的前提下，通过建立和落实合规管理、数据安全技术等手段，

[12] 中国信息通信研究院：数据要素白皮书（2022年），2023年1月

合法地实现数据要素的价值。

有人认为我国法律规定的“匿名化”是指通过使用匿名化技术实现“绝对的匿名化”，**但在一些数据应用场景中，将原始个人数据完全匿名化处理，将可能大大降低数据本身的利用价值，甚至导致数据资源无法使用，这无疑违背了通过匿名化促进数据合规流通利用的目的，难以满足数字经济发展的现实需求。**

本报告认为，绝对的匿名化既不可能也不现实，**法律意义上的匿名化并不等于绝对的匿名化，而是通过风险管理的方式实现“无法识别且不能复原”，并保留数据的使用价值。**因此，结合具体业务对匿名化程度进行分类分级，从而**实现数据利用、业务发展、用户体验和安全保障的平衡，是当下更适合数字经济发展的方案。**

综上所述，本报告认为，**个人数据的高效流通利用应以重标识风险可控为前提，即应结合数据披露程度、预期接收者、拟采取的控制手段等，通过采用技术和管理手段相结合的风险管控方式，将重新识别个人信息主体的可能性降到足够低，实现个人信息的“无法识别特定自然人且不能复原”。**而评估重标识风险的高低以及是否满足隐私保护的要求，需要结合业务目标、安全风险，综合考虑数据类型、使用目的及披露范围、接收者能力与动机等多种因素，在具体场景中开展个人信息保护影响评估，确认相应的技术和管理措施是否达到了“无法识别且不能复原”。

为确保“三权分置”的实际落地，应结合个人信息处理的技术及合规管理措施，赋予其不同的法律效果。针对数据脱敏后重标识风险及对应的合规管理措施满足一定标准的个人信息，应结合符合立法本意的匿名化评价标准，促进符合要求的匿名化个人信息的确权和流通，充分释放高价值个人信息的价值。建立与复杂多元的个人信息处理场景相契合的数据流通安全要求，是保障数据高效合规安全流通的关键，这需要多方主体在不断的实践探索中进行验证。

3.2.3 参与主体准入标准

参与主体应具有业务经营相关的合法资质。首先，数据提供方作为数据处理者，应当具有数据处理的业务资质，如从事增值电信业务需要办理《增值电信业务经营许可证》，从事经营性互联网信息服务，应当办理互联网信息服务增值电信业务经营许可证，此外根据《移动互联网应用程序信息服务管理规定》的规定，通过移动互联网应用程序提供信息服务，应当依法取得法律法规规定的相关资质等。

参与主体应具备一定的数据安全保障能力。由于数据流转的链路涉及的主体众多且可能是动态的，一方的合规风险可能会传导至其他参与方，因此可以通过制定参与方准入能力标准，避免与不适格的主体进行合作，如要求参与方具备一定程度的数据安全保

障能力（例如通过了数据安全管理认证或个人信息保护认证等），具备处理特定类型数据必要的资质等。

3.2.4 数据源合法性要求

数据来源应具有合法性基础。对于数据资源提供方而言，即使流通的是经去标识化或匿名化处理后的数据，数据的来源也必须符合合法性，即原始数据的获取、加工处理以及对外提供的行为，必须通过用户充分授权以取得数据收集和处理的合法性基础。这要求数据提供方明确告知数据主体针对其个人数据开展的数据处理行为，征得个人同意并备案存证，以保障进入数据流通链条中的数据是合规合法的。

具体而言，数据资源提供方的数据来源可以分为直接收集和间接收集两种形式。直接数据来源主要包括各类移动终端、APP和小程序等，这类数据来源的合法性基础是充分自主、清晰明确的数据主体授权同意；间接数据来源包括向提供方采购、经提供方授权获取、与参与方共享的数据等，此时应要求数据提供方说明个人信息的来源以及相关授权的范围，确保需要进行的个人信息处理活动范围不会超过授权同意的范围。

3.3 承载个人信息的企业数据流通

自我国《个人信息保护法》出台以来，市场主体对个人信息的开发利用都持非常谨慎的态度。这类数据由于涉及个人信息主体的权益，因此数据流通的权责利关系更为复杂，隐私保护和安全风险是各方关注的焦点问题。

场外数据流通存在多种路径和模式。数据流通不仅涉及不同的数据流通参与主体，还会在数据流通链条中涉及不同形态的数据类型。对于不同形态的数据流通标的，以及不同的数据流通路径，将会在不同主体间分配不同的权利、责任和收益。

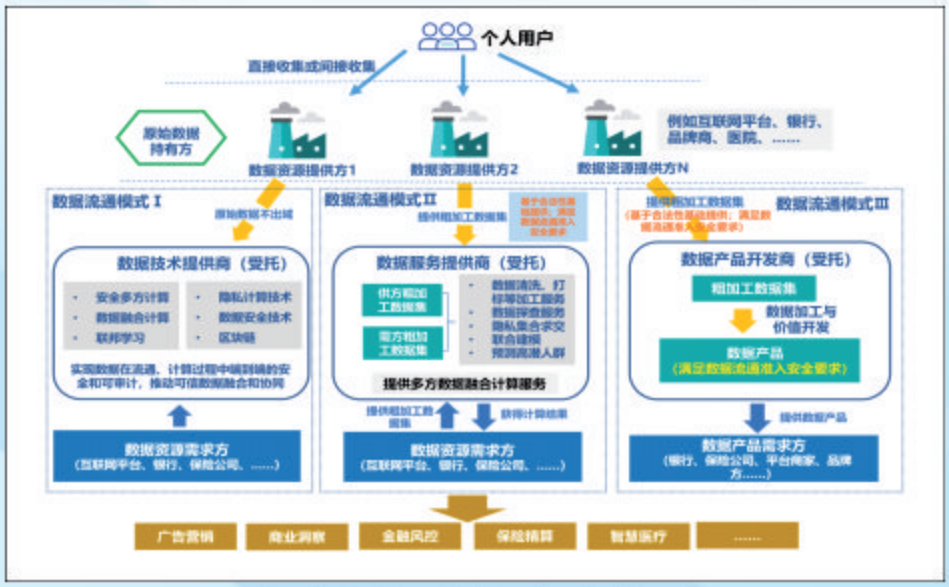


图1 数据流通模式示意图（场外）

如右图所示，我们结合当前的产业实践，将数据流通路径分为三种模式，分别为“数据流通模式Ⅰ”“数据流通模式Ⅱ”和“数据流通模式Ⅲ”，并在以下章节中分别进行具体介绍。

3.3.1 数据流通模式Ⅰ

在数据流通模式Ⅰ中，涉及三方主体，分别为数据资源提供方、数据资源需求方以及数据技术提供商。

其中**数据资源提供方**是持有个人原始数据的一方，数据的来源包括直接向用户收集或从其他主体间接获取得到，在数据流通链条中，数据资源提供方是数据流通的起点。**持有用户个人数据的组织和机构都可以作为数据资源提供方，例如互联网平台、银行、品牌商、医院等。**

数据资源需求方是指对数据资源有需求的一方，是数据流通链条的终点，其将数据资源融合分析得到的结果用于自身业务或其他合法目的。**对他方数据有需求的组织都可以称为数据资源需求方，例如互联网平台、银行、保险公司等。**

数据技术提供商是指为数据资源供需双方的数据融合计算提供技术能力的一方，例如提供数据安全技术、安全多方计算、联邦学习、数据融合计算、区块链等技术。数据技术提供商通过为数据供需双方提供技术能力，实现数据在流通、计算过程中端到端的安全和可审计，推动可信数据融合和协同。例如隐私计算技术公司就属于数据技术提供商。

符合这一数据流通模式的典型案例（案例Ⅰ）：

在银行反欺诈业务中，银行A为完善自身的反欺诈模型系统，希望获得银行B的用户信用数据，以扩充自身的模型训练样本数据。双方基于隐私计算公司C提供的隐私计算能力，在各方的数据服务器部署安全计算中心并进行相关配置，来完成双方数据之间的横向联邦学习和建模。在此案例中，银行A是数据资源需求方，银行B是数据资源提供方，隐私计算公司C是数据技术提供商。

以下章节将针对这种数据流通模式，分别对各方主体之间的权、责、利如何合理分配进行分析。

3.3.1.1 权利分配

对数据权利进行配置，首先需要对数据资源持有权、数据加工使用权以及数据产品经营权等权利的具体权能进行界定。

数据资源持有权是指数据持有者对于通过合法途径获取的数据，无论是基于业务运营的需要采集以及产生的数据，还是通过采购、共享等方式获取的数据，有权依照法律规定或合同约定自主管控所取得的数据资源，并拥有排除他人对控制状态侵害的权利。如不存在法定正当事由，且未经持有者同意，他人不得侵扰权利人对数据的稳定持有状态[13]。数据资源持有权是其他数据权利的基础。

[13] 熊丙万：数据产权制度的理论挑战与现代回应，2022年12月

数据加工使用权可以再细分为数据加工权和数据使用权，其中数据加工权是指对具有合法来源的数据，权利人在法律规定或合同约定的限制条件内，对数据开展加工、分析、计算等处理活动的权利；数据使用权是指基于数据共享、数据交易等方式，数据需求方（权利人）对合法获取的数据资源或数据产品在法定或合同约定范围内进行使用的权利。

数据产品经营权是指权利人对通过合法途径获取的数据资源，在法律规定或合同约定的范围内，对经过加工处理而形成的数据产品或服务，享有在合法范围内进行营销、销售和获取收益的权利。

《数据二十条》对数据产权的种类采取了开放式的描述，即“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”，这意味着在数据实际流通过程中可以通过实践进一步确认其他合理的数据产权种类。

数据流通模式Ⅰ中各方参与主体的数据权利分配如下图所示。

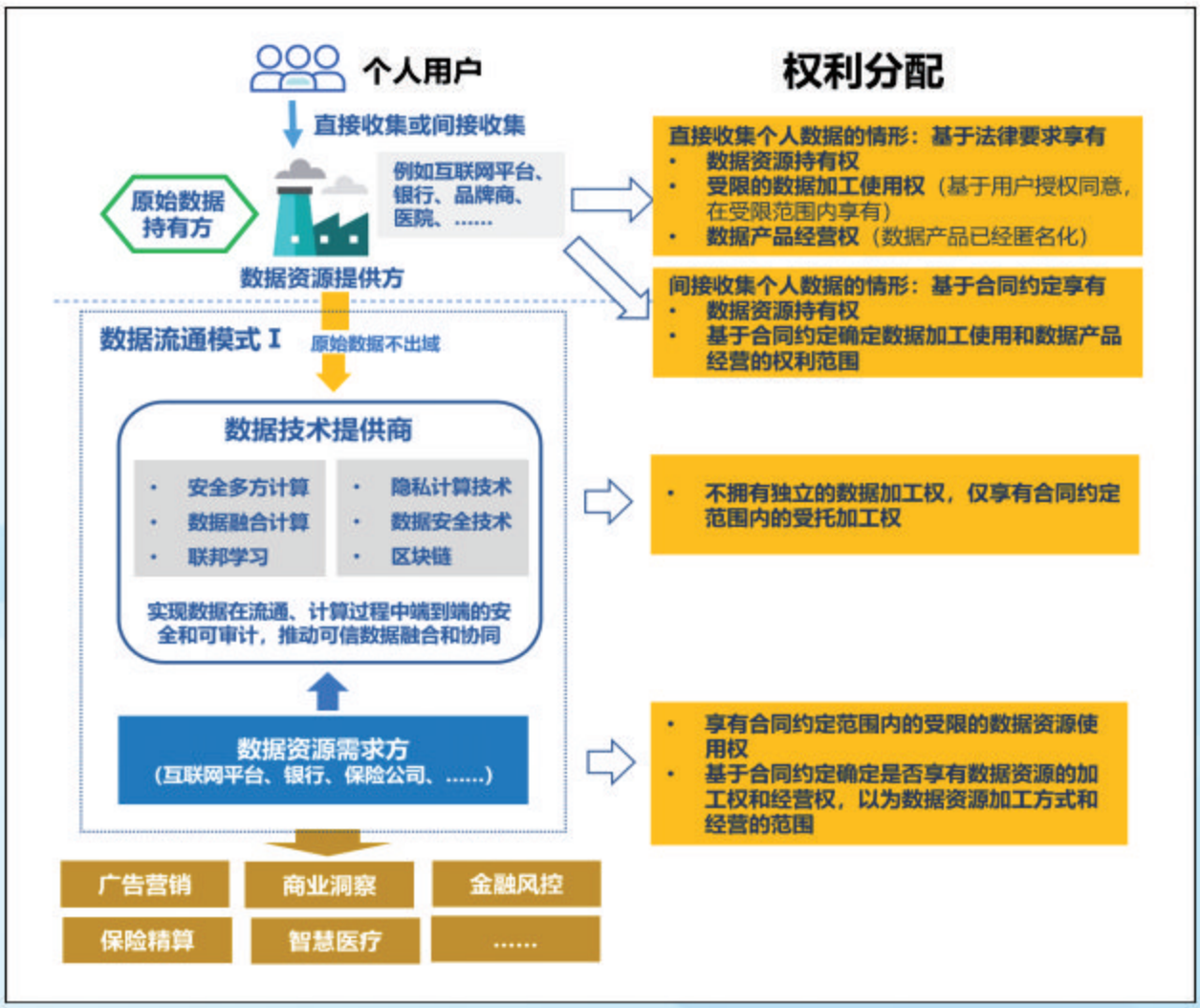


图2 数据流通模式Ⅰ权利分配机制

（1）数据资源提供方的权利

由于数据提供方的数据存在直接收集及间接收集（指向个人用户收集）两种情况，不同的收集方式导致其所拥有的权利也不尽相同，因此以下首先分析直接收集个人数据的情形。

数据资源提供方具有数据资源持有权。近几年，社会各界对数据权属问题一直争论不休，欧盟委员会于2017年提出设立数据生产者权的建议，引发广泛关注。数据生产者权的设立主要是为了促进和鼓励机器生成数据的访问与共享，但由于涉及到客户的相关权益，在2022年2月欧盟发布的《数据法案》草案中，对数据持有者使用由产品或相关产品产生的非个人数据提出了限制，即只有在与客户签订合同的基础上才能提供服务并使用上述非个人数据。我国在《数据二十条》中提出了“数据持有权”的概念，这个权利针对的主体类似于欧盟的数据生产者，即在业务活动开展过程中由于业务需要而收集了用户数据的市场主体，例如在互联网领域的一些生活服务平台，以及在工业领域的工作设备制造商等。这类市场主体在自身业务开展过程中产生了大量数据，这些数据不仅包含了原始数据主体的信息内容，更是融合了平台企业主体在其中所投入的资本和技术等因素，**因此平台企业主体应具有这些数据的持有权，但数据持有权的权能边界应不同于欧盟于2017年提出的数据生产者权，其不应具有对数据开展自主处理的权利。**

数据资源持有权的权能：如上所述，针对数据资源提供方因自身业务开展而产生的大量数据，数据持有权应包括一系列除合同关系以外对抗任何第三方侵害其稳定持有状态的权利，从而避免无权使用数据的第三方对数据进行持有和利用，还包括对未经授权获取和使用数据的行为请求损害赔偿的权利。**但数据持有权并不代表可以采用任意方式对数据进行加工、处置等处理活动，而是需在法律规定或合同约定的范围内进行处置。**例如在案例Ⅰ中，银行A和银行B是直接收集用户个人信息的主体，其可在法律规定范围内对收集的数据享有保存、使用、处置的权利，但不可未经用户授权同意而对收集的数据随意出售、公开等。

数据资源提供方享有以合法授权同意为基础的受限的数据加工使用权。数据资源提供方在持有用户数据的基础上，根据《个人信息保护法》的要求，需公开告知数据的处理目的、处理方式和处理的个人信息种类，并需在用户授权同意的前提下，才能对个人数据进行处理，其加工使用数据的范围必须保证不超出用户授权同意的范围。因此，数据资源提供方享有个人信息主体授权范围内的受限的数据加工使用权，而不具有完全自主的数据加工和使用权。

数据资源提供方对满足安全流通要求的数据产品享有自主经营权。在3.2.2章节中，

我们论述了针对数据流通形态的安全要求，即需以重标识风险可控为前提。因此，如果按照要求，数据资源提供方经过加工处理形成的数据产品已经满足了数据流通的安全要求，并且已经通过合同协议等方式设置了风险管控的管理机制，那么数据资源提供方就可以拥有独立自主的数据产品经营权，即对数据产品享有在合法范围内进行营销、销售和获取收益的权利。例如在案例Ⅰ中，银行B作为数据资源提供方，在采用联邦学习、安全多方计算等隐私计算技术对数据在流通利用过程中进行匿名化管控的前提下，可以享有数据资源的自主经营权，并可以因此获得收益。

间接收集个人数据的情形：除了直接收集用户数据以外，数据资源提供方可能基于合同授权从其他市场主体处间接收集个人数据。这种情形下，数据资源提供方享有数据资源持有权、数据加工使用权和数据产品经营权的前提是合同授权，合同约定决定数据资源提供方所享有的权利范围。

（2）数据技术提供商的权利

数据技术提供商仅享有合同约定范围内的受托加工权。数据技术提供商仅为数据资源供需双方之间的数据融合分析提供相应的技术服务，例如数据安全技术、安全多方计算、联邦学习、数据融合计算、区块链等技术，其并不能够自主地决定如何加工使用供需双方的数据资源，也不能自主地对数据提供方的数据资源或数据产品进行经营。据此，数据技术提供商作为第三方服务商，基于数据资源供需双方的委托，提供数据处理的安全计算环境，基于三方之间的合同约定，仅享有合同约定范围内的受托加工权。例如在案例Ⅰ中，隐私计算公司C作为银行A和银行B的受托方，仅可在合同约定范围内对银行A和银行B的数据资源进行加工计算，其不享有自主的数据加工使用权。

合同示范条款：“受托加工权”条款（三方协议）

丙方（数据技术提供商）仅能在甲乙双方的委托范围内对双方的数据资源进行处理，不得超出委托范围对双方数据开展任何处理活动。数据计算结果归乙方（数据需求方）所有，除另有约定外，丙方对计算结果不享有任何的加工使用权和经营权。

（3）数据资源需求方的权利

数据资源需求方仅享有合同约定范围内的数据使用权。数据资源需求方作为数据流通的终点，基于自身需求通过数据技术提供商提供的技术能力与数据提供方进行数据融合计算，获取所需的数据计算结果，其可在合同约定的范围内使用获得的计算结果类数据。至于数据资源需求方对所获得的计算结果享有的加工处理、分析使用等权利的范围，要依据与数据资源提供方签订的合同来确定。

合同示范条款：数据资源需求方权利约束条款（三方协议）

乙方（数据资源需求方）仅能在甲乙双方约定的范围内对从甲方（数据资源提供方）获得的基于双方数据融合计算得到的结果进行使用，不得超出约定范围使用、共享或公开。

3.3.1.2 责任分配

本报告所关注的责任分配机制主要是指在《个人信息保护法》项下数据处理者相关的个人信息保护法律义务在不同数据流通参与主体之间的分配问题，这是当前数据要素流通市场发展面临的关键问题之一。其他市场主体之间的商事责任不在本节进行讨论。

数据流通参与主体都应基于持有的数据和获取的授权承担法定责任。当前数据流通的主要阻碍之一是数据持有者出于合规风险的担忧，不愿将数据共享出来，因此在三权分置框架下，需要匹配合理的数据安全责任分担机制，通过合同协议的方式明确数据链路中其他参与主体的数据安全保护责任。

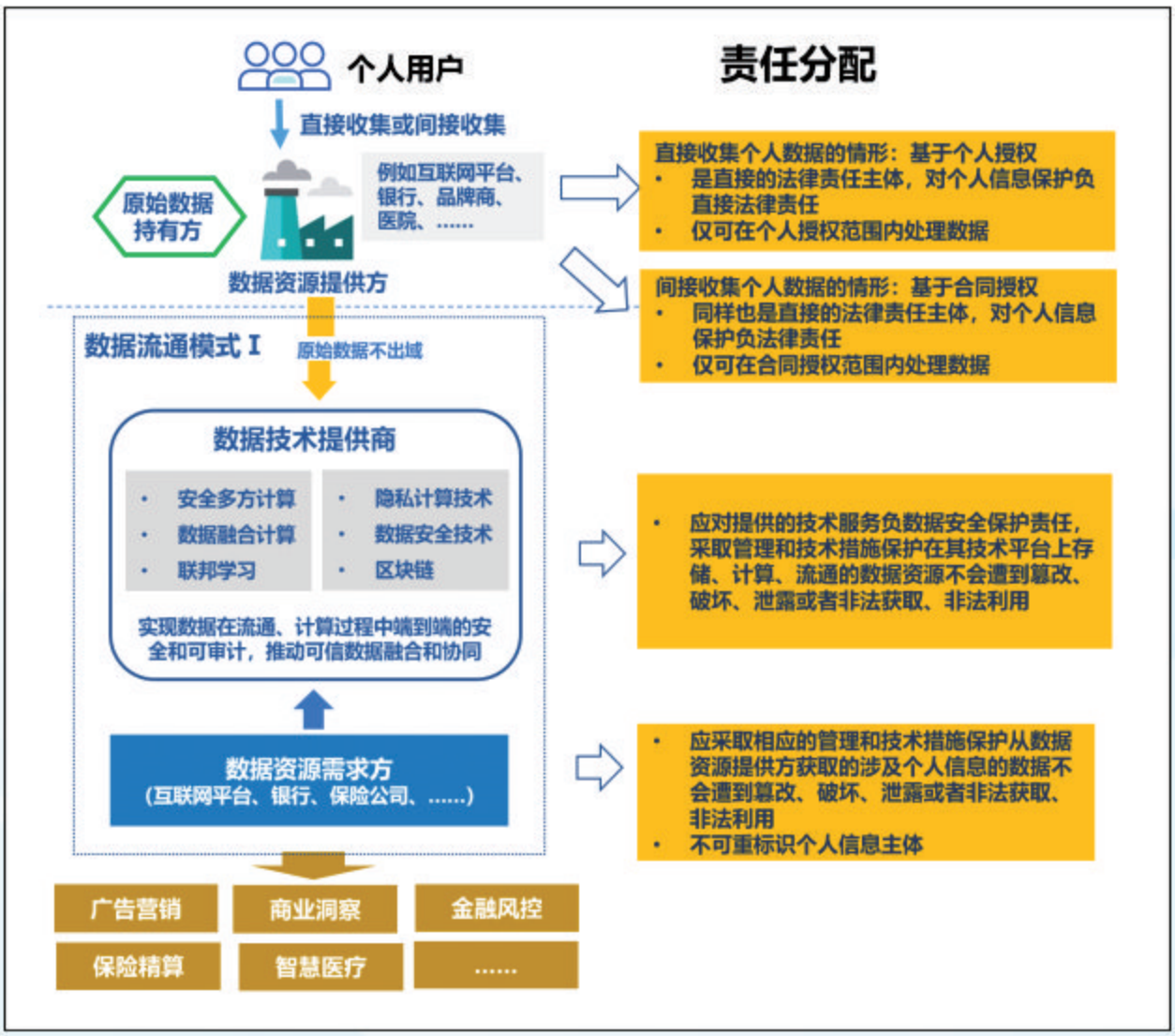


图3 数据流通模式 I 责任分担机制

（1）数据资源提供方的责任

数据资源提供方负有个人信息保护的法律义务。无论是直接收集还是间接收集个人数据，数据资源提供方作为个人信息处理者，即法律意义上的直接法律责任主体，在《个人信息保护法》法律体系下，应对个人信息保护负直接法律责任。例如针对直接收集个人数据的情形，数据资源提供方收集和处理用户数据需获得用户授权、需采取措施保护个人信息不被泄露或非法使用、需响应个人信息主体的合法权利等。针对间接收集个人数据的情形，数据资源提供方仅可在合同授权范围内处理数据，并应采取措施保护个人信息不被泄露或非法使用。例如在案例Ⅰ中，银行A和银行B都持有用户的个人数据，双方都受个人信息保护法律法规的约束，必须按照法律要求保护好用户的个人数据。

（2）数据技术提供商的责任

数据技术提供商应对提供的技术服务负数据安全保护责任。对于数据技术提供商提供的安全多方计算、数据融合计算、联邦学习等技术，数据技术提供商作为第三方提供商，应基于合同承担数据安全保护义务，采取管理和技术措施保护在其技术平台上存储、计算、流通的数据资源不会遭到篡改、破坏、泄露或者非法获取、非法利用。对于数据技术提供商因管理不善或未采取相应的技术和其他必要措施，导致数据资源供需双方的数据遭到篡改、破坏、泄露或者非法获取、非法利用的情况，数据技术提供商应当对给数据资源供需双方造成的损失承担法律责任。例如在案例Ⅰ中，隐私计算公司C应在提供隐私计算技术服务过程中，采取数据加密、权限管理等技术和管理措施保护银行A和银行B的数据资源不被泄露和非法访问。

合同示范条款：数据技术提供商责任条款（三方协议）

丙方（数据技术提供商）应采取相应的管理和技术措施保护在其技术平台上存储、计算、流通的甲方（数据资源提供方）和乙方（数据资源需求方）的数据资源不会遭到篡改、破坏、泄露或者非法获取、非法利用。如果由于丙方过错导致发生数据泄露事件或甲、乙方的数据资源被非法获取、非法利用，丙方应立即采取适当的补救措施，以减轻对个人信息主体和甲、乙方造成的不利影响。丙方应当赔偿由此给甲、乙方造成的全部损失。

（3）数据资源需求方的责任

为保障数据流通安全，数据资源需求方也应对获得的计算结果类数据承担相应的安全保护义务，即采取管理和技术措施保护从数据资源提供方获取的涉及个人信息的计算结果不会遭到篡改、破坏、泄露或者非法获取、非法利用。此外，数据资源需求方也应被约束通过获取的数据资源重标识个人信息主体的行为，因违反法律规定及合同约定而

侵害个人信息主体权益的，应当对个人信息主体承担法律责任，并承担对数据资源提供方造成的损失。

合同示范条款：数据资源需求方责任条款（三方协议）

乙方（数据资源需求方）应采取相应的管理和技术措施保护从甲方（数据资源提供方）获取的涉及个人信息的数据不会遭到篡改、破坏、泄露或者非法获取、非法利用。乙方不得基于获得的甲方数据采取任何手段重标识个人信息主体。如果由于乙方过错导致发生数据泄露事件或数据被非法获取、非法利用，乙方应立即采取适当的补救措施，以减轻对个人信息主体和甲方造成的不利影响。乙方应当赔偿由此给甲方造成的全部损失。乙方因违反合同而侵害个人信息主体权益时，应当对个人信息主体承担法律责任。

3.3.1.3 收益分配

数据资源提供方和数据技术提供商都应基于提供的相应服务获得收益。如下图所示，收益产生于需求方对数据资源的需求，收益从需求方流向数据资源提供方。数据资

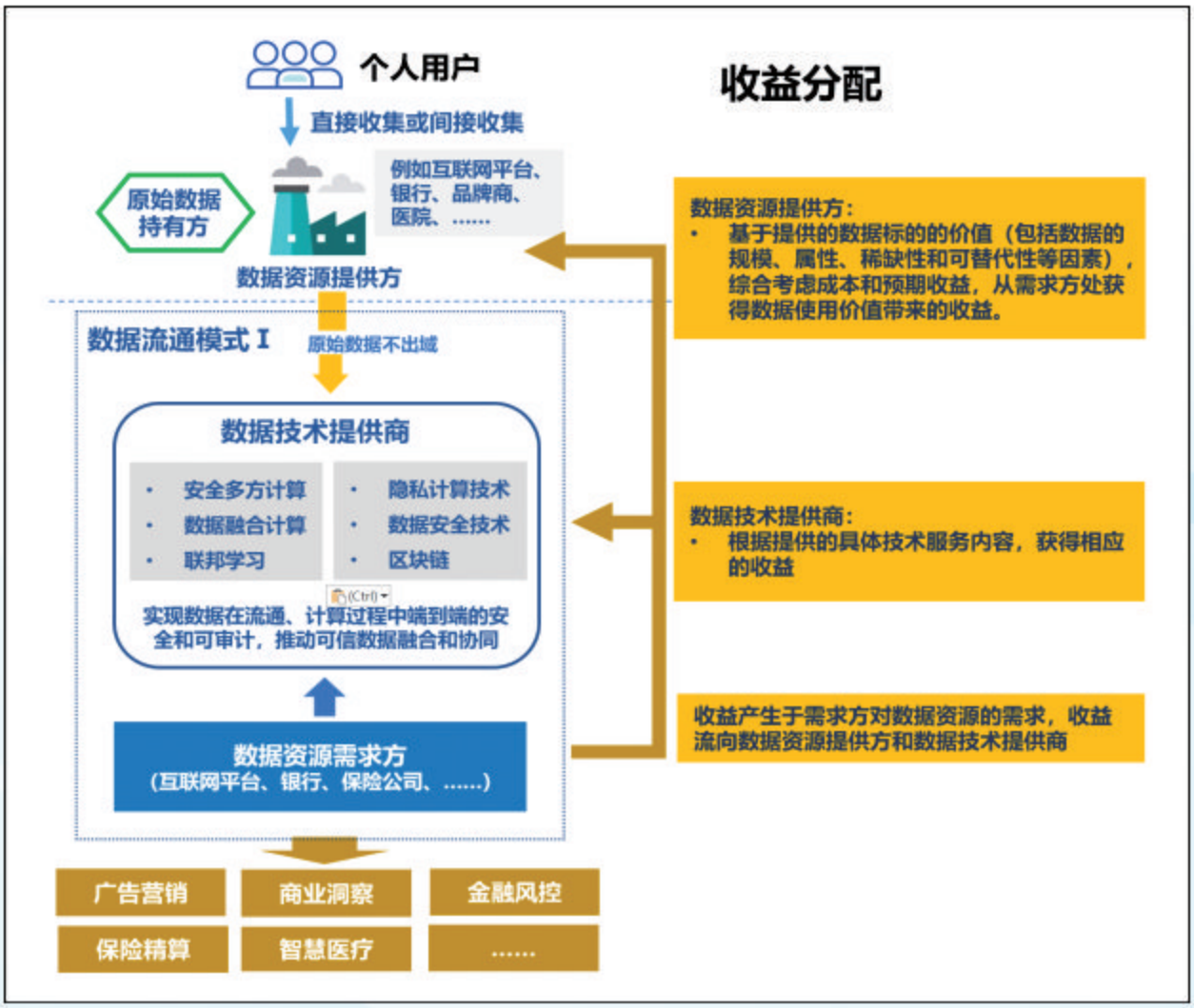


图4 数据流通模式 I 收益分配机制

源提供方基于提供的数据标的的价值（包括数据的规模、属性、稀缺性和可替代性等数据质量、应用和成本因素），综合考虑成本和预期收益，从需求方处获得数据使用价值带来的收益。数据技术提供商由于提供算法、算力等技术服务，形成了有价值的结果数据，因此应按提供的具体技术服务内容，获得相应的收益。例如在案例Ⅰ中，银行A是发起数据需求的一方，基于自身和银行B的用户数据，通过采购隐私计算公司C的技术服务，获得了预期的所欺诈模型，因此银行A应支付隐私计算公司C相应的技术服务费，同时，应就银行B提供数据价值支付其相应的费用，银行B的数据价值定价可综合考虑数据资源的获取和运营成本以及银行A的预期收益来确定。

3.3.2 数据流通模式Ⅱ

在数据流通模式Ⅱ中，也涉及三方主体，分别为数据资源提供方、数据资源需求方和数据服务提供商。在这种模式中，数据资源提供方将自身持有的数据经粗加工并满足数据流通安全要求后，形成衍生数据集，然后委托数据服务提供商进行衍生数据集的清洗、打标等数据加工处理，并授权数据服务提供商利用其数据资源向需求方提供数据服务（多方数据融合计算服务），包括数据探查、隐私集合求交、联合建模、高潜人群预测等。数据资源需求方根据自身需求在数据服务提供商处获取数据服务，并获得数据融合计算结果，用于广告营销、商业洞察等需求。

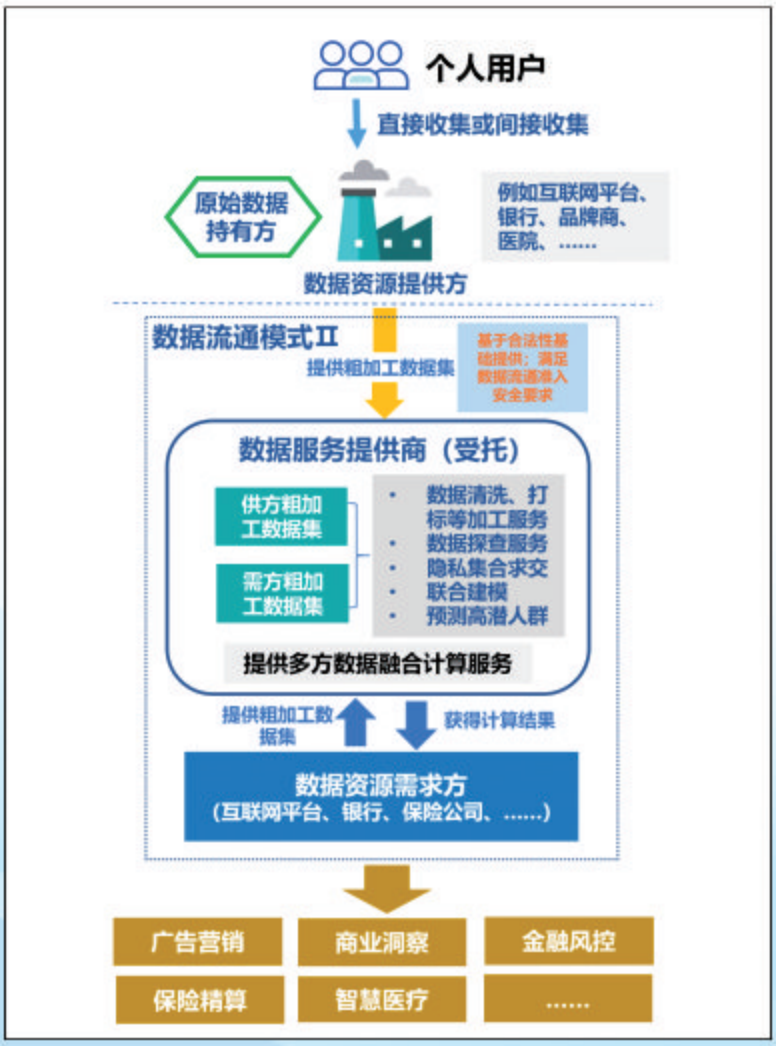


图5 数据流通模式Ⅱ示意图

数据服务提供商在数据流通利用中起着关键作用，它能提供数据资源供需对接的功能。数据服务提供商基于数据资源提供方的委托和数据资源提供方的数据资源，通过建立底层技术能力和统一的合规机制，向需求方提供数据服务，在供需双方间建立了数据高效流通的桥梁，使供需双方相互被看见，从而实现数据流通效率的整体提升。

符合这一数据流通模式的典型案例（案例Ⅱ）：

数据资源提供方A和数据资源提供方B，分别委托技术公司Z进行数据清洗、打标、命名等数据技术服务。在此基础上，根据合同约定，公司Z基于受托加工后的数据集拓展数据技术研发，建立数据流通所需安全风控及技术管理体系，在A、B公司委托合同约定范围内，向符合条件的其他方D、E提供数据产品或服务，包括数据探查、隐私集合求交、联合建模、高潜人群预测等。在此案例中， A、B公司是数据资源提供方，D、E公司是数据资源需求方，技术公司Z是数据技术服务提供商。

3.3.2.1 权利分配

数据资源提供方与数据资源需求方所享有的权利与3.3.1.1中数据流通模式Ⅰ是一样的，此处不再赘述。本节仅分析数据服务提供商所享有的权利。

数据服务提供商仅享有合同约定范围内的受托加工权和经营权。数据服务提供商基于数据资源提供方的委托开展相应的数据加工处理、数据融合计算并对外提供数据服

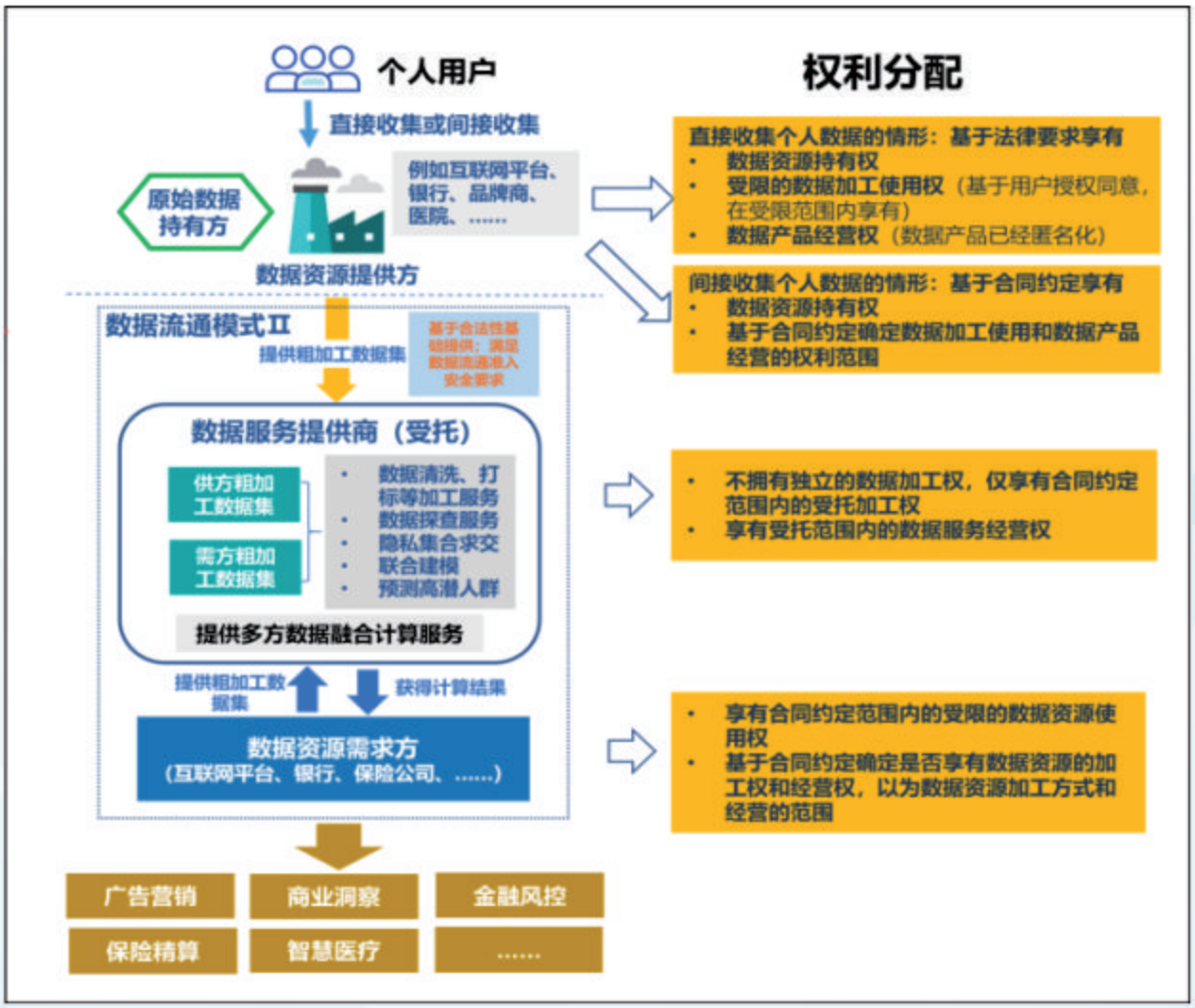


图6 数据流通模式Ⅱ权利分配机制

务，因此其对数据资源提供方的数据资源仅能在合同约定范围内进行加工处理，仅享有受限的受托加工权；其仅能对外提供委托范围内的数据服务种类，不得未经数据资源提供方同意擅自增加额外的数据服务类型，且其对数据服务仅享有委托经营权，不享有独立自主的经营权。例如在案例Ⅱ中，技术公司Z对于A、B公司委托其加工处理的数据资源，以及可对外提供的数据服务类型，仅享有合同范围内受限的加工权和经营权。

合同示范条款：“受托加工权和经营权”条款（双方协议）

乙方（数据服务提供商）仅能在甲方（数据资源提供方）的委托范围内对甲方的数据资源进行加工和处理，不得超出委托范围对甲方数据开展任何加工处理活动。乙方仅能在经甲方授权的范围内对外提供基于甲方数据资源的数据服务，不得对外提供未经甲方同意的数据服务类型。数据计算结果归甲方及需求方所有，乙方对计算结果不享有任何的加工使用权和经营权。

3.3.2.2 责任分配

数据资源提供方与数据资源需求方应承担的责任与3.3.1.2中数据流通模式Ⅰ是一样的，此处不再赘述。

数据服务提供商应对持有的供需双方数据负安全保护责任。数据服务提供商基于数据资源提供方的委托开展相应的数据加工处理、数据融合计算并对外提供数据服务，会存储数据供需双方的数据，作为受托方，应基于合同承担数据安全保护义务，采取管理和技术措施保护在其技术平台上存储、计算、流通的数据资源不会遭到篡改、破坏、泄露或者非法获取、非法利用。对于数据服务提供商因管理不善或未采取相应的技术和其他必要措施，导致数据资源供需双方的数据遭到篡改、破坏、泄露或者非法获取、非法利用的情况，数据服务提供商应当对给数据资源供需双方造成的损失承担法律责任。例如在案例Ⅱ中，技术公司Z应采取数据加密、权限管理等技术和管理措施保护供需双方的数据资源不被泄露和非法访问。

合同示范条款：数据服务提供商责任条款（双方协议）

乙方（数据服务提供商）应采取相应的管理和技术措施保护在其技术平台上存储、计算、流通的甲方（数据资源提供方）的数据资源不会遭到篡改、破坏、泄露或者非法获取、非法利用。如果由于乙方过错导致发生数据泄露事件或甲方的数据资源被非法获取、非法利用，乙方应立即采取适当的补救措施，以减轻对个人信息主体和甲方造成的不利影响。乙方应当赔偿由此给甲方造成的全部损失。

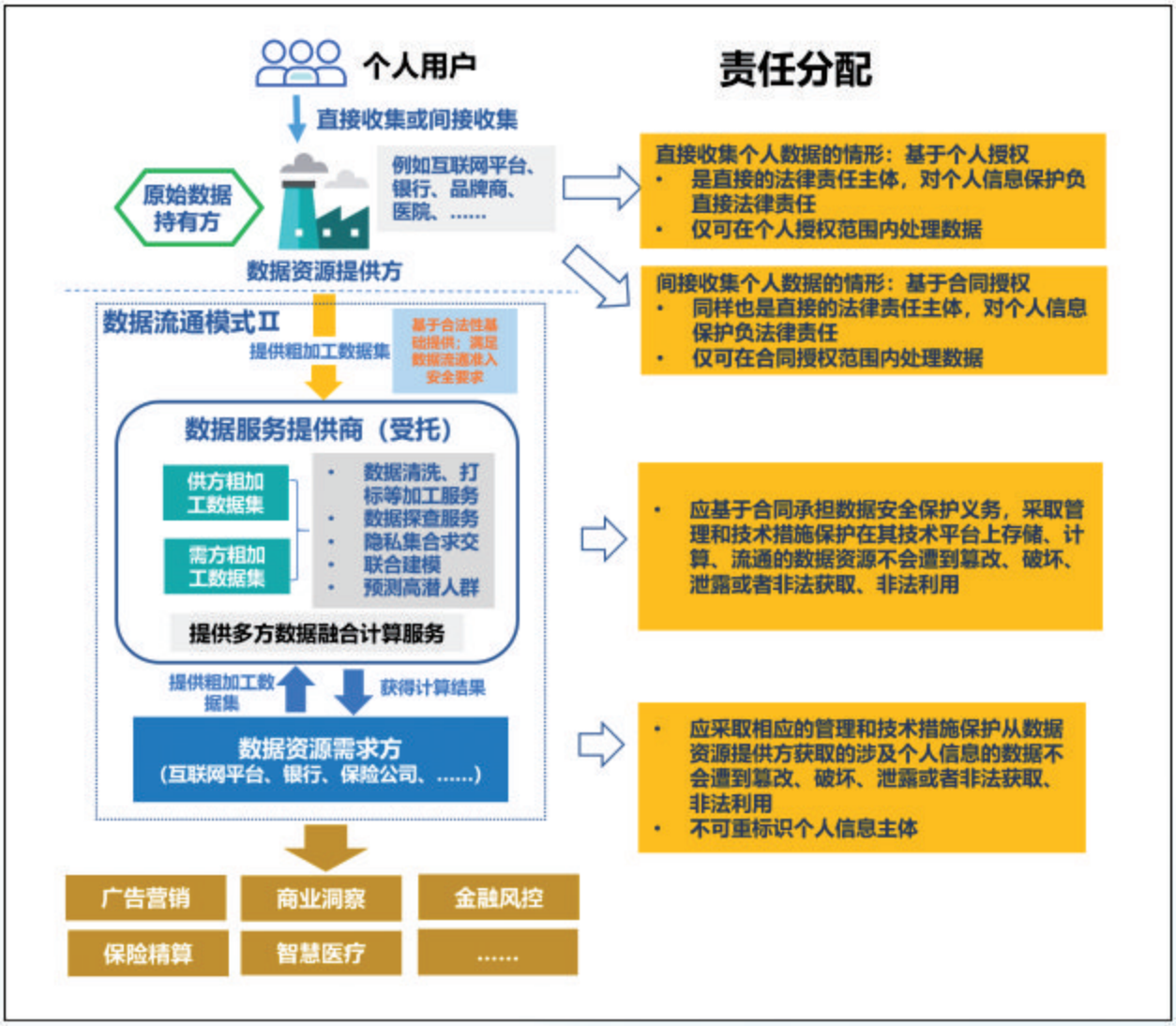


图7 数据流通模式Ⅱ责任分配机制

3.3.2.3 收益分配

数据服务提供商基于提供的数据服务从数据资源需求方处获得收益。如下图所示，数据服务提供商基于数据资源提供方的委托，对数据进行加工处理、数据融合计算并代其对外提供数据服务，收费模式由数据服务提供商基于服务类型进行确定。收益产生于需求方对数据服务的需求，由于数据服务提供商是直接提供数据服务的一方，因此收益从需求方首先流向数据服务提供商。**数据服务提供商将服务收益按约定的模式分配给数据资源提供方。**在具体的数据服务中，可能涉及一方或多方数据资源提供方的数据，数据服务提供商应基于数据的具体使用情况，以及具体数据资源的价值（包括数据的规模、属性、稀缺性和可替代性等因素），向涉及的数据资源提供方按双方约定的模式，进行服务收益分配。

例如在案例Ⅱ中，D公司在技术公司Z处获得了来源于A、B公司的数据服务，D公司

应按照Z公司制定的收费方式向Z公司支付服务费。此外，Z公司应按照与A、B公司约定的收益分配模式，基于数据实际使用情况，向A、B公司分别支付相应的数据使用费用。

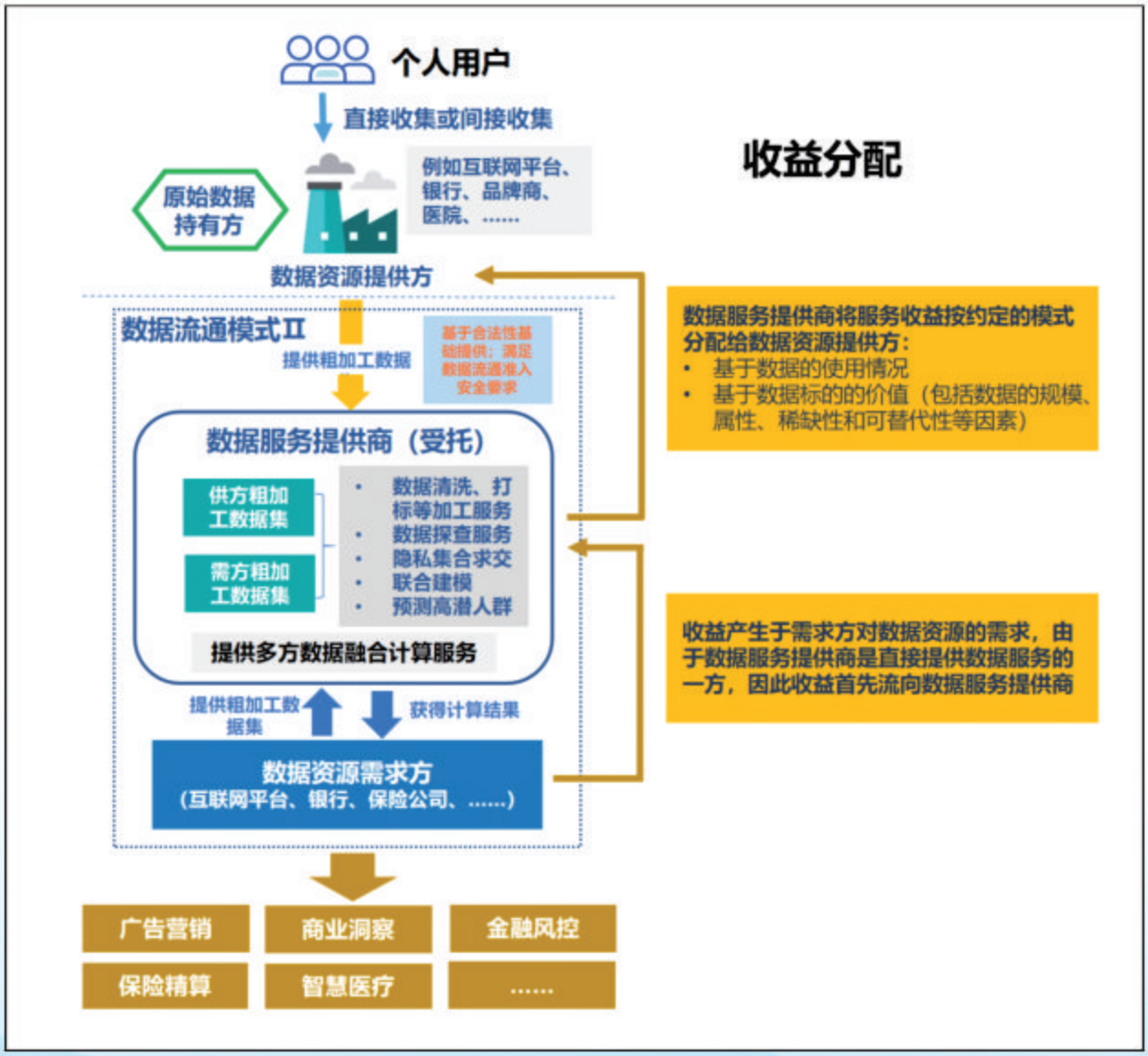


图8 数据流通模式Ⅱ收益分配机制

3.3.3 数据流通模式Ⅲ

数据流通模式Ⅲ可称为数据产品模式，其与前两种模式的主要区别在于在这种模式下数据**以数据产品的形式**进行流通。这种数据流通模式也涉及三方主体，分别为数据资源提供方、数据资源需求方和数据产品开发商。在这种模式中，数据资源提供方将自身持有的数据经粗加工并满足数据流通安全要求后，形成衍生数据集，然后委托数据产品开发商将其开发成商业化的数据产品，并对外提供。数据产品开发商基于自身的技术能力，在粗加工数据集的基础上，对数据价值进行开发，并对数据形态进行加工，形成可向市场需求方提供的数据产品。数据资源提供方对数据产品开发商的数据价值开发活动

进行监督管理，并对数据开发和数据产品进行合规和安全风险评估。

符合这一数据流通模式的典型案例（案例Ⅲ）：

互联网企业A基于自身业务产生用户和商家经营数据，为了更好地服务商家，A公司委托技术公司B基于其数据资源，以商家为主要客户群体进行商业洞察类数据产品开发，致力于帮助商家基于该数据产品进行更好的商业运营。在此案例中，互联网企业A是数据资源提供方，商家是数据资源需求方，技术公司B是数据产品开发商。

数据提供方利用自身的数据加工技术能力直接对数据价值进行开发，形成并面向市场提供数据产品和服务的模式也是较为普遍的，在这种模式下，数据提供方将数据的“三权”全面控制在企业内部，不对外授权数据加工权和数据产品经营权。这种模式由于不涉及权责利在多主体间的分配，因此本报告不做过多讨论。

图9 数据流通模式Ⅲ示意图

数据产品模式一般适用于通用和标准化的数据产品，其面向的市场需求对象具有确定性的特征，即面向某一类特定的需求群体进行数据价值开发，例如上述案例Ⅲ中互联网平台开发的面向平台商家的数据智能服务，其属于“一对多”数据流通模式。

3.3.3.1 权利和责任分配

数据资源提供方与数据资源需求方所享有的权利和责任边界与3.3.1中数据流通模式Ⅰ是一样的，此处不再赘述。本节仅分析数据产品开发商所享有的权利和应承担的责任。

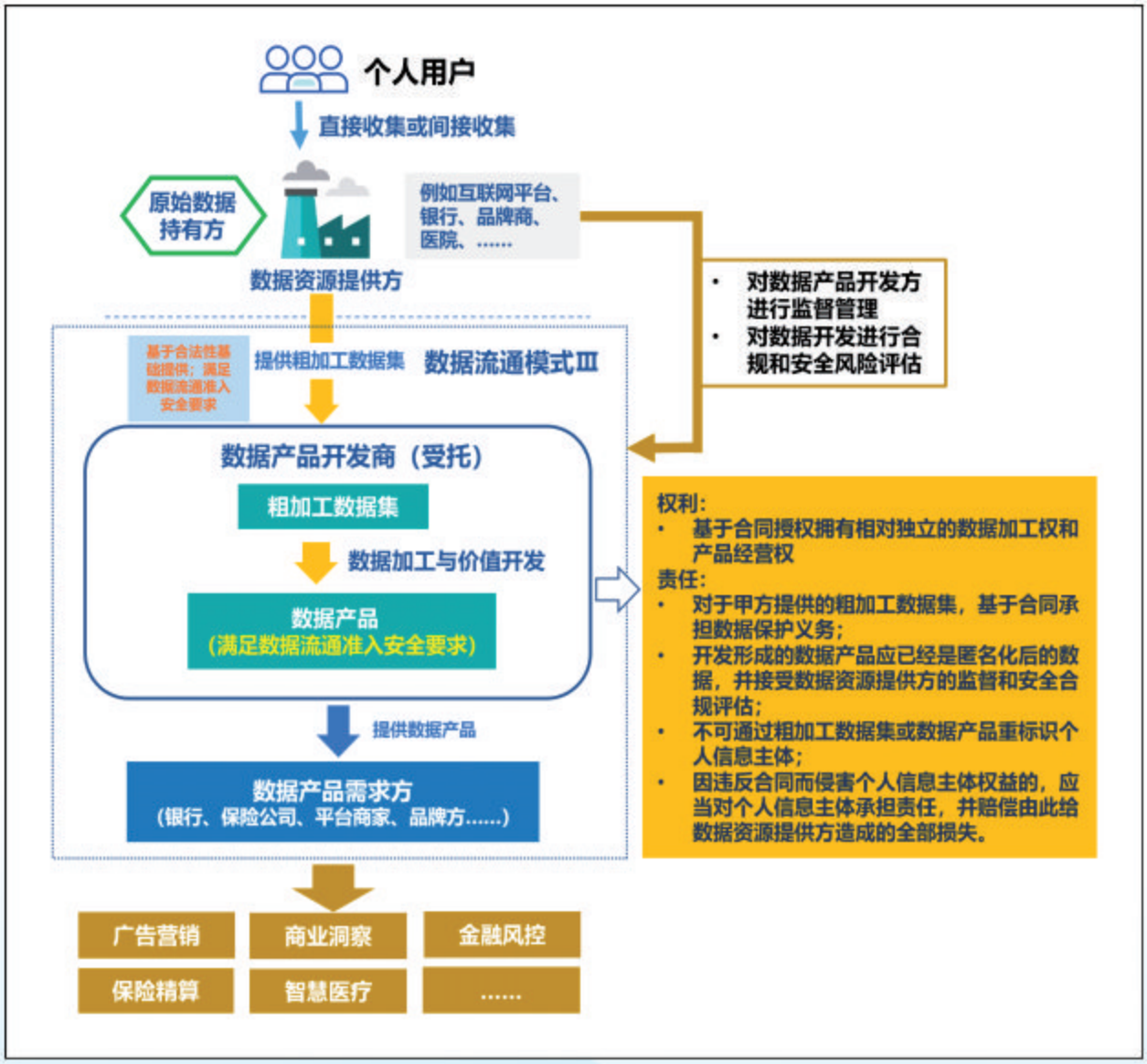


图10 数据流通模式Ⅲ权利责任分配机制

数据产品开发商基于合同授权拥有相对独立的数据加工权和产品经营权。为让数据产品开发商充分开发挖掘数据资源的价值，发挥数据产品开发商在数据加工和分析技术方面的专业性，数据资源提供方可基于合同授权数据产品开发商享有独立的数据加工权和数据产品经营权，但约定数据资源提供方对数据产品开发商的数据价值开发活动进行监督管理，并对数据开发和数据产品进行合规和安全风险评估。同时，基于隐私安全的考虑也应通过合同让其承担一定的数据隐私保护责任，包括：对于数据资源提供方提供的粗加工数据集，基于合同承担数据保护义务；开发形成的数据产品应满足数据流通安全要求；不可通过粗加工数据集或数据产品重标识个人信息主体；因违反合同而侵害个人信息主体权益的，应当对个人信息主体承担责任，并赔偿由此给数据资源提供方造成的全部损失。

合同示范文本：“数据加工权和数据产品经营权”条款（双方协议）

乙方（数据产品开发商）可针对甲方（数据资源提供方）的数据资源（在本合同约定范围内的数据资源），进行加工处理、开发挖掘等数据价值和数据产品开发和经营活动。甲方对乙方的数据价值开发活动进行监督管理，并对数据产品和服务进行事前合规和安全风险评估。以上所指的甲方数据资源的所有权归甲方所有，乙方不得提供给任何第三方并因此获得任何收益。经乙方开发形成的数据产品的所有权归甲乙双方共同所有。

乙方应采取有效的管理和技术方面的保护措施，防止甲方数据资源遭受任何未经授权的访问、泄露、篡改或丢失。如果由于乙方过错导致发生数据泄露事件，应及时采取适当的补救措施，以减轻对个人信息主体和甲方造成的不利影响。

乙方不得基于持有的甲方数据采取任何手段重标识个人信息主体。乙方因违反合同而侵害个人信息主体权益时，应当对个人信息主体承担法律责任。甲方因乙方造成的损害承担法律责任的，有权向乙方追偿。

3.3.3.2 收益分配

数据资源提供方和数据产品开发商基于协商确定收益如何分配。在这种数据流通模式下，数据的收益分配机制应该主要基于各方主体对于最终的数据产品与服务所投入的要素的价值，推动数据要素收益向数据价值和使用价值的创造者合理倾斜，确保在开发挖掘数据价值各环节的投入有相应回报。如下图所示，数据资源提供方贡献了数据资源投入，数据产品开发商贡献了技术、人力和经营等方面的成本，并承担了一定的市场风险，因此，双方应基于流通的数

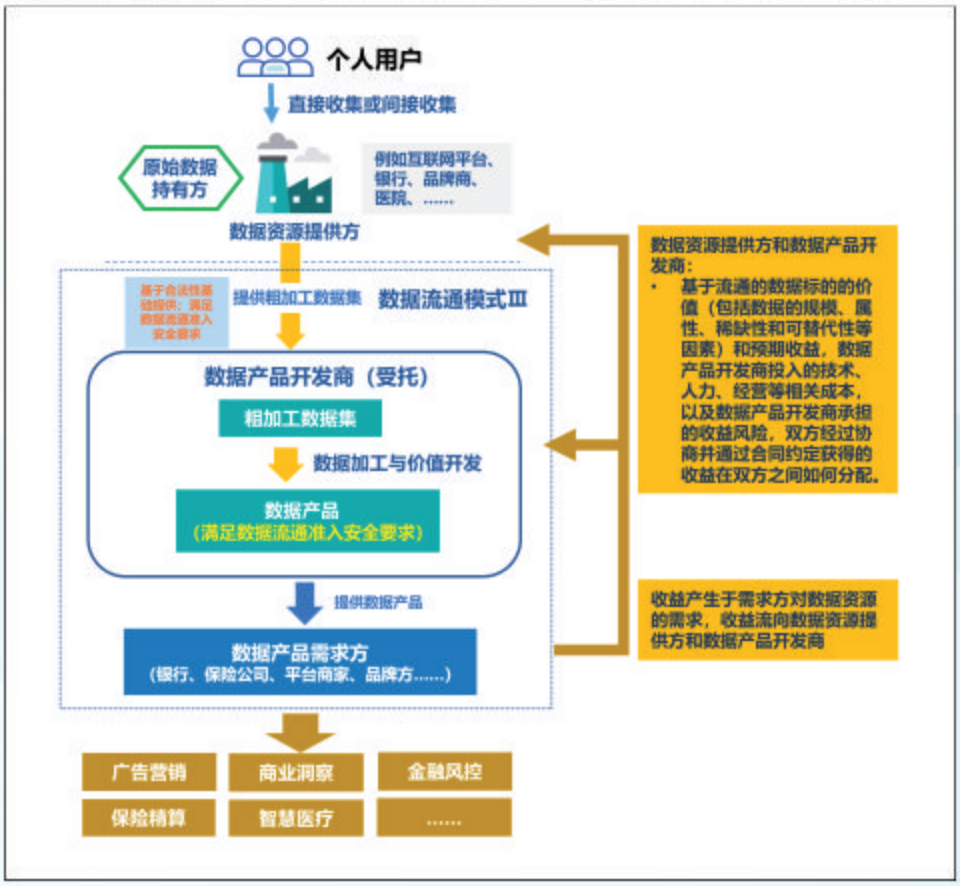


图11 数据流通模式Ⅲ收益分配机制

据标的的价值（包括数据的规模、属性、稀缺性和可替代性等因素）和预期收益，数据产品开发商投入的技术、人力、经营等相关成本，以及数据产品开发商承担的收益风险，经过协商并通过合同约定数据产品经营获得的收益在双方之间如何分配。

3.3 公共数据流通“三权分置”实施路径

3.3.1 公共数据流通框架

公共数据授权运营是我国公共数据要素流通的重要探索方向。公共数据，是指国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织，在履行公共管理和服务职责过程中收集和产生的数据[14]。公共数据授权运营是指政府将公共数据授权给特定市场主体，通过开发数据产品和服务的形式精准满足社会对公共数据需求的过程，是实现公共数据资源的优质供给和政企数据融合的关键模式之一。《数据二十条》明确提出，对各级党政机关、企事业单位依法履职或提供公共服务过程中产生的公共数据，加强汇聚共享和开放开发，强化统筹授权使用和管理，推进互联互通，打破“数据孤岛”。鼓励公共数据在保护个人隐私和确保公共安全的前提下，按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供。

公共数据授权运营模式类似于企业数据流通模式Ⅱ和Ⅲ。公共数据授权运营模式如下图所示。在公共数据授权运营模式中，公共数据来源于各个公共数据持有部门，即在履行公共管理和服务职责过程中收集和产生数据的公共管理和服务机构。这些部门将公共数据统一归集到公共数据授权运营管理部门（例如各地建立的大数据中心等部门）。公共数据开放利用政府管理部门（例如各地政府办公厅数据管理办公室）负责管理该地区的公共数据开发利用，并统筹管理和监督公共数据授权运营管理部门开展公共数据授权运营工作。公共数据授权运营管理部门授权具有资质的机构（被授权运营主体）开展公共数据代运营。被授权运营主体建设公共数据授权运营平台，该平台应具有安全可信环境和隐私计算能力。公共数据授权运营管理部门将公共数据提供给公共数据授权运营平台进行开发利用。

直接基于公共数据采用隐私计算等方式与需求方进行数据融合分析计算的模式，类似于3.3.2中描述的数据流通模式Ⅱ，被授权运营主体可基于公共数据授权运营平台提供基于公共数据的多项数据融合分析服务。

[14]《上海市数据条例》，2021年11月

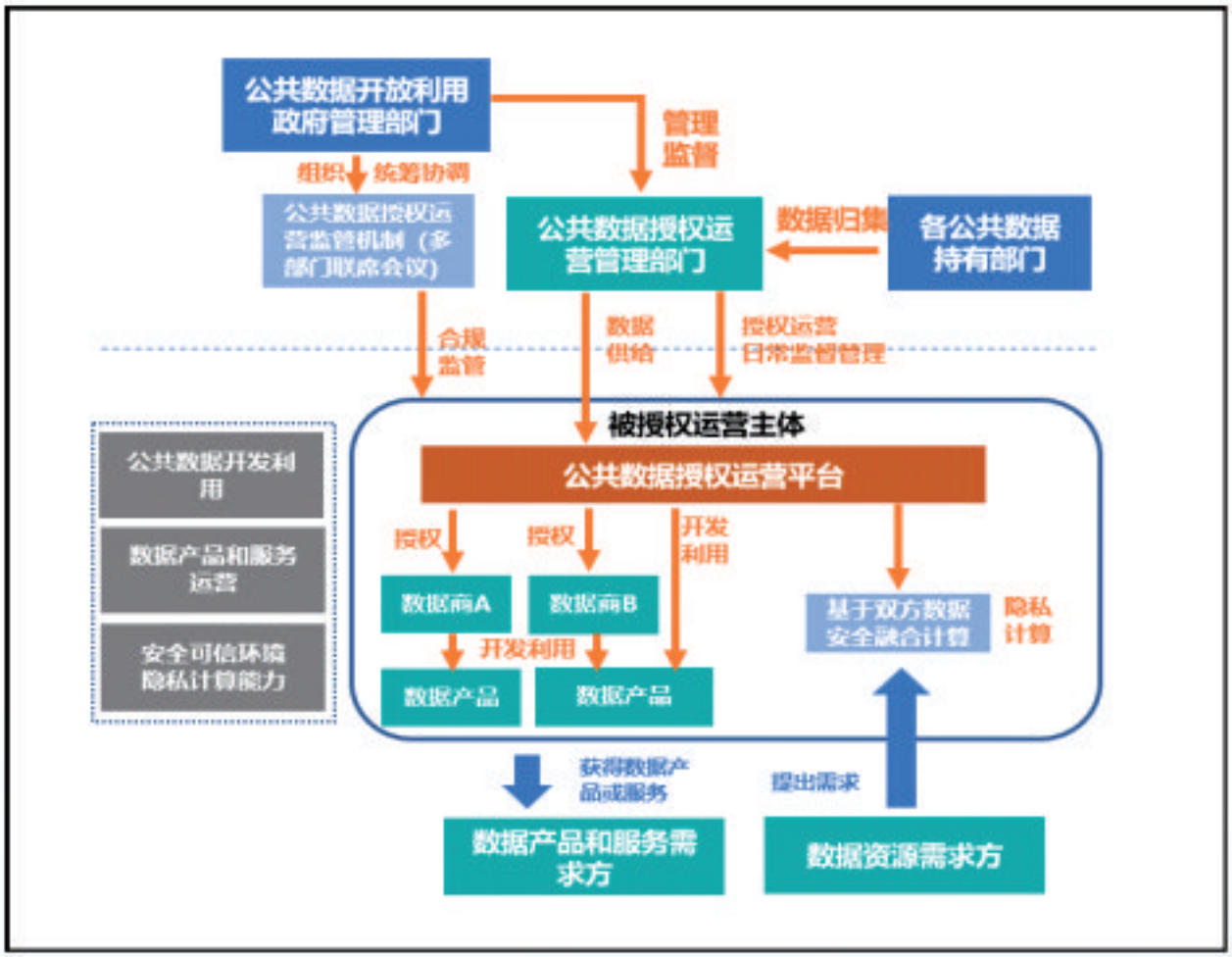


图12 公共数据授权运营模式示意图

另外，在以上授权运营模式的基础上，被授权运营主体再进一步把将公共数据开发成数据产品和服务的权利授权给多个数据商，数据商在公共数据运营平台上对公共数据资源进行开发加工，形成可对外提供的数据产品和服务，并通过经营活动提供给数据需求方。**这种模式类似于3.3.3中描述的数据流通模式Ⅲ**。例如2023年2月发布的《杭州市公共数据授权运营实施方案（试行）》征求意见稿，提出“加工使用主体按照协议对所申请的公共数据资源在数据开发与运营平台进行加工使用,形成可面向市场提供的数据产品或数据服务”。此外，被授权运营主体也可以基于自身技术能力直接对公共数据资源进行加工开发并形成数据产品或服务，提供给数据需求方。

此外，在上述模式中，公共数据开放利用政府管理部门组织成立公共数据授权运营监管机制（例如多部门联席会议的形式），对被授权运营主体和数据商的公共数据开发利用和授权运营活动开展合规监管。

3.3.2 公共数据权责利分配机制

权利分配：授权监督管理下的数据加工权和数据产品经营权。由于公共数据具有公

共属性，并可能涉及到大量个人信息和商业秘密，因此国家普遍对公共数据要素流通施加更加严格的安全管控。例如，《上海市数据条例》第四十四条规定，市大数据中心应当根据公共数据授权运营管理办法对被授权运营主体实施日常监督管理；第四十五条规定，市政府办公厅应当会同市网信等相关部门和数据专家委员会，对被授权运营主体规划的应用场景进行合规性和安全风险等评估。再如，《杭州市公共数据授权运营实施方案（试行）》征求意见稿规定，加工使用主体应当按照应用场景申请公共数据，实行“一场景一清单一审定”原则进行数据授权，数据产品或数据服务不得用于或变相用于未经审批的应用场景。

因此，相较企业数据流通场景，**公共数据流通场景具有更强制性的自上而下的安全管控机制设计，被授权运营主体持有的数据加工权和数据产品经营权更加具有非独立性。同样，数据商所享有的数据加工权和数据产品经营权也仅能基于被授权运营主体的授权，在其监督管理下享有强受控和受限的权利。**

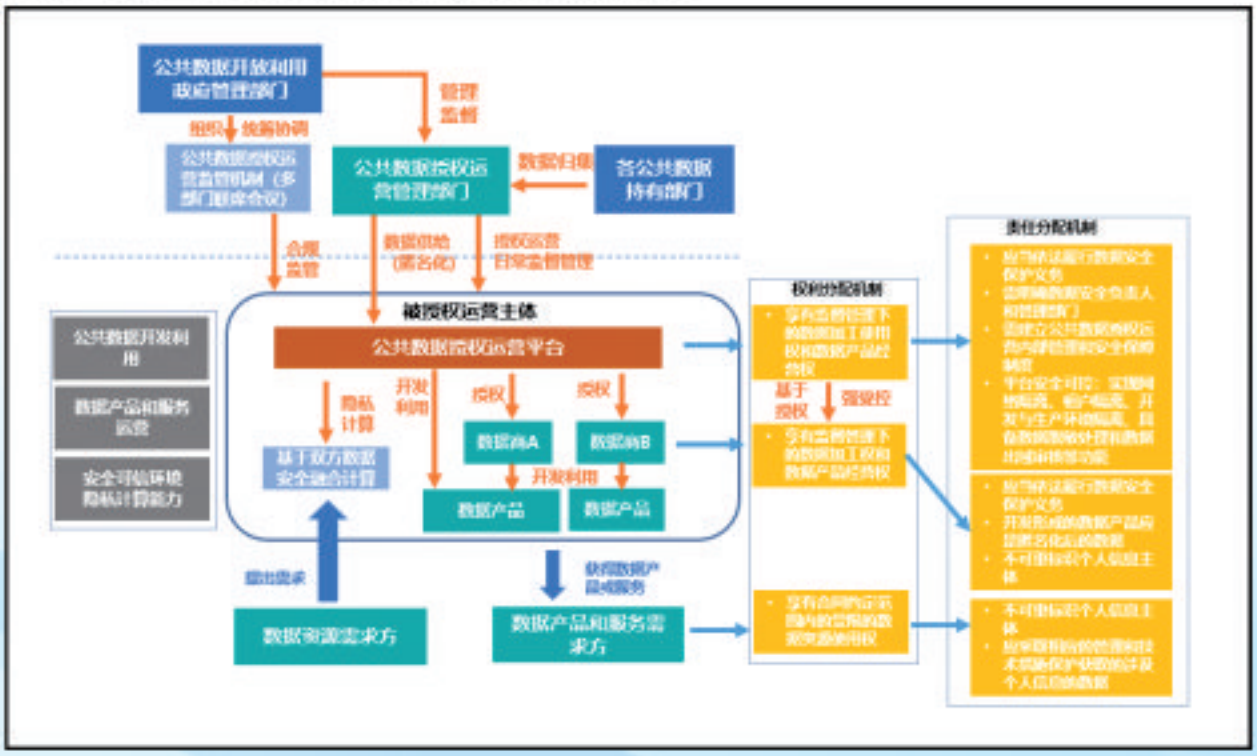


图13 公共数据授权运营模式权责分配机制

责任分配：被授权运营主体需承担更高水平的数据安全保护责任。例如，《上海市数据条例》第四十五条规定，授权运营的数据涉及个人隐私、个人信息、商业秘密、保密商务信息的，处理该数据应当符合相关法律、法规的规定；被授权运营主体应当依法履行数据安全保护义务。《杭州市公共数据授权运营实施方案（试行）》征求意见稿规定，加工使用主体需明确数据安全负责人和管理部门，建立公共数据授权运营内部管理

和安全保障制度；具备通过网络安全等级保护三级标准的系统开发和运维实践经验；按照《数据安全管理认证实施规则》通过数据安全管理认证规范数据处理活动，鼓励通过数据管理能力成熟度（DCMM）和数据安全能力成熟度（DSMM）3级以上认证；公共数据安全体系评估结果无高风险项。此外，北京市经济和信息化局授权北京金融控股集团有限公司下属北京金融大数据公司建设金融公共数据专区，北京金融大数据公司建立了涵盖系统运维、数据管理、合规管理等38项制度在内的数据安全管理制度体系。

因此，在公共数据要素流通场景下，为保障公共数据安全，被授权运营主体需按要求建立更高水平的数据安全保护能力，包括需明确数据安全负责人和管理部门、需建立公共数据授权运营内部管理和安全保障制度，并采取网络和数据安全技术措施实现平台安全可控。此外，数据商也应当依法履行数据安全保护义务，并且未经个人信息主体授权或有其他法律依据，不可利用持有的数据集重标识个人信息主体。

收益分配：公共数据授权运营收益模式应分为公益性和经济性两种。其中基于公共数据的公益属性，对于用于道路交通、证照证明、资源环境、教育文化、公用设施、公共卫生、公益事业等公共治理、民生服务、社会发展的公共数据，应推动无偿使用，而对于用于产业发展、行业发展的公共数据可采取有条件有偿使用的模式，并按政府指导定价确定数据交易流通价格。在第二种情况下，公共数据的收益产生于市场需求主体对

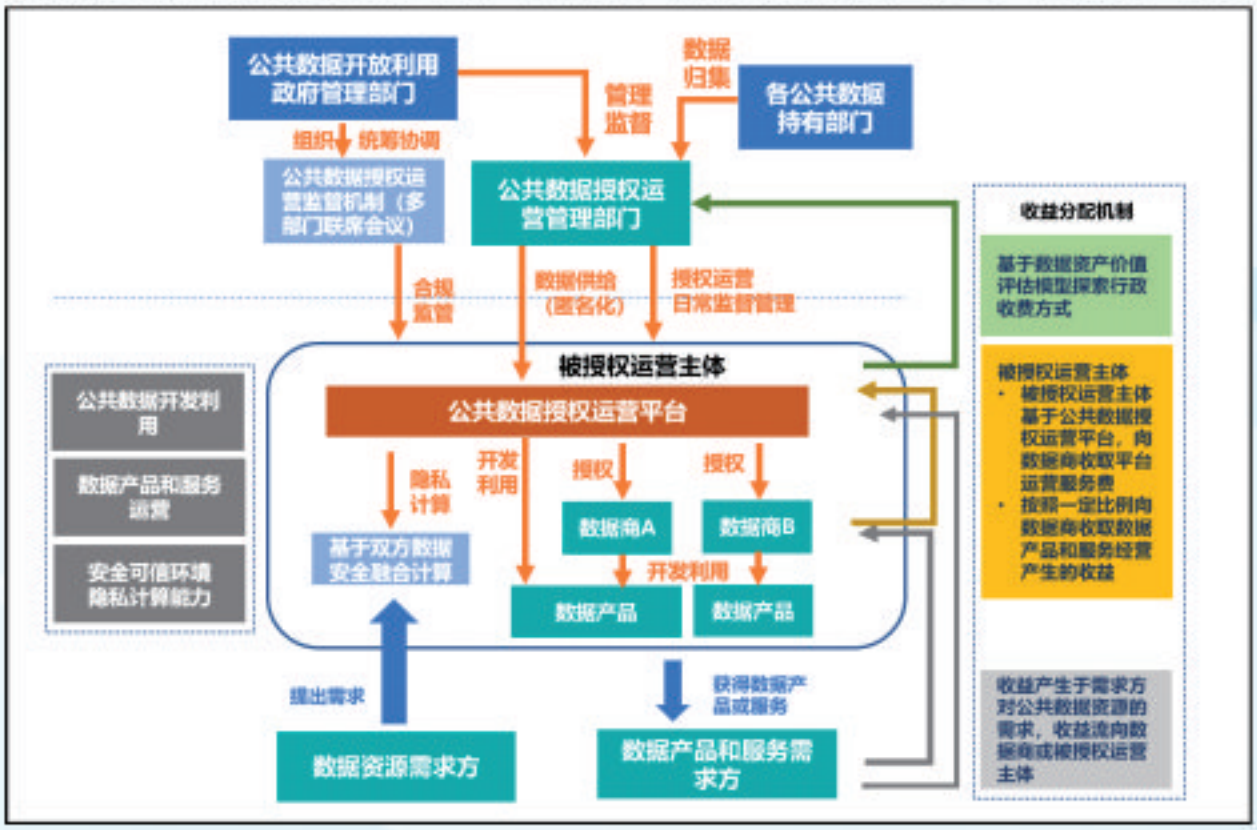


图14 公共数据授权运营模式收益分配机制

于公共数据资源的需求，对于由数据商开展数据产品经营的场景，公共数据流通产生的收益由数据需求方流向数据商。同时，由于被授权运营主体属于公共数据资源的授权提供方，因此这部分收益还需按照一定比例分配给被授权运营主体。

此外，由于数据商需在公共数据授权运营平台中对数据进行开发和加工，因此被授权运营主体可以基于公共数据授权运营平台，向数据商收取平台运营服务费。在此基础上，公共数据授权运营管理部门可基于数据资产价值评估模型探索行政收费方式。

此外，针对由被授权运营主体直接对数据开展价值开发活动，形成数据产品或服务并直接进行经营的情况，被授权运营主体可直接从数据需求方处获取收益。

3.4 数据流通对安全技术的需求

3.4.1 隐私计算实现数据“可用不可见”

隐私计算是一类技术的统称，用于数据流通利用过程中的数据安全与隐私保护。隐私计算可以理解为是在隐私保护的前提下，完成对数据的计算工作。面向敏感数据有使用需求而又不能明文出域的情况，隐私计算保障数据的隐私性和安全性，并使得数据参与了计算但是所有的参与者无法获取到敏感数据明文，达到数据“可用不可见”的效果。根据联合国大数据和数据科学专家委员（UNCEBD）发布的《联合国官方统计隐私增强技术（PETs）指南》报告，隐私增强技术分为两大类，分别用于输入隐私和输出隐私。“输入隐私”关注的是一方或多方如何以一种保证数据不会在域外使用的方式处理数据；“输出隐私”关注的则是使输出数据不能用于对原始输入进行逆向工程。隐私计算面对不同的场景，有多种技术路线可以适配，包括安全多方计算、同态加密、差分隐私、合成数据、分布式学习、零知识证明、可信执行环境和安全飞地等。当用户对隐私计算有需求时，可以综合使用多种技术来实现个人信息安全。

隐私计算作为促进数据流通利用的关键技术，是“三权分置”理论落地所必需的技术加持手段，隐私计算可以在保障数据安全的基础上分置出数据加工使用权和数据产品经营权，实现数据流通的安全可控，助力“三权分置”更好地落地于企业实践中。

当前，实现“原始数据不出域、数据可用不可见”的数据交易和共享模式已经成为业界推动数据流通的统一共识。企业侧一直在政策和市场的引导下积极开始数据要素可信共享融合，利用区块链、隐私计算等技术打造数据共享与隐私计算平台，确保原始数据不出域，仅提供数据计算的结果。

但隐私计算技术的应用在法律监管层面也存在一些挑战，目前国内外法律法规普遍尚未就采用隐私计算技术的合规性效果进行确认。这是因为不可能确保任何一项隐私计算技术在任何特定场景中使用的效果都是遵从法律法规的，例如对于在一个场景中已被

相关监管机构“批准”或积极评价的隐私计算技术，由于涉及的数据类型或数据来源方面的差异，可能在另一个场景中应用就不能完全满足合规性[15]。而要确定隐私计算技术的合规性效果，必须验证所有参与者都履行了所有的法律义务，并且需采用风险分析的方法来评判。因此，立法部门无法在法律法规中精确到要求采用任何特定的隐私计算技术。但这一问题确实对当前采用隐私计算技术造成了比较大的障碍。

目前，国内外立法和监管机构对允许甚至鼓励使用隐私计算技术越来越开放。立法者、公共机构已开始研究并发布在特定用例中使用隐私计算技术的建议和指南性文件，例如英国信息专员办公室一直在就隐私增强技术和匿名化工具发布相关指南。从目前行业应用实践来看，监管机构的具体指导将是推动采用新技术的关键一步。

3.4.2 利用区块链技术解决数据追踪难题

当前，数据要素市场化建设推动数据加速从企业内部流通延伸至外部共享、交易和使用，加大了数据流向和使用追踪难度。传统数据访问控制技术无法解决跨组织的数据授权管理和数据流向追踪问题，一旦数据集交付或接口调用结束，仅凭协议很难有效约束和监督数据需求方对数据的后续处理行为。需求方可能改变原有授权许可的数据处理目的，引发数据非法披露、未授权二次转移等数据滥用风险[16]。因此当前数据提供方对数据追踪技术的需求很强烈。数据流转追踪的应用对于保护标的数据安全，确保标的数据在适当范围内流转，保护相关主体的合法权益具有重要意义。

区块链，即一个又一个区块组成的链条。每一个区块中保存了一定的信息，它们按照各自产生的时间顺序连接成链条。相比于传统的网络，区块链具有两大核心特点：一是数据难以篡改、二是去中心化。基于这两个特点，区块链所记录的信息更加真实可靠，可以帮助解决互不信任的问题。因此，可以借助区块链的这些技术特点，解决数据流向难追踪的问题。具体而言，可以将交易的数据上链，并留存数据交易记录，以此实现数据交易每一环节的可信追踪。

除了技术层面以外，数据追踪需要考虑在必要范围内，给予供方一定的授权，允许供方或指定技术服务提供方利用数据追踪技术，跟踪标的数据在交付后的流转轨迹。

数据追踪技术对各方主体间互信的实现，将进一步促进三权分置理论落地，一方面可以促使数据加工权利的转移，另一方面可以监督数据需求方处理和使用数据的行为，一旦出现数据泄露等问题，可以作为存证手段证明需求方需承担相应的法律责任，同时通过更透明的方式保障供给方获取收益的权利。

---

[15] UNCEBD：UN Guide on Privacy-Enhancing Technologies for Official Statistics，2023

[16] 中国信息通信研究院安全研究所：数据要素流通视角下数据安全保障研究报告（2022年），2022年12

第四章 产业实践中“三权分置”的最佳模式案例

基于以上的“三权分置”实施路径，我们选取了产业界符合“三权分置”理论框架的业务实践案例，这些案例在技术和业务流程等方面能既能满足数据合规要求，又能很好地落实“三权分置”的制度理念，可以作为最佳实践案例供业界参考。

4.1 企业数据流通案例

4.1.1 金融场景营销

中国银保监会发布《关于进一步促进信用卡业务规范健康发展的通知(征求意见稿)》，要求银行不得以发卡量、客户数量等作为单一或主要考核指标，同时强化睡眠信用卡动态检测管理，严格控制占比，长期睡眠信用卡数量占发卡数量的比例不得超过20%。从市场而言，产业发展进入存量时代，粗放规模扩张和红利期打法不再适用，精准化触达增量用户、精细化运营存量用户，同时提升用户粘性，成为银行信用卡部门的战略目标。

从场景而言，在互联网领域，具备全链路营销方案、多维度触达渠道、高曝光资源位、消费黏性强，具备广泛的数据维度和精准数据纵深，是信用卡促活的“完美”阵地。为此，银行需要和流量端合作，进行广告营销。同时，银行的需求是，只想对同时符合电商平台的某些特质用户发起活动，得出最小集用户包，节约成本同时满足最小化原则。

在本案例中，银行机构和流量平台之间通过第三方机构提供隐私计算技术，实现了双赢。借助隐私计算技术，对双方的用户ID进行安全匹配，只得出共有交集，再对共有交集进行精准人群的识别和触达。最终，双方在互相不获得对方用户原始数据的基础上，银行机构通过流量平台触达到了消费者，通过在流量平台的支付环节给消费者更加优惠的支付方式，推广本银行业务，唤起低活跃用户，提高转化。

此案例符合3.3.1中描述的数据流通模式Ⅰ，其中流量平台是数据持有和提供方，银

行机构是数据需求方，同时也是其自身用户的数据持有方，第三方隐私计算技术提供方是数据技术提供商。流量平台和银行机构分别享有其自身用户数据的持有权，在此基础上，双方授权第三方机构享有基于合同范围内的数据加工权，第三方技术机构基于双方的原始数据采用隐私计算的技术对数据进行加工，得出用户共有交集，并通过提供最终的计算结果获取收益。

通过第三方机构的隐私计算技术方案，银行机构在没有获得流量平台原始数据的基础上实现了数据流通，避免了数据超范围使用和滥用，在合规前提下释放了数据价值。数据加工权被在一定范围内授权给专业的技术机构，通过权利分置，流量平台也通过提供数据价值获得了相应的收益。

4.1.2 平台跨端营销

目前互联网平台都普遍对跨端营销有很大的需求，但以往目标投放端不愿意共享自身的用户数据给需求方，因此需求方只能跨端盲投，这样做不仅成本高，而且转化率低，但引用隐私计算技术能很好的解决这一问题。

例如，平台A希望在平台B上投放活动广告进行营销。首先，双方基于各自用户ID数据，利用PSI隐私集合求交技术进行求交计算，得到双方的用户交集。PSI隐私集合求交采用密码学技术避免非交集数据的暴露，仅能得到加密交集。第二步，利用平台A的用户ID和标签数据，以及平台B的用户ID和用户特征数据，利用联邦学习、多方安全计算、可信硬件技术等技术进行联合建模。联合建模和预测过程中，仅有模型梯度信息交互，梯度信息通过同态加密/差分隐私保护，无法反推原始数据，实现数据“可用不可见”。第三步，基于联合模型对潜客意向度进行概率预测，形成预测指数分值，分值越高意向度越高。由平台A自主设定阈值，对阈值内目标用户进行投放。在预测过程中，采用数据去标识/脱敏/水印技术，确保阈值设定阶段的数据安全。第四步，对接平台B的APP等渠道完成广告投放，如APP端内广告（如开屏、横幅）、Push消息、短信营销等。

利用隐私计算技术，平台A在不获取平台B用户数据的前提下完成了基于平台B用户数据的精准跨端营销，转化率大大提升。在这个案例中，平台A和平台B都是数据资源持有方，平台A也是数据资源需求方，第三方隐私计算技术公司是数据技术提供商或数据服务提供商。平台A和平台B分别享有其自身用户数据的持有权，在此基础上，双方授权第三方机构享有基于三方协议范围内的数据加工权，第三方机构基于双方的原始数据采用隐私计算的技术对数据进行加工，并通过提供最终的计算结果获取收益。

在安全合规方面，一是通过基于密码学技术的PSI隐私集合求交避免非交集数据的暴露，二是在联合建模和预测过程中，仅有模型梯度信息交互，且梯度信息通过同态加密

/差分隐私进行保护，无法反推原始数据，实现数据“可用不可见”。通过上述数据安全流通技术，避免数据被非授权使用和滥用，确保合规性和安全性。

图15 平台跨端营销案例示意图

4.1.3 数据产品

数据产品是数据流通利用的重要形式之一。当前，商家跨平台经营也成为普遍现象，商家迫切需要整合与洞察跨平台的店铺经营数据的产品，辅助商家基于跨平台的数据洞察提升数字化运营能力。例如，为了获得更专业的数据产品服务，商家A将其自有的或从其他平台合法获得的店铺经营数据，委托数据智能服务技术公司B开发了一站式数据化运营工具（数据产品C）。该工具基于商家经营数据，为商家A提供跨平台经营场景的数据服务和经营动态，帮助商家快速制定运营计划。

上述工具使用的是不含个人信息的或剔除可识别或已识别个人字段后的商家经营数据，主要涉及商家的商业秘密，基于商家A授权以及委托服务协议，商家A将其提供给专业的数据智能服务技术公司B进行加工、整合，最终由数据智能服务技术公司B衍生出跨平台经营的数据产品并向商家A提供服务，该工具未侵犯消费者个人信息，同时获得了商家的授权，在合规性方面符合我国法律法规要求。

此案例符合3.3.3中描述的数据流通模式Ⅲ，其中数据持有、提供方以及需求方均是商家A，数据产品开发商是数据智能服务技术公司B。商家A享有数据资源持有权，授权给数据智能服务技术公司B数据加工使用权和数据产品经营权。原始数据是商家的店铺经营数据，数据产品是上述一站式数据化运营工具。

这个案例通过三权分置使得数据的价值得以释放，数据产品开发交由专业的技术公司来完成，并由专业的运营团队来经营数据产品取得收益。

4.2 公共数据流通案例

4.2.1 授权建设金融公共数据专区

为推动某市公共数据在金融及社会领域的应用，该市经济和信息化局创新“政府监管+企业运营”的公共数据市场化应用模式，利用金融业覆盖领域广、数据需求大、应用场景多等方面的优势，授权某国有企业下属金融大数据公司建设金融公共数据专区，并承接公共数据亟需、特需的工商、司法、税务、社保、公积金、不动产等多维数据25亿余条，覆盖14个部门机构、240余万市场主体，实现按日、按周、按月稳步更新，公共数据汇聚质量和更新效率均处于全国领先水平，实现全国首个公共数据授权运营模式落地。

（1）“政府监管+企业运营”模式，明确相关职责

授权合规运营机构，明确政企相关职责。该国有企业是人民银行确定的全国5家金控公司模拟监管试点机构之一，其下属金融大数据公司由该市经济和信息化局授权建设运营金融公共数据专区。专区作为该市大数据行动计划的重要组成部分，承担全市金融公共数据“统、管、用”职责及创新应用任务，并接受地方金融监督管理部门、市经济和

信息化局及数据提供部门机构的监督和管理。

（2）“三个构建” 确保数据安全合规

构建完善的数据安全管理制度体系、数据集成开发平台、敏感数据输出的脱敏规则及主体授权机制，确保数据安全合规输出，提升数据标准化服务水平。针对数据脱敏难问题，金融公共数据专区建立了涵盖系统运维、数据管理、合规管理等38项制度在内的数据安全管理制度体系，利用多方安全计算等技术建成数据集成开发平台，对数据进行集中清洗、加工和脱敏，确保敏感数据不出域，实现数据价值不打折。

4.2.2 公共数据授权运营&数据经纪人模式案例

银行在贷前和贷中监管都需要大量数据支撑。例如，在放贷前对客户进行尽职调查时，银行希望获知相关数据，从而更好地进行产品设计和客户筛选。我国某市探索出一条“政府主导规则，各方形成合力，共同从数据中获益”的新模式。该市授权一家国资企业作为公共数据运营服务商，助力解决数据可靠问题，并遴选行业内具有丰富数据应用经验的两家企业作为数据经纪人，撮合数据供需双方，从而更好解决数据交易互信问题，达成数据交易流通。

作为数据经纪人，这两家企业与10家数据需求方签订了公共数据需求服务协议，数据产品所有方（上述国有企业）与6家金融机构签订了公共数据产品服务合同，在公共数据支持企业融资等方面先行先试。

通过数据产品扫清金融机构和融资企业间信息不对称的障碍，有效缓解了企业融资难、融资贵问题，有助于解决金融机构对中小微企业“不敢贷、不愿贷、不能贷”问题，也为保险机构在投保获客、承保企业风险分级分类管理、保险产品设计方面提供了数据支撑。

第五章 总结与建议

5.1 关键结论

《数据二十条》的发布为加快我国数据要素高效合规流通指明了方向，但具体如何破解当前的现实困局是法律界、行业界、公共部门等各方亟需研究和突破的难题。本报告基于《数据二十条》提出的“三权分置”数据产权机制，以及当前我国数据要素流通面临的瓶颈，为产业实践提供了具体的实施路径参考。综上，本报告的关键结论为：

（1）数据要素市场的生产关系构建需“技术+合同+管理”三管齐下。当前数据安全问题是阻碍数据要素流通的最痛点问题之一，数据价值得不到充分释放的症结在于个

人数据权利扩张背景下带来的权利捆绑困局。解决隐私安全成为解绑数据权利的关键途径。因此，技术是最直接的解决方案。通过发展隐私计算等数据加工利用技术，实现“数据不动价值动”，在管控安全与合规风险的同时松绑数据的流通和利用。同时，技术不能解决全部问题，合同和合同之外的企业合规管理措施是明确权利和约束责任的重要手段。通过合同协议约定数据流通利用相关的权责利关系，并施加对外的事前、事中、事后的合规管理机制，是在技术之上有效管理风险、落实尽职履责的关键举措。

（2）应落实所有数据流通参与主体的数据安全保护责任。报告提出个人数据的高效流通利用应以重标识风险可控为前提，即应结合数据披露程度、预期接收者、拟采取的控制手段等，通过采用技术和管理手段相结合的风险管控方式，将重新识别个人信息主体的可能性降到足够低，实现个人信息的“无法识别特定自然人且不能复原”。因此，数据安全风险管理涉及数据流通利用的每一环节和每一个参与主体。每个阶段的数据流通参与主体都应基于持有的数据和获得的授权承担相应的法定责任。在三权分置框架下，匹配合理的数据安全责任分担机制，是消除数据持有方顾虑、实现数据安全风险可控并最终激活数据要素市场的前提。

（3）数据权利的范畴应以法律法规和合同约定为边界。从本报告对三种企业数据流通模式以及公共数据授权运营模式中数据权利分配机制的分析可以看出，数据资源持有权、数据加工使用权、数据产品经营权的权利职能范围都需在法律规定或合同约定的范围内行使。其中数据资源持有权代表数据的持有者有权依照法律规定或合同约定自主管控所取得的数据资源，并拥有排除他人对控制状态侵害的权利。但数据资源持有权并不代表可以采用任意方式对数据进行加工和处置，而是需在法律规定或合同约定的范围内。数据加工使用权和数据产品经营权的职能范围则更加受限，两者都来源于数据持有者的有条件的权利授予，因此都被限定在合同约定的范围内。

5.2 主要建议

本报告结合产业实践，对我国数据要素流通市场发展提出以下几点建议：

（1）产业界应积极探索，为国家政策法规制定提供更多实践参考。《数据二十条》明确提出，积极鼓励试验探索，坚持顶层设计与基层探索结合，支持浙江等地区和有条件的行业、企业在制度建设、技术路径、发展模式等方面先行先试。因此，在当前国家相关配套政策和法律法规尚未建立健全的阶段，产业界在技术和模式方面的实践路径探索将加速国家政策的出台，为其提供更多的实践案例参考。例如数据产权的分置，尤其是数据加工权和产品经营权的市场流通模式及其示范合同，作为数据流通的关键前提，可从市场实践中积累经验。产业界可以积极在实践中通过合同约定的方式探索数据的确

权授权和权利的市场化流通，充分发挥市场在资源配置中的决定性作用，积累市场经验，并最终为我国相关法律法规的制定提供实践经验。

（2）国家层面应尽快建立弹性包容的数据要素流通监管机制。当前，数据持有方对安全风险的担忧使得数据流通在起点处就失去了动力。国家层面应尽快制定数据流通和交易的负面清单，明确不能交易、限制交易、鼓励交易的不同类型数据项或场景，划定合规监管红线，为市场主体的责任判断提供更加稳定的预期。同时，加快建立健全鼓励创新、包容创新的容错纠错机制，在监管红线之上，建立弹性包容的数据要素流通监管合规机制。

（3）建议加快推进数据要素流通试点示范。国家数据局可在全国范围内针对公共数据、企业数据和个人数据等不同类型数据的交易和流通，遴选流通模式创新高效、各方权益充分保障、数据利用价值高且安全合规的数据流通典型案例，开展试点示范工作。应采取措施激励试点地区和试点企业创新数据流通的新模式和新业态，并作为典型案例在各行业各地区推广。

（4）加快数据流通安全技术创新发展和标准化建设。当前隐私计算、区块链、数据沙箱等数据流通安全技术的应用范围尚不够广泛，技术水平良莠不齐，技术标准尚未建立健全，技术实施的法律效果尚待明确，技术应用尚处于发展初期。因此，应加大对数据流通安全技术的研发投入，鼓励企业加强技术创新和融合应用，为数据高效、合规流通提供更多有效的解决方案。同时，应加快数据流通安全技术标准化建设，不仅可以规范技术市场化应用，还能降低数据需求方在交易中的安全性、合规性顾虑。