



中国数据产权制度蓝皮书

(2022)

人民数据 | 浙江大学网络空间安全学院

2023年5月

版权声明

本报告版权属于人民数据，并受法律保护。转载、摘编或利用其他方式使用本报告文字或者观点的，应注明“来源：人民数据”。违反上述声明者，将追究其相关法律责任。

编委会

学术顾问: 王春晖 任 奎

主 编: 郑光魁 方兴东

副主编: 刘 畅 陈 丽

学术支持单位: 浙江大学网安学院、浙江大学网络空间国际
治理研究基地

编写人员: (按照姓氏字母顺序排名)

白 杨 褚晓坤 邓思敏 甘怡淳 顾烨烨 侯鑫淼 黄小龙

李 放 李熠超 刘 聰 刘金飞 刘文中 马 炬 唐 风

王 简 王 姚 吴汉华 吴 健 吴梅芳 薛 峰 杨森滟

叶德恒 张文祥 赵秀梅 钟祥铭 钟新星 周佳琪 左卓瑾

美编: 周 波 薛 娴

前 言

习近平总书记指出，要构建以数据为关键要素的数字经济。数据作为新型生产要素，已快速融入到生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。近年来，我国数字经济快速发展，数字经济规模已经连续多年位居世界第二，数据规模量持续上升。数据显示，2022年，我国数据产量达8.1ZB（泽字节，代表十万亿亿字节），同比增加22.7%，占全球数据总量的10.5%。据IDC测算，中国2025年数据量将增至48.6ZB，占全球总量的27.8%。

我国数据要素市场也在不断扩大，数据要素作为数字经济深化发展的核心引擎，促进数字技术与实体经济深度融合，推动我国经济的高质量发展。数据显示，2021年，我国数据要素市场规模达815亿元，预计“十四五”期间市场规模复合增速将超过25%，整体将进入群体性突破的快速发展阶段。

数据要素市场是一个横跨各领域的综合要素市场，我国数据资源规模大、应用场景丰富，新形势下充分发挥数据要素的基础作用和创新引擎功能，激发数据要素与其他生产要素融合，对其他要素的叠加、倍增、乘数效应，可以充分发挥我国海量数据规模和丰富应用场景优势，推动资源快捷流动、市场主体加速融合，提升经济社会各领域资源配置效能，不断做强做优做大我国数字经济，拓展经济发展新空间。其

中，数据要素制度建设至关重要。

习近平总书记强调，数据制度建设事关国家发展和安全大局，要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据制度体系。数据制度建设关系着我国数据要素市场发展的根基。激活数据要素潜能，进一步增强经济发展新动能，需加快构建数据制度，更好发挥数据要素作用。

《中共中央 国务院关于加快建设全国统一大市场的意见》《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）、《数字中国建设整体布局规划》、国家数据局组建等利好消息，促进我国构建数据制度，形成数据要素市场“全国一盘棋”，推动我国数据要素高质量发展。

“数据二十条”提出加快构建数据制度，提出“充分发挥我国海量数据规模和丰富应用场景优势，激活数据要素潜能，做强做优做大数字经济，增强经济发展新动能，构筑国家竞争新优势”的目标，要求建立保障权益、合规使用的数据产权制度，合规高效、场内外结合的数据要素流通和交易制度，体现效率、促进公平的数据要素收益分配制度，安全可控、弹性包容的数据要素治理制度。

其中，数据产权制度更是“基础”。只有完善数据产业

链中各劳动主体的权益配置，才能促进数据的应用，加快数字经济的高质量发展。

当前，我国数据要素市场的建设尚处于探索阶段，数据要素确权、定价、流通、监管等基础制度体系尚不健全，从数据要素市场的全流程看，数据要素的供给与流通环节均待进一步优化和完善。数据权益和行为规则界定不清带来的些问题日益显现，数据权益相关纠纷呈上升趋势。因此，必须通过构建数据产权制度，实现数据要素的获取、加工、流通、利用以及收益分配等行为有法可依、有规可循，才能推动数据要素市场规范化、制度化建设，最终有效提升数据要素的市场化配置效率。

没有归属清晰、合规使用、保障权益的数据产权制度，就无法形成高效公平、安全可控的数据要素市场。数据要素市场运行的前提是产权配置清晰，确立数据产权制度，需要解决数据产权在两大层面的清晰问题：一是数据在法律层面的清晰；二是数据在经济层面的清晰。

数据确权是世界性难题，目前欧盟、美国等地区也正探索数据要素的确权授权机制。构建具有中国特色的数据产权制度体系是我国未来数据要素发展的方向。国家发展和改革委员会提出构建数据产权制度的主要思路：一是探索数据产权结构性分置制度；二是建立健全数据要素各参与方合法权益保护制度；三是数据分类分级确权授权，主要针对数据持

有主体——公共数据、企业数据和个人数据。

“数据二十条”提出探索数据产权结构性分置制度，“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”，并指出推进实施公共数据确权授权机制、推动建立企业数据确权授权机制、建立健全个人数据确权授权机制。“数据二十条”对公共数据、企业数据、个人数据的确权授权提出系列性指导意见，也为构建数据产权制度提供了发展方向和主要思路。

建立“归属清晰、合规使用、保障权益”的数据产权制度，可以为数据要素流通和交易制度体系、数据要素收益分配制度体系、数据要素治理制度体系夯实基础，促进我国数据基础制度建设，激活数据要素潜能，推动我国数字经济高质量发展，加快建设数字中国，助力实现中国式现代化。

目 录

第一章 我国数据产权制度研究的背景	1
第一节 数据产权理论研究现状	1
1.1.1 科斯与现代产权理论	4
1.1.2 数据产权权属研究	6
1.1.3 数据要素与数据保护机制研究	10
第二节 数据产权制度法律法规探索	14
1.2.1 国家大数据战略	14
1.2.2 数据正式成为生产要素	20
1.2.3 数据产权相关法规	23
1.2.4 数据安全法	30
第三节 数据生产力促进生产方式根本变革	33
1.3.1 数据生产力的提出	34
1.3.2 数据生产力的研究现状	34
第二章 我国数据产权制度内涵	37
第一节 我国当前数据及各类产权制度	38
2.1.1 我国当前生产要素的产权制度解析	38
2.1.2 数据产权区别于其他产权的独特性	51
第二节 建立数据产权制度的重要性分析	53
2.2.1 数据产权制度是“四大制度”的核心	53
2.2.2 确权是数据交易流通的前提	55

2.2.3 授权是数据交易流通的重要方式	57
第三章 主要发达国家数据要素产权发展介绍	59
第一节 当前数据要素的通用性国际规则介绍	59
3.1.1 各主要发达国家的相关法规政策	59
第二节 美国对数据要素、数据产权的做法解析	62
第三节 欧盟对数据要素、数据产权的做法解析	66
3.3.1 GDPR 规范数据要素	67
3.3.2 《数据治理法》《数据法案》对数据确权授权的规范	68
第四节 RCEP、DEPA 等区域性组织的数据规则	72
3.4.1 RCEP 中数据要素的章节	72
3.4.2 DEPA 数据要素相关的内容	75
3.4.3 CPTPP 与数据跨境流动相关的规则	77
第四章 探索建立数据产权制度、推进技术发展	80
第一节 推动实施公共数据确权授权机制	81
4.1.1 公共数据的界定及使用	81
4.1.2 公共数据现有产权机制现状	87
4.1.3 公共数据产权机制应遵循的原则	100
第二节 推动建立企业数据确权授权机制	106
4.2.1 企业数据的内涵及要点	107
4.2.2 企业数据现有产权机制现状	115
4.2.3 企业数据产权机制运行要求及原则	124

4.2.4 企业数据分类分级发展现状及使用原则	133
第三节 建立健全个人信息数据确权授权机制	138
4.3.1 个人信息数据的界定	138
4.3.2 个人信息数据产权机制现状	148
4.3.3 个人信息数据产权机制处理规则与原则	165
第四节 推动数据产权的技术发展与应用	176
4.4.1 现有技术在数据产权的探索	176
4.4.2 数据产权技术方面的未来发展	184
4.4.3 数据交易所等数据产权探索	186
第五章 建立健全数据要素各参与方合法权益保护制度的思考 ..	190
第一节 保护数据来源者合法权益	191
5.1.1 保障知情同意权、可携带权和收益权	191
5.1.2 法律、平台、标准共同保护合法权益	193
第二节 保护数据处理者合法权益 确立准入机制	195
5.2.1 数据处理者的身份界定与权益依法保护	196
5.2.2 制定数据处理者准入的标准	200
第三节 依法保护数据及数据衍生产品的经营权	201
5.3.1 依法规范数据使用者许可他人的权利	202
5.3.2 保障数据衍生产品的合法权益	203
第四节 做好数据全生命周期的服务	204

表目录

表 1 中国国家大数据战略部分文件	17
表 2 国内信息数据相关法律法规	24
表 3 区域数据管理条例	26
表 4 五类生产要素产权制度组成	54
表 5 部分地方立法条例或管理办法	85
表 6 我国数据交易所相关信息	89
表 7 数据分级确定参考规则	135
表 8 隐私计算各技术路径总结	184

图目录

图 1 2010—2021 年全球数据量增长情况	3
图 2 2017—2021 年我国数据产量及全球占比情况	15
图 3 我国地级以上数据开放平台数量	88
图 4 秧归脐橙大数据平台展示	92
图 5 北京市金融公共数据专区场景案例展示	95
图 6 人民版权智能大屏	121
图 7 世纪互联个人数据中心建设图	153
图 8 世纪互联个人数据中心各部分联系示意图	155
图 9 Nexus 手机：第一款基于人民数保的示范产品	157
图 10 用户权限授权场景示意图	170
图 11 联邦学习流程图	179
图 12 联邦学习分类	181
图 13 ARM TrustZone 架构	183
图 14 人民数据确权流通平台示意图	209

场景案例目录

场景案例 1	91
场景案例 2	94
场景案例 3	119
场景案例 4	151
场景案例 5	155
场景案例 6	168
场景案例 7	206

摘要

蓝皮书对我国数据产权制度进行梳理研究，探讨数据产权制度的内涵，了解主要发达国家当前数据要素产权发展情况，并从公共数据、企业数据、个人数据等方面探讨建立数据产权制度，对建立健全数据要素各参与方合法权益保护制度提出一定的思考建议。

第一章主要探讨我国数据产权制度研究的背景，对数据产权理论研究现状进行梳理，深入研究相关法律法规，并指出数据生产力变革生产方式的作用。

第二章主要探究我国数据产权制度的内涵，通过对我国当前生产要素产权制度的解析，发现数据要素产权制度的独特性，并解析建立数据产权制度的重要性。

第三章主要介绍主要发达国家数据要素产权制度的内容，对美国、欧盟、国际组织的数据要素产权制度的内容进行剖析。

第四章主要解析建立数据产权制度中公共数据、企业数据、个人数据的确权授权机制的重要方面，并介绍当前推动数据产权的技术发展与应用。

第五章主要分析建立健全数据要素各参与方合法权益保护制度中，保护数据来源者、数据处理者及数据经营者的主流方式。

第一章 我国数据产权制度研究的背景

第一节 数据产权理论研究现状

数据是数字经济的核心关键要素，数据要素对经济社会的发展起着关键作用。2020年4月，中共中央 国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，正式将“数据要素”列为五大生产要素之一，与土地要素、劳动力要素、资本要素、技术要素并列。“数据二十条”提出建立四大数据基础制度：一是建立保障权益、合规使用的数据产权制度；二是建立合规高效、场内外结合的数据要素流通和交易制度；三是建立体现效率、促进公平的数据要素收益分配制度；四是建立安全可控、弹性包容的数据要素治理制度。^①其中，数据产权制度体系是其他三大类数据要素基础制度体系的根基，数据产权制度体系下的基础制度在“数据二十条”中多达五项，从数据产权结构性分置，到公共数据、企业数据、个人数据的确权授权，以及对数据要素各参与方合法权益的保障，构建了数据产权运行的基本规则，为其他三类数据要素制度的建设奠定了基础，因此，没有归属清晰、合规使用、保障权益的数据产权制度，就无法形成高效公平、安全可控的数据要素市场。^②

2023年3月，国家数据局正式获批成立，负责协调推进

^① 王春晖：《解析“数据二十条”中的数据产权制度》，东方法学，2022.12.22. <https://mp.weixin.qq.com/s/m9Q9QXbjmRzIYSEvwk1CcA>.

^② 王春晖,方兴东《构建数据产权制度的核心要义》，《南京邮电大学学报（社会科学版）》，2023.2.10.

数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。这表明，国家对数据要素的高质量发展越加重视。

数字经济发展迅猛，全球数据规模爆发增长、海量聚集。随着行业集中度的逐步提升，全球超大型数据中心数量总体增长。据 Synergy Research Group 的最新数据，截至 2021 年，超大规模提供商运营的大型数据中心总数增加到 700 个左右，较 2020 年同比增长 17.25%，该机构预测，据目前已知的 314 个未来新超大规模数据中心的规划，运营数据中心的安装基数将在三年内突破 1000 个大关，并将继续快速增长。依据 IDC 发布的《数据时代 2025》报告，随着 5G、物联网的发展，2010—2021 年数据呈现爆发式增长状态，2020 年全球数据量为 60ZB，初步统计 2021 年达到 70ZB；预计 2025 年全球数据量将达到 175ZB（见图 1）。^①同时，据 IDC《中国数据库安全能力市场洞察（2022）》预计，到 2026 年，全球结构化与非结构化数据总量将达到 221.2ZB。

^① IDC. Worldwide IDC Global DataSphere Forecast, 2022 - 2026: Enterprise Organizations Driving Most of the Data Growth [EB/OL]. 2022-05. <https://www.idc.com/getdoc.jsp?containerId=US49018922>

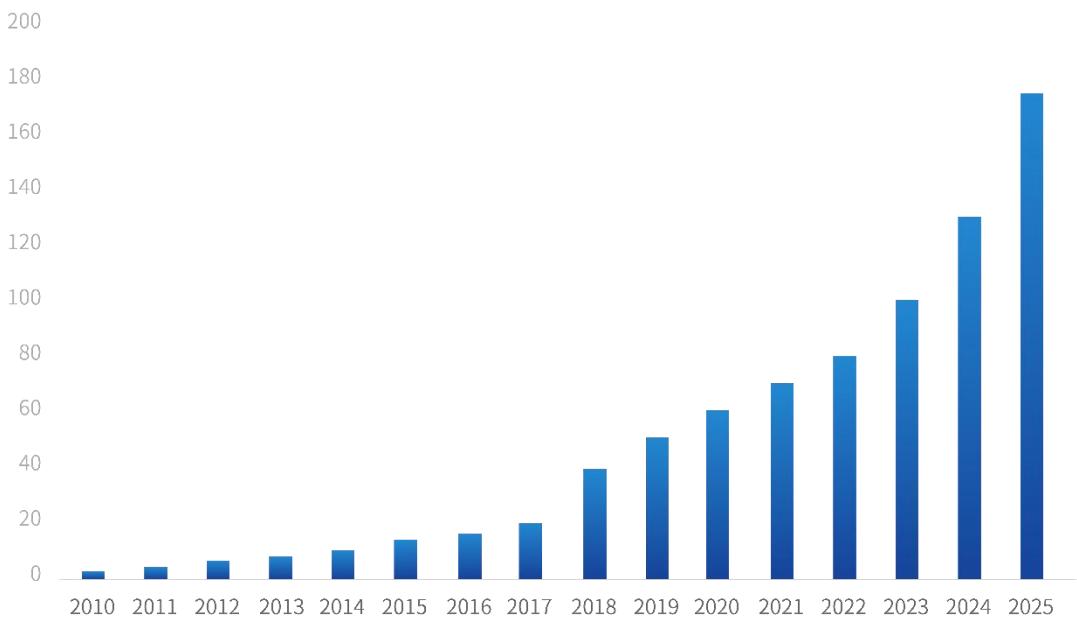


图 1 2010—2021 年全球数据量增长情况

来源：IDC 前瞻产业研究院（单位：ZB）

近年来，国内外学者对数据产权相关问题展开深入研究。数据权利属性作为社会治理的法律逻辑起点，既关系到公民的个人隐私保护问题，又与数据的收集、分析、运作主体行为的界定与划分密切相关，研究其属性能为数据保护提供立法参照。吕志祥、张强（2019）认为，数据作为信息技术发展后的存储介质，自发地与人们的财产权利、人格权利相连接，形成了一种存在广泛争议的权利形态，并且需要得到自身发展的路径。在私法中，“法无规定皆自由”的精神，使我们看到民法领域可以作为数据权利进入法律体系的突破口，提升整个社会对数据权利的认知。^①

浙江大学教授、网络空间治理与数字经济法治（长三角）研究基地主任王春晖指出，数据产权制度的确立，最重要的

^① 吕志祥, 张强: 《大数据背景下数据权利的法理分析》, 昆明理工大学学报（社会科学版）, 2019, 19(01):18-23.

是解决数据产权的法律层面清晰和经济层面清晰的问题。可见，构建数据产权制度必然要加快完善相应的法律法规体系，加强对数据产权的支持与保护，准确定位数据产权权属。

在定位数据产权权属之前，首先要对现代产权理论有所了解，在现有研究中，对大数据权利属性的定位主要有隐私权说、新型人格权说、知识产权说几种主要观点，基于此，学者们还对数据要素与数据保护机制进行了探讨。

1.1.1 科斯与现代产权理论

现代产权理论始于新制度经济学鼻祖罗纳德·哈里·科斯对企业和交易费用的研究。1937年11月，科斯发表《企业的性质》，指出价格机制运行并非像古典经济学描述得那样平滑，经济主体发现价格会有交易、谈判与签约等成本。而企业这一组织形式减少了市场上价格发现与讨价还价的费用，从而节约了生产成本，提高了社会生产效率。针对普遍存在的外部性问题，1960年，科斯发表《社会成本问题》，首次使用交易费用概念，并把交易费用、产权界定与资源配置效率联系起来，揭示了产权的不同安排对资源配置的重要作用。^①

科斯第一定理的含义是：在市场交易费用为零时，产权安排对经济资源配置没有影响。这是因为各市场主体会进行无交易成本的要素充分交换，从而使自身效用增大，直到各

^① 张燕飞：《现代产权思想的变迁》，中国政法大学学报，2021, No. 83 (03) :105-116.

方都无法在不损害他人效用的前提下提升自己的效用，此时即达到了帕累托有效的均衡状态。交易费用为零时，无论初始的产权如何配置，社会都会通过交换经济最终变成这种均衡状态。

科斯第二定理的含义是：在交易费用大于零的现实世界，产权的不同界定将对资源配置产生不同的效率。科斯第三定理的含义是：在交易费用为正的现实情况下，制度安排本身也是有成本的。这两则定理更为贴近现实，为数据产权的研究提供重要参考价值。

数据作为一种生产要素，其使用权无疑也是一种可交换的产权。而在相关市场主体利用数据信息进行生产活动时，也可能会产生外部性问题，对个体用户隐私和生命财产安全的负面影响等，例如企业的排污行为就会影响周围居民的生活环境。所以数据的各方面权利应当和污水排放权一样，作为一种产权置于交换经济中。生产主体方和数据来源方依据自身的效用函数，来交易解决利用数据进行的生产活动中的外部性问题。

从解决外部性问题出发，科斯第一定理是为第二、三定理做铺垫，阐述了新古典经济学中市场会自动实现资源最优配置的传统理论。科斯第二定理认为在交易费用较小的情况下，只要产权界定清晰，外部性当事人可以通过产权交易解决外部性问题，政府应把产权界定给能以较低交易费用解决

外部性问题的一方。科斯第三定理的核心是制度生产和运行也有其成本，我们应当选择带来净产值最大的制度安排，不论它是市场交易机制还是政府管制机制。根据这样的理论思想，我们可以进一步研究数据产权具体应该采取怎样的界定和制度安排。

不过，科斯本人并没有对什么是科斯定理给出正面的直接回答，而是不同的学者在阅读科斯的著作过程中对其中体现的经济学思想做出的总结。用通俗的语言对其可以进行如下描述：只要产权是明确的，并且交易成本为零或者很小，那么，无论在开始时将产权赋予谁，市场均衡的最终结构都是有效率的，能够实现资源配置的帕累托最优。^①

1.1.2 数据产权权属研究

纵观国内现有与数据产权权属相关的研究，主要有隐私权说、新型人格权说、知识产权说三种。每种理论的解释都有其合理性和一定缺陷。隐私权说很好地贴合了一直以来各方对个人数据的隐私属性的认同，新型人格权说则强调了数据的财产权属性，但两者都局限于个人数据的层次。知识产权与数据产权在法律属性上相似，但具体使用的理论更为复杂。

（1）隐私权说

^① 田洪鳌：《科斯定理中产权概念的法学解析》，东北师大学报（哲学社会科学版），2011, No. 250 (02) :209-211.

我国《民法典》三个版本的草案中都将关于个人数据的规定放在“隐私权”章。隐私权说倾向于将个人数据信息作为隐私权保护的代表，其将隐私权视为基本人权，关系到人的荣誉和尊严，而为此以从上至下的理念和方法来制定法律，限制对个人数据信息的使用，对其使用需要得到数据信息主体的明确同意。McDermott (2017) 认为隐私权说反映了欧洲法律秩序中的关键价值属性，即隐私、透明度、自主性和非歧视。^①但很多学者表示不应过分“隐私思维”，不应该将隐私权与数据保护过度联系起来，Fuster 和 Gellert(2012)认为将两种权利混淆的观点是错误的，数据保护权为个人提供了比隐私权更多的个人数据控制权，并提倡在司法上将两种权利相区分。^②

(2) 新型人格权说

新型人格权说从个人数据的角度出发，认为经济的发展导致人格权的商品化、现有的隐私制度不足以保护个人数据信息，应当创立一种新型人格权以实现个人对自身信息资料的自主控制，即“个人信息资料权”。

高志宏 (2022) 认为就属性而言，隐私权具有人格权属性，数据仅具有财产权属性，而个人信息兼具人格权属性和

^① McDermott Y. :Conceptualising the Right to Data Protection in An Era of Big Data. *Big Data&Society*. 2017, 1-7.

^② Fuster G G. , Gellert R. :The Fundamental Right of Data Protection in the European Union: In Search of An Uncharted Right. *International Review of Law, Computers & Technology*. Vol. 26, No. 1, March 2012, 73-82.

财产权属性。^①因此，新型人格权与隐私权相接近但又有所区分，个人数据既包括隐私数据，也包括非隐私的数据。数据人格权的产生背景、权利内容和保护措施都有别于传统隐私权。^②哈耶克认为数据人格权的主要支撑是责任规则，即“只要愿意支付一个客观确定的价值，就可以消灭一个初始法益”。^③换言之，法定情形下，他人可以以法定赔偿强行剥夺责任规则下的法益。

（3）知识产权说

国家知识产权局高度重视数据知识产权，陆续发布《知识产权强国建设纲要（2021—2035年）》和《“十四五”国家知识产权保护和运用规划》等文件，对构建数据知识产权保护规则、实施数据知识产权保护工程等作出部署。各地高度重视数据知识产权工作，稳步推进相关工作：北京市、上海市、江苏省、浙江省、福建省、山东省、广东省等地成为数据知识产权工作的试点地方，并作为“先遣队”，从推动制度构建、开展登记实践等方面开展数据知识产权地方试点工作。2022年9月通过的《浙江省知识产权保护和促进条例》第十六条规定：“省知识产权主管部门应当会同省有关部门依法对经过一定算法加工、具有实用价值和智力成果属性的数据进行保护，探索建立数据相关知识产权保护和运用

^① 高志宏：《隐私、个人信息、数据三元分治的法理逻辑与优化路径》，法制与社会发展，2022, 28(02):207-224.

^② 肖冬梅,文禹衡：《数据权谱系论纲》，湘潭大学学报（哲学社会科学版），2015, 39(06):69-75.

^③ [英]哈耶克：《致命的自负》，冯克利等译，北京：中国社会科学出版社，2000, 11.

制度。”深圳市标准技术研究院贯彻落实《数据知识产权登记试点工作方案》建立了配套制度规范，为数据处理者提供“数据哈希值存证—登记申请—材料审核—信息公示—证书发放”全流程服务。

财产权可以划分为物权、债权和知识产权。其中，知识产权作为一种无形财产权，具有“客体共享、利益排他”的特殊属性，即不必通过配置客体再间接地配置客体上的利益，而是直接对客体上的利益进行排他性配置。而数据产权也是无形的，且具有上述特殊属性，法律属性上与知识产权最为接近。吴汉东（2022）认为，数据知识产权属于知识产权领域的特别权利，一方面，数据知识产权应具有信息产权的基本属性，知识产权法就是信息保护法，传统知识产权保护的是作为知识的信息，数据知识产权保护的是作为过程的信息与作为事实的信息；另一方面，数据知识产权是不具备民法典第123条规定的专有属性的特别权利，其权能应参照知识产权的使用权能与禁止权能，并进行相应限制，即其应为不完整的控制权、有条件的使用权与非绝对的排他权。^①

在数据知识产权的制度构成上，吴汉东（2022）认为，数据知识产权应采取“数据制作者权—数据使用者权”的二元结构。一方面，数据制作者权属于数据财产权，数据库制作者权属于著作权；另一方面，数据使用者权的内涵外延广

^① “我国推动数据知识产权规则构建，多地开展试点工作”法制日报，2022.11.25.
<https://news.cctv.com/2022/11/25/ARTIS80p02wpAFresbSLqmQt221125.shtml>.

于数据访问权，同时包含数据访问、获取与使用的权能。但在赋予范围更广的权能同时，需注意合理使用的“宽进宽出”，尤其是为了数据产业发展，可以赋予第三方数据使用者在满足 FRAND 原则（即公平、合理和无歧视性的专利许可原则）下可获得默示许可，或是可通过付费强制许可的方式对数据进行访问与使用。^①

1.1.3 数据要素与数据保护机制研究

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。我国《数据安全法》率先在法律层面提出了“数据要素”的制度内涵，其中第七条规定，“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。”

王春晖（2022）认为，我国数据的法定含义是“以电子或其他方式对信息的记录”。在非结构化数据规模呈指数级增长的大趋势下，不可能出现组织或个人拥有数据所有权的命题。由此，数据产权制度最大的特征是“去所有权化”。要深刻理解《数据安全法》确立的数据的内涵和外延，数据是数据处理者在运营中以电子或其他方式“收集”和“产生”的对信息的记录，因此，不存在所有权（占有、使用、收益、

^① 光明网：为全球知识产权治理体系提供数据产权制度产品. 2022. 11. 25.
<https://m.gmw.cn/baijia/2022-11/25/36187654.html>.

处置) 问题。

现代数据产权的核心要点是推动数据持有权、使用权等相关权利的有序分离, 确保数据在安全治理基础上充分利用和交易流通。至于数据的分配制度, 应当由数据要素市场评价其贡献、按照贡献决定报酬。^①

此外, 王春晖 (2022) 还指出目前的数据要素市场尚在培育期, 缺乏基础性制度, 因此, 这一时期的重点任务应该是进行数据基础性制度性建设, 一是要优化数据要素布局结构、保障各社会主体平等使用数据、促进数据合规高效流通使用; 二是一定要以赋能实体经济为重点, 要改善和优化数据要素市场的发展环境, 特别是要提升安全保障能力为支撑, 坚决破除阻碍数据要素供给、流通、使用的体制机制障碍。

同时, 要对接和引领国际高标准数字规则。^②

在数据保护方面, 学者们认识到“数据”不同于传统的物, 具有复合价值。传统的权利保护理论会阻碍数据的发展和流通, 因此需要构建新型的数据保护理论。如梅夏英 (2019) 认为“数据”是新型的法律对象, 具有互惠分享的特征。因此在对数据进行保护时应转换思维模式, 建立“分享—控制”的理论结构。^③高富平 (2018) 主张个人信息具有社会性、公共性的特征, 个人信息不仅有个人利益的面向, 还有他人、

^① 王春晖: 现代数据产权的特征是“去所有权化”, 工业交流馆, 2022.8.2. <https://www.sohu.com/a/573666237-121124375>.

^② 王春晖: 构建数据基础制度需确立现代数据产权制度, 人民邮电报, 2022.6.23. https://www.cnii.com.cn/rmydb/202206/t20220623_391185.html.

^③ 梅夏英:《在分享和控制之间 数据保护的私法局限和公共秩序构建》, 中外法学, 2019, 31(04):845-870.

社会的利益面向。主张建立平衡个人利益和社会利益的个人信息保护制度。^①周汉华（2018）认为在大数据时代，由于数据本身的特性，信息控制者有很强的利用激励而缺乏同等程度的保护激励。如果立法缺乏科学性，只是简单施加各种强烈性外部要求，忽视信息控制者内在激励机制设计，就不能消除失衡根源。只有外部要求与内生激励相容，才能实现大数据利用与个人信息保护协调发展。^②

对于数据保护的路径研究多是从技术层面进行切入。李伦（2019）提倡运用区块链技术、算法治理等数字化的规制方式与法律的规制路径相结合，以更好地保护数字社会中的数据权利。例如区块链、分布式网络、密码学账户等技术改变了传统的交易模式，分布式账本是建立在共识算法的基础上以第三方记录全信息数据流的新型账本模式。^③数据库、云计算等导致了数据的垄断，区块链是共享、去中心化、开放的革命性新技术，大数据技术和区块链技术的结合将为数据权利保护与数据自由流通的权益平衡提供解决思路。^④大数据面临着数据孤单、信息壁垒等问题，区块链技术具有可追溯且不可篡改的特征，区块链技术的使用可以建立一个记录时间先后、保证数据安全、去中心化的数据库，能够使得

^① 高富平：《个人信息保护：从个人控制到社会控制》，法学研究，2018, 40(03):84-101.

^② 周汉华.探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向[J].法学研究, 2018, 40(02):3-23.

^③ 李伦：《数据伦理与算法伦理》，科学出版社，2019.

^④ Sartor G, Rotolo A. <AI and Law>, *Netherlands: Springer*, 2013.

用户完成交易平台的数据确权。^①大数据、算法、人工智能等技术在给人们生活带来便利的同时也带来了新的挑战，社会资源的不公平再分配、定向广告推送、行为歧视等都是由“算法经济”所主导，各国需要重新审视反垄断机构的执法工具，以应对新型的市场垄断保护市场竞争。^②

综上所述，目前国内几种主流的数据产权说各有利弊。首先，我国大多将数据权定位在隐私权、财产权以及知识产权之间，这侧面反映了数据权属的不明确，这对法律政策的出台形成了障碍。其次，以人格隐私权、财产权、知识产权为逻辑起点的数据权属定位，无法为数据权以及个人信息权提供完善的保护路径。正如学者指出，大数据技术下的人数据信息具有数量大、价值密度低、智能处理以及信息获得与其使用结果之间相关性弱等特征。这些特征使得个人无法以私权为制度工具对个人数据信息的产生、存储、转移和使用进行符合自己意志的控制。^③最后，以财产权说、知识产权说为逻辑起点的数据权属定位，在大数据运用与交易过程中，数据得以纳入法律调整的方式是作为债权的客体。这也是目前数据在收集、加工、分析、交易环节中主要采取的法律规制方式。这种数据权之债权调整方式仅仅具有主体相对性，而缺乏对世权的绝对保护。^④

^① [美]保罗·维格纳、迈克尔·凯西：《区块链：赋能万物的事实机器》，凯尔译，中信出版社，2018.

^② 井底望天等主编：《区块链与大数据：打造智能经济》，人民邮电出版社，2017.

^③ 吴伟光：《大数据技术下个人数据信息私权保护论批判》，政治与法律，2016, No. 254 (07) :116–132.

^④ 邓刚宏：《大数据权利属性的法律逻辑分析——兼论个人数据权的保护路径》，江海学刊，2018, No. 318 (06) :144–150+255.

此外，现有研究对数据保护的新思路进行了分析和探讨，反映了目前最新、备受关注的学术动态。但与此同时，这些研究主要从社会学、伦理学、政治学、科技学等角度出发对数据保护问题进行研究，从法学角度出发进行数据保护研究的相对不足，且多是较分散的现象问题研究，缺乏体系构建和理论提炼。

第二节 数据产权制度法律法规探索

1.2.1 国家大数据战略

随着第四次工业革命的深入发展，大数据成为驱动新一轮科技创新和信息革命的新引擎，被视为数字经济时代科学、健康、工业、商业等领域的重要战略资源，价值堪比“石油”“黄金”。

近年来，全球数据生产量呈现爆炸式增长。预计在未来五年内，数据将以 21.2% 的复合年增长率（CAGR）增长。中国的数据产量同样呈现出强劲的增长态势（见图 2）。《数字中国发展报告（2021 年）》指出，2017 年—2021 年，我国数据产量从 2.3ZB 增长至 6.6ZB，这一数据产量在 2021 年全球占比 9.9%，仅次于美国（16ZB），位居世界第二。近三年来，我国数据产量每年保持 30% 左右的增速。^①IDC 预测，到 2025 年，中国将拥有全球最大数据圈。^②

^① 国家互联网信息办公室. 数字中国发展报告（2021）[EB/OL]. 2022-08-02.

http://www.cac.gov.cn/2022-08/02/c_1661066515613920.htm

^② IDC. Data Age 2025 [EB/OL]. 2017-04.

<https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf>



图 2 2017—2021 年我国数据产量及全球占比情况

来源：中国信息通信研究院、中国网络空间研究院

我国大数据产业发展态势好、动力足。根据中国信息通信研究院 2023 年 1 月发布的《大数据白皮书（2022 年）》，2021 年我国大数据产业规模高速增长，增加到 1.3 万亿元，复合增长率超过 30%。大数据产业生态持续优化，2021 年我国大数据市场主体总量超 18 万家，一批大数据龙头企业快速崛起，初步形成了大企业引领、中小企业协同、创新企业不断涌现的发展格局。市场前景广受认可，我国大数据领域投融资金额多年来总体呈现上升趋势，2021 年大数据相关企业获投资总金额超过 800 亿元，再创历史新高。^①

当前大数据主要应用于医疗、通信、零售等行业，因为这些行业需要处理大量顾客和用户的数据。在未来，随着人工智能、VR 等技术更多地为大众所使用，相关行业也会随之产生大量用户数据处理的需求。大数据的巨大发展潜力引起

^① 光明网. 白皮书：中国大数据产业规模高速增长 [EB/OL]. 2013-01-06.
<https://m.gmw.cn/baijia/2023-01/06/36283111.html>

了全球各界的广泛关注，围绕大数据布局国家战略已成全球趋势。2012年3月，美国奥巴马政府投资超2亿美元，正式启动“大数据研究和发展计划（Big Data Research and Development Initiative）”，率先将大数据上升为国家战略，被认为是继1993年美国宣布“信息高速公路”计划后的又一次重大科技发展部署。^①此后，澳大利亚、英国、法国、韩国等国家纷纷出台大数据战略，试图抢先占领大数据发展先机和竞争优势。

大数据也引起了国际组织的高度重视，成为近年来国际讨论的核心话题之一。2012年5月，联合国“全球脉冲计划”（Global Pulse）发布《大数据开发：机遇与挑战》（Big Data for Development: Challenges & Opportunities）报告，阐述了大数据带来的历史机遇、主要挑战和未来应用。^②经合组织、世界银行、欧盟等国际组织也纷纷加速大数据研究并发布系列指导性文件，为世界各国特别是发展中国家正确运用大数据提出了策略建议。

中国正视大数据时代潮流，主动抓住发展机遇，着力规划大数据战略（见表1）。2015年8月，国务院下发《促进大数据发展行动纲要》，从国家战略的高度突出强调了大数据资源的战略地位，明确提出了建设“数据强国”的目标，系统部署了大数据发展工作。《促进大数据发展行动纲要》

^① 李国杰,程学旗:《大数据研究:未来科技及经济社会发展的重大战略领域——大数据的研究现状与科学思考》,中国科学院院刊,2012,27(06):647-657.

^② 刘叶婷,唐斯斯:《大数据对政府治理的影响及挑战》.电子政务,2014(06):20-29.

设定了三方面的主要任务：一要加快政府数据开放共享，推动资源整合，提升治理能力；二要推动产业创新发展，培育新兴业态，助力经济转型；三要强化安全保障，提高管理水平，促进健康发展。^①

表 1 中国国家大数据战略部分文件

时间	文件	着力点
2015 年 8 月	《促进大数据发展行动纲要》	明确“数据强国”目标，系统部署大数据发展工作
2015 年 10 月	《中国共产党第十八届中央委员会第五次全体会议公报》	首提“国家大数据战略”，大数据战略上升为国家意志
2016 年 3 月	《中华人民共和国国民经济和社会发展第十三个五年（2016—2020 年）规划纲要》	明确数据的基础性战略资源地位，制定大数据发展促进计划
2016 年 12 月	《大数据产业发展规划（2016—2020 年）》	部署大数据产业发展工作，推动大数据产业持续健康发展
2017 年 5 月	《政务信息系统整合共享实施方案》	推动政务信息系统整合共享，最大程度利企便民
2021 年 11 月	《“十四五”大数据产业发展规划》	激发数据要素价值潜能，夯实产业发展基础

2015 年 10 月，党的十八届五中全会强调要“实施网络强国战略，实施‘互联网+’行动计划，发展分享经济，实施国家大数据战略。”^②这是我国首次公开提出“国家大数据战略”，表明中国已将大数据视作战略资源并上升为国家战略，期望运用大数据推动经济发展、完善社会治理、提升政府服务和监管能力。

2016 年 3 月出台的《中华人民共和国国民经济和社会发展第十三个五年（2016—2020 年）规划纲要》将“实施国家大数据战略”单列一章，明确提出把大数据作为基础性战略资

^① 中国政府网. 国务院印发《促进大数据发展行动纲要》

[EB/OL]. 2015-09-05. http://www.gov.cn/xinwen/2015-09/05/content_2925284.htm

^② 共产党员网. 中国共产党第十八届中央委员会第五次全体会议公报

[EB/OL]. 2015-10-29. <https://news.12371.cn/2015/10/29/ARTI1446118588896178.shtml>

源，全面实施促进大数据发展行动，加快推动数据资源共享开放和开发利用，助力产业转型升级和社会治理创新。“十三五”规划围绕加快政府数据开放共享和促进大数据产业健康发展两方面制定了大数据发展促进计划，作为实施国家大数据战略的指导性文件，其对各地贯彻党和国家的大数据战略部署、制定大数据发展相关政策具有重要的指导意义。^①

2016年12月，工业和信息化部正式印发了《大数据产业发展规划（2016—2020年）》，明确了大数据产业发展的指导思想、发展原则、发展目标、重点任务和重大工程、保障措施，全面部署了“十三五”时期大数据产业发展工作，加快从数据大国向数据强国转变，为实现制造强国和网络强国提供强大的产业支撑。^②

在延续“十三五”规划关于大数据产业定义和内涵的基础上，2021年11月，工业和信息化部发布了《“十四五”大数据产业发展规划》，进一步强调了数据要素价值，旨在充分激发数据要素价值潜能，夯实产业发展基础，构建稳定高效产业链，统筹发展和安全，培育自主可控和开放合作的产业生态，打造数字经济发展新优势，为建设制造强国、网络强国、数字中国提供有力支撑。该规划明确了大数据产业发展的“3个6”，即6项重点任务、6个专项行动和6项保

^① 中国政府网. 中华人民共和国国民经济和社会发展第十三个五年规划纲要[EB/OL]. 2016-03-17. http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm?url_type=39&object_type=webpage&pos=1

^② 中华人民共和国工业和信息化部.《大数据产业发展规划(2016-2020年)》正式发布. [EB/OL]. 2017-01-17. https://www.miit.gov.cn/jgsj/xxjsfzs/rjcy/art/2020/art_268542a20cad4f0fa090af480599d019.html

障措施。其中，6项重点任务包括：一是加快培育数据要素市场；二是发挥大数据特性优势；三是夯实产业发展基础；四是构建稳定高效产业链；五是打造繁荣有序产业生态；六是筑牢数据安全保障防线。^①

此外，在国家大数据战略的驱动下，政府数据也加快了共享开放的步伐。为更好推动政务信息系统整合共享，从全局上和根本上解决长期以来困扰我国政务信息化建设的“各自为政、条块分割、烟囱林立、信息孤岛”问题。2017年5月，国务院印发《政务信息系统整合共享实施方案》，围绕政府治理和公共服务的迫切需要，以最大程度利企便民，让企业和群众少跑腿、好办事、不添堵为目标，提出了加快推进政务信息系统整合共享、促进国务院部门和地方政府信息系统互联互通的重点任务和实施路径。^②

党的十八大以来，我国针对大数据的发展目标、发展方向和重要任务等方面制定了一系列的战略部署和规划，已经形成了较为成熟的大数据战略体系，具有深刻的时代价值。实践证明，大数据战略给我国的政治、经济、文化、教育和科研等方面带来了重大而深刻的影响，全方位推动了我国的社会发展。如今，大数据技术已成为大国博弈的关键领域，面对新的挑战与机遇，中国应牢牢掌握大数据发展主动权，

^① 中国政府网.《“十四五”大数据产业发展规划》解读[EB/OL].2021-12-01.

http://www.gov.cn/zhengce/2021-12/01/content_5655197.htm

^② 新华网.突出重点精准发 把握关键务求实效 全面推进政务信息系统整合共享[EB/OL].2017-06-02.

http://www.xinhuanet.com/politics/2017-06/02/c_1121076349.htm

坚持“数据强国”战略不动摇。

1.2.2 数据正式成为生产要素

随着信息技术呈指数式快速发展，新一代信息技术的革新推进了数字技术在社会场域的深化，也加快了“数字中国”“智慧城市”等建设，人类以“数字化生存”的方式栖息在数字社会。其中，数据作为人类数字化生存的产品，正成为新型生产要素，改变原有政治、经济、文化的存在和实践逻辑，催动新经济模式和制度结构的诞生。

2019年10月31日，中共第十九届四中全会通过《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》，提出“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。”^①增列“数据”为一种生产要素、将其与传统生产要素相对等是历史发展的必然选择，数据从“作为数据的数据”到“作为要素的数据”，反映的正是数据在当下社会带来的生产方式变革。^②

此后，中央高度关切数据要素市场的培育，出台《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》，明确指出要“推进政府数据开放共享”“提升社

^① 中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定 [EB/OL]. 中华人民共和国中央人民政府网

[2019-11-05]. http://www.gov.cn/zhengce/2019-11/05/content_5449023.htm.

^② 王文臣, 马梦雪: 《论大数据作为生产要素的资本化及其双重影响》, 上海财经大学学报, 2022, 24 (06): 108-122.

会数据资源价值”和“加强数据资源整合和安全保护”。^①在《中共中央 国务院关于加快建设全国统一大市场的意见》中同样强调要“加快培育数据要素市场”^②，为数据的进一步开放共享提供政策保障。2022年12月，“数据二十条”提出“建立合规高效、场内外结合的数据要素流通和交易制度”“建立体现效率、促进公平的数据要素收益分配制度”“建立安全可控、弹性包容的数据要素治理制度”等，^③从交易、分配、治理等面向对数据要素的社会潜能做出政策指引。2023年2月，中共中央、国务院印发了《数字中国建设整体布局规划》，明确数字中国建设按照“2522”的整体框架进行布局，即夯实数字基础设施和数据资源体系“两大基础”，推进数字技术与经济、政治、文化、社会、生态文明建设“五位一体”深度融合，强化数字技术创新体系和数字安全屏障“两大能力”，优化数字化发展国内国际“两个环境”。

2023年3月，国家数据局正式获批成立，解决“九龙治水”难题，从国家层面协调统筹，消除“数据孤岛”和“数据烟囱”，打通数据壁垒，全国下“一盘棋”。

但数据作为生产要素，从政法角度看仍面临诸如数据确

^① 中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见[EB/OL]. 中华人民共和国中央人民政府网[2020-04-09]. http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm.

^② 中共中央 国务院关于加快建设全国统一大市场的意见[EB/OL]. 中华人民共和国中央人民政府网[2022-04-10]. http://www.gov.cn/xinwen/2022-04/10/content_5684385.htm.

^③ 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[EB/OL]. 中华人民共和国中央人民政府网[2022-12-19]. http://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

权等问题，明确数据的使用权、所有权、收益权等是创设健康数据要素市场的要义。首先，在信息科学角度来看，数据是描述事物的符号记录，^①但若从资产权益角度出发，数据则是一种隐形资产，^②数据拥有者可以挖掘“推测数据（inferred data）”，^③从而获取更多信息甚至盈利。数据在经由生产、收集、流转等环节进入社会生产生活，便实现了价值转化成为新型生产要素，^④期间历经数据交易、数据交换等商业手段和原始数据生产者、平台技术方、第三方服务公司等多个相关主体，数据的使用权、所有权、收益权等归属之争各执一词。因此，明确数据的权责归属与界限范围是加快推动数据要素市场和谐稳定的首要问题。

此外，数据作为数字经济中的关键变量，也已成为基础性资源进入社会应用场域，携实体经济共同推动经济高质量发展。2022年1月12日，国务院正式发布《“十四五”数字经济发展规划》，指出“数据要素是数字经济深化发展的核心引擎”，提出到2025年“数据要素市场体系初步建立”“数字经济治理体系更加完善”等一系列发展目标，^⑤这也是对未来数字经济发展做出的战略规划。

微观来看，在产业发展中，百度、阿里、腾讯等数字平

^① 王珊，萨师煊：《数据库系统概论》，.北京：高等教育出版社，2006:3-4.

^② 徐全华.试论：《字资产的会计确认、计量与报告》，广西经济管理干部学院学报，2002（03）：66-68.

^③ 吴飞，傅正科：《大数据与“被遗忘权”》，浙江大学学报（人文社会科学版），2015（02）：68-78.

^④ 潘家栋,肖文：《新型生产要素：数据的生成条件及运行机制研究》，浙江大学学报(人文社会科学版)，2022, 52 (07) :5-15.

^⑤ 国务院关于印发“十四五”数字经济发展规划的通知[EB/OL].中华人民共和国中央人民政府网[2022-04-10]. http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

台的日益基础设施化为数字产业提供生产阵地，推动了数字经济这一新经济形态的发展，在未来发展中需加快与实体经济的合作步伐，推动传统产业的升级和转型。在经济治理方面，用户的信息发布、收集、浏览、反馈等数字化生产和消费行为都是平台化实践，在数据成为资产进入市场时需要与平台规则、市场规则相适应、协商、抗衡，因此，要加快数字经济市场体系的建设和数字经济治理能力的提升，形成数字经济高质量发展的有序格局。

1.2.3 数据产权相关法规

随着“数据作为生产要素”的正式提出，“数据二十条”对现下数据产权制度高度重视，提出要“逐步形成具有中国特色的数据产权制度体系”，将公共数据、企业数据、个人数据进行分类分级确权，推动数据资源持有权、数据加工使用权、数据产品经营权等数据产权的结构性分置，保障数据要素相关方的利益与数据要素市场的有序流通。^①在数据要素深化经济政治体制变革的过程中，政府更要把握制度建设里对数据产权的监管作用和市场经济里作为“有形的手”的调控作用，同时发挥地方作用加强区域执法，构建中央与地方共同建设、协同治理的模式。

我国自 1994 年便开始探索信息数据安全相关法制建设，并随着时代发展历时性对内容进行修订。（见表 2）在近年

^① 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[EB/OL]. 中华人民共和国中央人民政府网[2022-12-19]. http://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

的立法中，对个人数据处理走向的公开、透明偏向越来越明显，且强调个人数据处理需经得本人同意或告知，这与美国2019年1月通过的《开放政府数据法》明确数据开放共享义务遥相呼应，也与欧盟2018年出台的《通用数据保护条例》中提出的“被遗忘权”有异曲同工之妙。数据的价值属性和法律属性被不断开发，但确权问题仍是法律层面的重点和难点，国内也亟待发行真正意义上的数据产权相关法律条文。

表 2 国内信息数据相关法律法规

相关法律法规	实施年份	侧重点
中华人民共和国计算机信息系统安全保护条例	1994	保护计算机信息系统的安全，促进计算机的应用和发展。
计算机信息网络国际联网安全保护管理办法	1997	加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定。
中国互联网络域名注册暂行管理办法	1997	保证和促进我国互联网络的健康发展，加强我国互联网络域名系统的管理。
计算机信息系统国际联网保密管理规定	2000	加强计算机信息系统国际联网的保密管理，确保国家秘密的安全。
互联网电子公告服务管理规定	2000	加强对互联网电子公告服务的管理，规范电子公告信息发布行为。
互联网信息服务管理办法	2000	规范互联网信息服务活动，促进互联网信息服务健康有序发展。
软件产品管理办法	2000	加强软件产品管理，促进我国软件产业的发展。
计算机软件保护条例	2001	保护计算机软件著作权人的权益，调整计算机软件在开发、传播和使用中发生的利益关系。
计算机软件著作权登记办法	2002	鼓励软件登记，并对登记的软件予以重点保护。
电信网码号资源管理办法	2003	促进电信事业的发展，保障公平竞争，有效地利用电信资源。
中国互联网络域名管理办法	2004	规范互联网络域名服务，保护用户合法权益，保障互联网络域名系统安全、可靠运行。
中华人民共和国电子签名法	2005	规范电子签名行为，确立电子签名的法律效力。
互联网著作权行政保护办法	2005	加强互联网信息服务活动中信息网络传播权的行政保护。
互联网电子邮件服务管理办法	2006	规范互联网电子邮件服务，保障互联网电子

		邮件服务使用者的合法权利。
信息网络传播权保护条例	2006	保护著作权人、表演者、录音录像制作者的信息网络传播权。
信息安全等级保护管理办法	2007	加强信息安全等级保护，规范信息安全等级保护管理，提高信息安全保障能力和水平。
电子认证服务管理办法	2009	规范电子认证服务行为，对电子认证服务提供者实施监督管理。
国家网络空间安全战略	2016	阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作。
中华人民共和国网络安全法	2017	保障网络安全，维护网络空间主权和国家安全、社会公共利益。
互联网新闻信息服务管理规定	2017	规范互联网新闻信息服务，满足公众对互联网新闻信息的需求。
个人信息出境安全评估办法（征求意见稿）	2019	保障个人信息安全，维护网络空间主权、国家安全、社会公共利益。
数据安全管理办法（征求意见稿）	2019	保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全。
互联网个人信息安全保护指南	2019	有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益。
信息安全技术个人信息安全规范	2020	规范个人信息在收集、存储、使用、共享、转让与公开披露等信息处理环节中的相关行为。
中华人民共和国数据安全法	2021	规范数据处理活动，保障数据安全，促进数据开发利用。
中华人民共和国个人信息保护法	2021	保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用。

除上述中央层面出台的《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等之外，地方积极响应，颁发数据管理条例，如贵州省作为国内第一个省级层面对大数据进行立法的省份，先后出台《贵州省大数据安全保障条例》《贵州省大数据发展应用促进条例》，保障大数据治理安全。深圳市发布了国内数据领域首部基础性、综合性立法的《深圳经济特区数据条例》，强调“坚持个人信息保护与促进数字经济发展并重”^①。上海市也依托《中华人民共和

^① 重磅！《深圳经济特区数据条例》正式公布[EB/OL]. 深圳市政务服务数据管理局 [2021-01-07]. http://www.sz.gov.cn/szzsj/gkmlpt/content/8/8935/post_8935483.html#19236.

国数据安全法》等出台了《上海市数据条例》，以“推进数据权益保护、数据流通利用、数据安全管理”^①。据不完全统计，此外还有一些省份出台区域性数据管理相关规定（见表3），江西省、河南省也于2022年发布地方草案试行数据条例。可以看到，现下虽未发行切实以数据产权为主题的法律法规，但相关政策正日趋完善，中央与地方也正联合并进，加快完善数据要素市场培育与发展。

表3 区域数据管理条例

地区	条例名称	内容要点	数据产权相关表述
北京市	北京市公共数据管理办法	旨在规范公共数据的共享，推动公共数据的开放，提升政府治理能力和公共服务水平。办法明确了公共数据的定义范围。	/
上海市	上海市数据条例	旨在规范数据处理活动，促进数据依法有序自由流动，保障数据安全，加快数据要素市场培育，推动数字经济更好地服务和融入新发展格局。包括总则、数据权益保障、公共数据、数据要素市场、数据资源开发和应用、浦东新区数据改革、长三角区域数据合作、数据安全、法律责任和附则，是国内首部省级人大制定的数据条例。	上海市依法保护自然人、法人和非法人组织在使用、加工等数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益。
浙江省	浙江省公共数据条例	旨在加强公共数据管理，促进公共数据应用创新，保障数字化改革，深化数字浙江建设，推进省域治理体系和治理能力现代化。从明确公共数据定义范围、平台建设规范、收集归集规则、共享开放机制、授权运营制度、安全管理规范等方面对公共数据发展和管理作出具体规定。	浙江省公共数据主管部门应当会同省网信、公安、国家安全、财政等部门制定公共数据授权运营具体办法，明确授权方式、授权运营单位的安全条件和运营行为规范等内容，报省人民政府批准后实施。
广东省	广东省公	旨在规范公共数据采集、使用、	单位和个人依法开发利用公共

^① 上海市数据条例[EB/OL]. 上海市人民政府[2021-11-29]. <https://www.shanghai.gov.cn/nw12344/20211129/a1a38c3dfe8b4f8f8fcba5e79fbe9251.html>.

	共数据管理办法	<p>管理, 保障公共数据安全, 促进公共数据共享、开放和利用, 释放公共数据价值, 提升政府治理能力和公共服务水平。有诸多制度创新, 包括国内首次明确将公共服务供给方数据纳入公共数据范畴、首次在省级立法层面真正落实“一数一源”、首次明确数据交易标的等。</p>	<p>数据所获得的财产权益受法律保护; 数据主体有权依法向公共管理和服务机构申请查阅、复制本单位或者本人的数据, 有权依法提出异议并请求及时采取更正、删除等必要措施。</p>
	深圳经济特区数据条例	<p>旨在规范数据处理活动, 促进数据作为生产要素开放流动和开发利用, 加快建设数字经济、数字社会、数字政府。内容涵盖了个人信息数据、公共数据、数据市场、数据安全等方面, 是国内数据领域首部基础性、综合性立法, 率先明确提出“数据权益”。</p>	<p>自然人对个人数据享有法律、行政法规及本条例规定的人格权益; 处理个人数据应当充分尊重和保障自然人与个人数据相关的各项合法权益; 自然人有权撤回部分或者全部其处理个人数据的同意。</p>
贵州省	贵州省大数据安全保障条例	<p>旨在保障大数据安全和个人信息安全, 明确大数据安全责任, 促进大数据发展应用。对大数据安全责任人的安全责任、监督管理、法律责任等进行了明确, 体现了发展与安全并重, 以安全保发展、以发展促安全的理念。</p>	<p>任何单位和个人都有维护大数据安全的义务, 不得从事危害大数据安全的活动, 不得利用大数据从事危害国家安全以及损害国家利益、社会公共利益和他人合法权益的活动。</p>
	贵州省大数据发展应用促进条例	<p>旨在运用大数据促进经济发展、完善社会治理、提升政府服务管理能力、服务改善民生, 培育壮大战略性新兴产业。对数据采集、数据共享开发、数据权属、数据交易、数据安全以及“云上贵州”等基本问题作出了宣示性、原则性、概括性和指引性规定, 是全国首部大数据地方性法规。</p>	<p>数据共享开放, 应当维护国家安全和社会公共安全, 保守国家秘密、商业秘密, 保护个人隐私, 保护数据权益人的合法权益。任何单位和个人不得利用数据共享开放从事违法犯罪活动。</p>
天津市	天津市促进大数据发展应用条例	<p>旨在发挥大数据促进经济发展、服务改善民生、完善社会治理的作用, 培育壮大战略性新兴产业, 加快构建数字经济和智慧城市。包括总则、政务数据、社会数据、开发利用、保障措施、数据安全、法律责任、附则。</p>	<p>数据资源交易、交换应当遵守法律法规规定和社会公德, 不得损害国家利益、社会公共利益和他人合法权益。</p>
海南省	海南省大数据开发利用条例	<p>旨在推动大数据的开发利用, 发挥大数据提升经济发展、社会治理和改善民生的作用, 促进大数据产业的发展, 培育壮大数字经济。</p>	<p>大数据生产经营单位不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由, 以默认授权、功能捆绑</p>

		济，服务中国（海南）自由贸易试验区和中国特色自由贸易港建设。从总则、大数据开发与共享、大数据开发与产业促进、数据安全与保护、法律责任等方面做出规定，覆盖了大数据采集、汇聚、存储、管理、开放共享等各个环节。	等形式强迫、误导被采集人同意其采集个人信息；依法获取的各类数据经处理无法识别特定数据提供者且不能复原的，或经过特定数据提供者明确授权的，可以交易、交换或者以其他方式开发利用。
山西省	山西省大数据发展应用促进条例	旨在发挥数据生产要素的作用和培育壮大新兴产业，推动经济社会各领域的数字化、网络化、智能化发展及促进高质量转型发展。从明确政府管理职责、制定促进发展优惠政策、提供服务保障措施等方面，推动大数据产业政策的法治化，为大数据健康发展创造良好的法治环境。	依法获取的各类数据经过处理无法识别特定个人且不能复原的，或者经过特定数据提供者明确授权的，可以交易、交换或者以其他方式开发利用。
吉林省	吉林省促进大数据发展应用条例	旨在促进大数据发展应用，规范数据处理活动，保护公民、法人和其他组织的合法权益，推进数字吉林建设。对数据采集、归集、整合、共享、开放做了全过程规范。	公共数据共享开放，应当维护国家安全和公共安全，保守国家秘密、商业秘密，保护个人隐私，保护数据权益人的合法权益。
安徽省	安徽省大数据发展条例	旨在发挥数据要素的作用，发展数字经济，创新社会治理，保障数据安全，建设数字江淮，加快数字化发展。从数据资源的归集整合、开发应用、安全管理和促进大数据发展的相关措施等方面进行规范。	依法获取的各类数据经过处理无法识别特定个人且不能复原的，或者经过特定数据提供者明确授权的，可以交易、交换或者以其他方式开发利用；安徽省人民政府数据资源主管部门应当会同有关部门统筹大数据交易服务机构的设立，搭建数据要素交易平台，建立数据产权交易机制，推动建立行业自律机制。
山东省	山东省大数据发展促进条例	旨在全面实施国家大数据战略，运用大数据推动经济发展、完善社会治理、提升政府服务和管理能力，加快数字强省建设。包括总则、基础设施、数据资源、发展应用、安全保护、促进措施、法律责任和附则。	自然人、法人和其他组织收集数据不得损害被收集人的合法权益；利用合法获取的数据资源开发的数据产品和服务可以交易，有关财产权益依法受保护。
福建省	福建省大数据发展条例	旨在促进大数据有序健康发展，发挥数据生产要素作用，推进数字福建建设。从数据资源、基础	数据交易、交换应当遵守法律法规和社会公德，不得损害国家利益、社会公共利益和他人

		设施、发展应用、数据安全、保障措施和法律责任等方面对大数据的发展作出了具体规定。	合法权益。
	厦门经济特区数据条例	旨在规范数据处理活动，保障数据安全，培育数据要素市场，促进数据有序流动和开发利用，推动数字政府、数字社会、数字经济建设与发展。聚焦数据流通利用、数据安全管理、数据权益保护三大环节。	自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规规定的财产权益。但是，不得危害国家安全和社会公共利益，不得损害他人的合法权益；探索数据分类分级确权授权使用，推动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。
重庆市	重庆市数据条例	旨在规范数据处理，保障数据安全，保护个人、组织的合法权益，培育数据要素市场，促进数据应用，推动数字经济发展。对全市数据领域工作统筹分工机制、数据处理规则和数据安全责任、市公共数据管理制度、数据要素市场框架制度加以明确，并提出了“数据赋能发展”系列举措。	建立公共数据授权运营机制。授权运营单位不得向第三方提供授权运营的公共数据，但是可以对授权运营的公共数据进行加工形成数据产品和服务，并依法获取收益。
黑龙江省	黑龙江省促进大数据发展应用条例	旨在发挥数据要素作用，加快大数据发展应用，推动数字经济发展，创新社会治理模式，保障数据安全。有针对性地对公共数据发展规划、平台建设、目录管理、数据标准、采集汇聚、质量管控、共享开放等作出规定。	鼓励探索建立数据权属登记制度，依法保护自然人、法人和非法人组织合法处理数据享有的财产权益，推动数据交易活动的开展。
辽宁省	辽宁省大数据发展条例	旨在充分挖掘数据资源，发挥数据效用，加快大数据发展，建设数字辽宁、智造强省。从培育壮大大数据要素市场、突出工业大数据特色、夯实新型基础设施底座、全面保障数据安全等方面进行了制度设计。	辽宁省、市人民政府应当按照建立全国统一的产权保护、市场准入和公平竞争等制度要求，加快培育数据要素市场，保护市场主体合法财产权益；依法保护数据处理市场主体在使用、加工等数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益。
四川省	四川省数据条例	旨在保障数据安全，促进数据依法有序流通和应用，推动以数据为关键要素的数字经济发展。在数据资源、数据流通、数据应用、	自然人、法人和非法人组织在使用、加工等数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益。

		数据安全、区域合作等方面做出具体部署。	关数据创新活动取得的合法权益受法律保护。
广西壮族自治区	广西壮族自治区大数据发展条例	旨在规范数据市场，保障数据安全，发挥数据要素作用，推动大数据发展应用，促进数字经济和实体经济深度融合，提升治理能力和水平，加快数字广西建设。对广西大数据发展的基础设施、数据资源、数据市场、发展应用、数据安全、法律责任等方面进行了规范。	自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、法规规定的财产权益，依法自主使用、处分；县级以上人民政府可以探索建立数据权属登记制度，依法保护自然人、法人和非法人组织合法处理数据享有的财产权益，推动数据交易活动开展。
江西省	江西省数据应用条例（草案）	旨在规范数据处理活动，促进数据应用，推动数字经济发展。包括总则、数据资源、数据要素市场、发展应用、促进措施、安全保护、法律责任和附则。	市场主体依法在使用、加工等数据处理活动中形成的法定或者约定的财产权益受法律保护，并可以依法交易。法律另有规定或者当事人另有约定的除外。
河南省	河南省数据条例（草案）	旨在规范数据处理活动，保障数据安全，培育数据要素市场，促进数据开发利用，服务经济社会发展和数字强省建设。对公共数据、非公共数据、数据开发利用、数据安全等内容作了详细规定。	自然人、法人和非法人组织依法对其合法收集的非公共数据享有权益，可依法开展数据利用、加工和交易；自然人、法人和非法人组织处理非公共数据，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任。
陕西省	陕西省大数据条例	旨在加强数据资源管理，规范数据处理活动，保障数据安全，推动大数据在工业领域的应用，加快数字陕西建设。包括总则、基础设施、数据资源、开发应用、产业发展、安全保障、法律责任、附则等内容。	数据提供者应当加强对共享数据的分类分级管理，落实数据收集、汇聚、整合、提供等环节安全责任。数据使用者要加强对共享数据授权管理，强化涉密、重要敏感等数据使用监管，按需申请共享数据，严格控制共享范围。

1.2.4 数据安全法

在国外，美国曾针对谷歌、苹果、脸书和亚马逊四家公司开展《数字市场竞争调查》，欧盟委员会曾向谷歌开出巨额罚单指控其通过滥用搜索引擎主导地位而展开广告服务，

商业巨头的垄断主导地位意味着数据话语权和商业主动性。在国内，百度、腾讯、阿里等大型互联网企业凭借用户优势、资源优势、技术优势等掌握了大量用户数据，上海数据交易所、贵阳大数据交易所、湖南大数据交易所、福建大数据交易所等在全国各地兴起的数据交易所反映着数据要素市场的建设与流通现状，加之数据开放平台、数据软件开发、数据咨询、数据征信评价、数据营销等商业模式迭出，数据行业亟待发布行业标准与执行法规。

近年来，国家愈加重视数据信息安全，除上述数据产权相关法规外，还出台了《中华人民共和国个人信息保护法》规范个人信息使用走向，颁布《中华人民共和国网络安全法》维护网络空间环境安全与良好网络治理体系，执行《信息安全技术个人信息安全规范》明确了第三方接入管理、用户画像使用限制、个性化展示的使用等。

其中，2021 年出台的《中华人民共和国数据安全法》是我国首部关于数据安全的法律，该法首次从法律意义上明确了“数据”的概念，即“本法所称数据，是指任何以电子或者其他方式对信息的记录”。此外还提出“促进以数据为关键要素的数字经济发展”^①，这不仅凸显了数据在法律层面上被确定为关键要素的意义，也为深入探索数据产权制度奠定了法律基础。

^① 中华人民共和国数据安全法 [EB/OL]. 中华人民共和国工业和信息化部 [2022-01-29]. https://www.miit.gov.cn/zwgk/zcwj/f1fg/art/2022/art_284b390b84484f10b0e43eeafad0f6d.html.

《中华人民共和国数据安全法》颁发的意义还在于其与《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等在数据安全与发展、数据保护与义务、数据开放与共享等层面形成了衔接、互补与合作^①。因此，地方也会基于上述法律条文制定区域性数据立法。

值得指出的是，《中华人民共和国数据安全法》与另二者的区别在于该法更重视数据处理活动、数据安全保护和数据安全治理体系建设，不仅关切国内各地区、各部门的数据安全规范，还注重参与国际数据安全相关的规则与标准制定，并且强调了数据作为数字经济背景下的生产要素的关键地位，使数据在未来的社会流动与市场流通中有法可依、依法合理。

从宏观来看，栖息在数字时代，数据驱动并影响着国家、社会、市场、企业、公众的多方权益。在美国“棱镜门”事件中，美国国家安全局的电子监控计划关涉苹果、谷歌、微软等多家互联网巨头，通过监控短信邮件、语音通话、视频通话、照片影像等挖掘信息情报。2021年，淘宝近12亿条用户数据被盗，涉及用户ID、淘宝昵称、手机号码等信息。在滴滴被罚事件中，滴滴公司共存在16项违法事实，主要是以不当方式收集信息数据、过度收集信息数据、未对个人信息数据采取相应的加密安全技术措施、未经授权处理个人

^① 曹开研：《数据安全法：新形势下数据风险治理的利器及实施展望》，青年记者，2021, 709(17):70-72.

信息数据等 4 类违法行为^①。诸多案例都反映了数据在现代社会举足轻重的地位，当个人信息数据泄露时，也意味着个人数据安全遭遇威胁、互联网市场秩序产生混乱和国家网络信息数据安全制度受到挑衅。此外，滴滴公司赴美上市一事，虽深化了互联网企业间的跨国合作，却也造成了数据安全管理障碍，衍生了数据跨境流动问题。因此，国家、社会、市场、企业、公众等都需要数据安全相关法律条文的实施保障，在此之下的统一治理才能使数据行业繁荣发展，《中华人民共和国数据安全法》的出台就是我国加快数据治理体系建设迈出的重要一步。

第三节 数据生产力促进生产方式根本变革

生产力决定生产关系，数据生产力的出现和发展必然催生生产关系的系统性变革，从而颠覆人类社会的旧有生产方式。王春晖（2023）指出，数据生产力决定数字化生产关系，其中数据生产力在两者关系中居支配地位、起决定作用的方面。数字化生产关系是人们在数字化生产过程中形成的一种新型社会经济关系，它包括生产、流通、分配、交易、消费过程中形成的各种经济关系，其中数据作为新的生产资料是数字化生产关系中最基本的问题。

张建云指出，数据生产力促进生产方式的根本变革，具体表现在：它使人们之间的深度协作全面化、普遍化；它使

^① 方兴东, 何可, 钟祥铭: 《数据崛起: 互联网发展与治理的范式转变——滴滴事件背后技术演进、社会变革和制度建构的内在逻辑》, 传媒观察, 2022, 466(10):49-59.

生产的直接社会化向纵深发展，并日益把人从直接生产过程中、从重复性的工作中解放出来。^①

1.3.1 数据生产力的提出

数据不仅对人类生产生活产生了深刻影响，而且成为人类生产生活的内在组成部分，是人类社会生产要素和生产力的新形态。2020年7月，数据生产力（Data Production）成为大数据战略重点实验室全国科学技术名词审定委员会研究基地收集审定的第一批108条大数据新词之一，经全国科学技术名词审定委员会批准试用。^②

“数智”化时代，数据作为关键生产要素正在引发新型社会经济形态的变革，带动“数据生产力”的快速发展。作为人类生产力更高层次的延续，数据生产力以数据为基础和核心，建立在“经验型数据”和“理论型数据”发展到“数字化数据”基础之上，标志着人类生产方式依次从“以土地为起点”“以劳动为起点”和“以资本为起点”向“以数据为起点”深入发展。^③

1.3.2 数据生产力的研究现状

有关“数据生产力”这一新兴概念的学术研究目前尚处于起步阶段。近年来，学者们着眼于快速发展的实践，专注于理论范式的建构，在马克思主义理论的指导下围绕数据生

^① 张建云. 大数据技术体系与当代生产力革命[J]. 马克思主义研究, 2021(04):58-68+164.

^② 全国科学技术名词审定委员会. 全国科学技术名词审定委员会大数据新词发布试用[EB/OL]. 2020-07-23. http://www.cnterm.cn/xwtd/tpxw/202007/t20200723_570712.html

^③ 王贊新. 数据生产力: 形成、属性与理论深化[J]. 海南大学学报(人文社会科学版), 2022, 40(05):180-190.

产力的内涵、影响、挑战等基本问题展开了深耕。

基于不同的分析视角，学者们对数据生产力内涵的界定不尽相同，目前尚未形成统一的话语体系。强调数据生产力的数字技术基础，阿里研究院认为数据生产力是在“数据+算力+算法”定义的世界中，知识创造者借助智能工具，基于能源、资源以及数据这一新生产要素，构建的一种认识、适应和改造自然的新能力。^①

立足于马克思生产力学说视角，李海俊指出数据生产力是马克思生产力思想在大数据时代的具体形态，是社会物质生产领域内提高物质生产活动效率的客体力量。^②回归生产力的三个基本要素，即劳动者、劳动资料、劳动对象，李海舰和赵丽将数据生产力定义为知识型劳动者以数字技术为劳动工具，以海量数据为劳动对象对社会进行改造和生产的能力。^③基于数据本身的复杂属性，王贊新强调数据生产力是一种融合多种生产力属性在内的复杂的生产力因素，即既是一种物质生产力，也是一种精神生产力；既是生产力主体的变革，也是生产力客体的变革。^④

数据生产力创造了巨大的物质财富，随之而来的生产关系的重构也带来了诸多风险与挑战，引起了学者们的高度关注。王贊新表示，数字鸿沟与收入分配格局的调整、产业利

^① 中国信息化百人会,阿里研究院.数据生产力崛起:新动能·新治理[M].北京:电子工业出版,2021.

^② 李海俊.数据生产力:主体异化与解放的生产力[J].西北民族大学学报(哲学社会科学版),2021(05):11-19.

^③ 李海舰,赵丽.数据成为生产要素:特征、机制与价值形态演进[J].上海经济研究,2021(08):48-59.

^④ 王贊新.数据生产力:形成、属性与理论深化[J].海南大学学报(人文社会科学版),2022,40(05):180-190.

润分配与劳资关系重构、劳动关系转型与新型劳动关系构建等问题已经成为我们在数字经济条件下必须面对的现实问题。李海俊指出，数据生产力与生产关系在成为新的社会形式时，也正在模糊主体与对象之间的界限，需警惕数据生产力对人的物理世界和精神世界的过度侵犯。^①王春晖表示，“数智”时代需要重构生产力三要素，即具有一定“数智”技术应用技能和生产运营的劳动者、与一定数字与智能技术相结合以及引入生产过程的劳动对象的数字化和智能化应用水平。^②

总体而言，我国数据生产力的理论研究还处于初步发展阶段，尽管已经取得了一定的理论成果，但相较于日新月异的数字经济实践仍存在鲜明的滞后性。面对数据生产力的理论盲区和现实隐忧，深刻把握生产力与生产关系的辩证关系、始终坚持人的主体地位，对于理论深化和生产力释放至关重要。

^① 李海俊. 数据生产力：主体异化与解放的生产力[J]. 西北民族大学学报(哲学社会科学版), 2021(05):11-19.

^② 王春晖, 方兴东. 构建数据产权制度的核心要义[J]. 南京邮电大学学报(社会科学版):1-12.

第二章 我国数据产权制度内涵

数据作为与土地、资本、劳动力、技术并列的第五大生产要素，已成为国家战略性资源。我国数据资源规模大、应用场景丰富，新形势下充分发挥数据资源优势、挖掘数据价值潜力，激发数据要素对其他要素的叠加、倍增、乘数效应，对于发挥数字经济创新引擎功能，促进经济高质量发展具有重要意义。当前，数据生产力的发展已经领先于数字化生产关系，工业时代形成的生产关系已经不能适应数据生产力时代的需要，所以需要在数字产业化，尤其是产业数字化的进程中不断创新数字化生产关系，以适应数据生产力的快速发展。同时，数字化生产关系的进步又反作用于数据生产力，当数字化生产关系符合数据生产力发展的客观要求时，对数据生产力的发展起推动作用，而当数字化生产关系不适合数据生产力发展的客观要求时，就会阻碍数据生产力的发展。数字化生产关系一定要适应数据生产力的发展，这是一条基本规律，当数据生产力超越数字化生产关系的发展时，就必须对数字化生产关系进行调整以适应快速发展的数据生产力。

目前中央文件已经明确了数据产权的概念，通过制度建设推动数字中国的建设和数字经济的发展，对于促进数据开发利用、推动政府数据开放、构建有序流动的数据市场格局、增强公民数据权益的保护意识、更好地协调和处理与数据生

产力发展相适应的数字化生产关系都具有重要的作用。

数据要素市场的发展要遵循其发展规律，应当在探索中发展，在实践中完善，最终形成与数据生产力相适应的新型生产关系。目前，数据要素市场仍处在培育期，构建适应数据生产力的数据要素基础制度是数据要素市场培育期的主要任务和重点工作，这对于充分释放数据要素价值，激活数据要素潜能，以数据流通促进生产、分配、流通、消费各个环节高效贯通，推动数据产品、应用范式、商业模式和体制机制协同创新，均具有重要的推动作用。

分析我国当前生产要素的特点，数据产权制度建立的重大意义，认识和理解“数据产权”，明确数据确权、数据授权在数据交易流通中的重要性，构建数据基础制度，有序推进数据应用，对加快数字经济和实体经济融合发展有积极意义。

第一节 我国当前数据及各类产权制度

2.1.1 我国当前生产要素的产权制度解析

生产要素（factors of production）在《政治经济学大辞典》中定义为“生产某种商品时投入的各种资源”。^①

随着经济社会的发展，生产要素概念扩展为“社会生产经营活动所必须具备的因素或条件”。^②

^① 张卓元主编：《政治经济学大辞典》，经济科学出版社，1998年版，第371页。

^② 《马宏伟：如何理解按生产要素分配》，共产党新闻网，2013年07月29日，<http://theory.people.com.cn/n/2013/0729/c367175-22367035.html>

当前，我国数字经济体量不断扩大，数据作为新型生产要素的生产力属性和技术支持性特征愈发明显。生产要素得以参与生产—流通环节，同各类要素所有者关系密切，生产要素的产权制度尤为关键。西方经济学中关于要素市场的理论指出，各类产品或服务的厂商购买生产要素不是为了自己的直接需要，而是为了生产和出售产品以获得收益，因而它是一种间接需求，是从消费者对产品的直接需求中派生出来的一种“引致需求”。^①马克思《资本论》也指出“商品不能自己到市场去，不能自己去交换。因此，我们必须找寻它的监护人，商品所有者”。同商品一样，若没有所有者，生产要素也无法自行交换，更不能投入生产。

中央党校（国家行政学院）经济学教研部宏观经济教研室主任陈启清教授认为，“明确产权、保护产权是生产要素参与生产并获得收入的前提，生产要素参与收入分配实际上是收入在不同要素所有者之间的分配。要实行最严格的产权保护制度，完善相关法律法规，形成清晰界定所有、占有、支配、使用、收益、处置等产权权能的制度安排，依法平等保护各类产权。要优化产权配置，推进产权制度改革”。

产权制度是新时代建设中国特色社会主义的基本保障。随着公有制经济和非公有制经济的快速发展，我国逐步确立了以公有制为主体、多种所有制共同发展的基本产权制度。

^① 冯伟《微观经济学讲义》，第六章 第二节，

<https://weread.qq.com/web/reader/5d932f90719972875d97713k6c8328f022d6c8349cc72d5>

党的二十大报告中指出，“完善产权保护、市场准入、公平竞争、社会信用等市场经济基础制度”。

确认、保护各类要素的产权是坚持社会主义基本经济制度的必然要求，也是促进各类要素共享企业发展、构建和谐劳动关系的前提条件。^①梳理我国现有产权制度，有助于推动产权制度进一步完善，调动各类生产要素参与生产的积极性、主动性、创造性，让各类生产要素的活力竞相迸发，让一切创造社会财富的源泉充分涌流，具有极其重要的理论意义和实践价值。

2.1.1.1 土地产权制度

古典经济学家威廉·配第在《赋税论》中说，“劳动是财富之父，土地是财富之母”。时至今日，土地作为生产要素已扩展为泛指各种自然资源，而非狭义上的土地资源，它具有数量有限、位置不变和不能再生等特点。土地作为生产要素具有稀缺性，将其投入到生产经营活动而形成的费用就形成了地租。西方经济学将地租定义为“土地使用者对使用土地所支付的价格或者是土地所有者因出让土地使用权而收取的报酬”，这一价格的形成离不开土地所有权和使用权两个关键概念的界定。^②

我国幅员辽阔，中国自然资源部数据显示，截至 2022

^① 胡乐明：《构建和谐劳动关系 扎实推动共同富裕》，光明日报 2021 年 10 月 12 日，第 11 版，http://www.qstheory.cn/qshyjx/2021-10/12/c_1127947808.htm

^② 冯伟《微观经济学讲义》，第六章 第二节，

<https://www.weread.qq.com/web/reader/5d932f90719972875d97713k6c8328f022d6c8349cc72d5>

年 6 月，耕地面积为 19.18 亿亩，土地资源事关我国粮食安全与乡村振兴建设，土地要素的产权制度更是农民增产增收、土地资源高效利用以及乡村振兴建设的关键。因而研究农村土地产权对理解土地生产要素制度有很好启示作用。^①

土地制度是农村生产关系的核心内容。我国农地产权是一个包含占有、使用、收益、处置等多项权利的权利束，每一项大的权利又可细分为多项具体权利。《农村土地承包法》作为规定我国农村土地产权的根本性法律文件，2019 年十三届全国人大常委会投票通过修改后，已完成从土地所有权和土地承包经营权的“两权分离”，到所有权—承包权—经营权的“三权分置”的法制化进程。^②《农村土地承包法》中第九条“承包方承包土地后，享有土地承包经营权，可以自己经营，也可以保留土地承包权，流转其承包地的土地经营权，由他人经营”，明确了经营权的独立。

农地产权明晰为三权分置后，对农地要素的利用、农地所有者权益的提升都有诸多益处。承包权的取得有严格的条件限制，而对经营权主体资格的限制则要少得多。这对于在更大范围内优化配置耕地资源、提高农业生产绩效具有重大意义，是通过土地制度创新实现多元经营的基本前提与必然

^① 《如何看待“三调”比“二调”少了 1.13 亿亩耕地》，农民日报 2021 年 08 月 27 日，第 2 版，https://szb.farmer.com.cn/2021/20210827/20210827_002/20210827_002_4.htm

^② 朱宁宁：《农村土地承包法首次大修把中央精神和实践经验转化为法律规范 落实所有权稳定承包权放活经营权》，中国人大网，2019 年 01 月 08 日，

<http://www.npc.gov.cn/npc/c199/201901/c5e9b9c2ec9648a6831345fa7a6322d2.shtml>

选择。^①将经营权独立于承包权，不仅从法律上保障村民作为土地承包人的权利，又具有提高土地要素利用效率、商品农产品生产率等效用。

2. 1. 1. 2 劳动力生产要素产权制度

马克思认为，劳动是生产的真正灵魂。法国庸俗政治经济学家萨伊指出，“事实已经证明，所生产出来的价值，都是归因于劳动、资本和自然力这三者的作用和协力”，劳动生产要素对社会生产活动参与之深、源远流长。

通常而言，劳动要素是更为常用的一个概念，但作为生产要素的劳动具有双面性。一方面代表劳动者所拥有的劳动力要素，另一方面体现为“活劳动”，即正在进行的劳动活动，是劳动者体力和脑力的消耗过程。生产劳动包括体力劳动和脑力劳动，因此可以说，社会生产的过程就是劳动力消耗的过程，也只有针对劳动力这一有形物而言，才能符合产权体系下“所有者（主体）—财产（客体）”之分，也就可凭借它形成财产权利关系，形成基本的“劳动力产权”体系的讨论。^②

劳动产权是人类社会一切其他产权的基础。因此，劳动产权理应得到现代社会的高度确认与保护。我国《宪法》中规定“按劳分配为主体、多种分配方式并存”作为社会主义

^① 张红宇：《从“两权分离”到“三权分离”》，中国人大网，2014年01月14日，<http://www.npc.gov.cn/npc/c222/201401/bff11bd015174338b2b0de9e3d09d8f2.shtml>

^② 陈位纲：《劳动、生产要素与价值----也谈国民经济新核算中的价值理论》，国家统计局网站，2010年10月15日，http://www.stats.gov.cn/ztjc/tjzdggy/hsyjh1/yjhxsjlh/hs11/201010/t20101015_69135.html

基本经济制度，在十九届四中全会进一步指出要“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”。二十大报告中也明确“努力提高居民收入在国民收入分配中的比重，提高劳动报酬在初次分配中的比重”。^①劳动产权在我国经济制度、分配制度中都具有重要地位，并不断得到完善。

劳动力生产要素产权制度，以所有权、支配权和使用权为主要组成，在劳动力的交易转换中能清晰地看到各权属的转移和变化。有观点分析，劳动力的交易（雇佣）使劳动力产权发生分离，工人凭借劳动力的归属权（狭义所有权）得到工资，而将劳动力的支配权、使用权转让给雇佣者。^②

在数字经济和平台企业快速发展的今天，以网约车、自媒体创作者为代表的平台从业者，也在不断探索数字经济背景下劳动力生产要素的概念边际。在数字经济发展浪潮下，传统的“雇佣者—劳动者”的雇佣关系逐步转变为“平台—用户”的松散生产关系，零工经济、兼职经济、直播经济等模式是这一转变的直接体现。

2.1.1.3 资本产权制度

资本是指由经济制度本身生产出来并被用作投入要素，

^① 《习近平：高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告》，求是网，2022年10月25日，

http://www.qstheory.cn/yaowen/2022-10/25/c_1129079926.htm

^② 《娄澜：对“劳动产权”理论的几点质疑》，《当代经济研究》2022年第9期，

http://ie.cssn.cn/academics/thinktank_center/202212/t20221206_5568856.html

以便进一步生产更多商品和劳务的物品。^①资本概念与资产概念息息相关，而资产可以理解为货币资金、厂房场地、机器设备等有形资产，也可以是专利权、商标权等无形资产。在马克思政治经济学定义下，资本与资产的本质不同，资本是一种以追求剩余价值的抽象价值，而资产仅是静态的实物。由此可见，资本作为生产要素加入社会生产过程中的应该是资产或者说资本品。

在社会主义市场经济体制下，资本是带动各类生产要素集聚配置的重要纽带，是促进社会生产力发展的重要力量。

“资本与其他生产要素的显著差别在于，资本是黏合剂，会把劳动力、土地、科技等要素黏合起来，达成合作机制，满足现实生产需求。”^②但资本生产要素的抽象价值和实物概念两面性，让资本在生产要素之外又作为生产关系。从现象上和资本在市场经济中的作用来看，资本是不可缺少的生产要素；从本质上和商品价值的创造来看，资本是生产关系，本身不能创造价值。^③

马克思在分析资本时指出，“要将自己的货币作为生息资本来增殖的货币占有者，把货币让渡给第三者，把它投入流通，使它成为一种作为资本的商品；不仅对他自己来说是

^① 冯伟：《微观经济学讲义》，第六章 第二节，
<https://weread.qq.com/web/reader/5d932f90719972875d97713k6c8328f022d6c8349cc72d5>

^② 中国经济网：《发挥好重要生产要素的积极作用》2022年8月8日，
<https://baijiahao.baidu.com/sid=1740546930575277933&wfr=spider&for=pc>

^③ 简新华：《正确认识“资本是社会主义市场经济的重要生产要素”》，《光明日报》，2022年09月27日，https://share.gmw.cn/news/2022-09/27/content_36050269.htm

作为资本，而且对别人来说也是作为资本；它不仅对把它让渡出去的人来说是资本，而且它一开始就是作为资本交给第三者的”。在货币资产成为商品、交付第三方并成为生产要素的过程中，资产产权的界定是关键。^①有学者指出，在保留所有权的前提下，把货币或其他生产资料的使用权让渡给职能资本家，从而产生所有权和支配权、使用权的分离。^②

这种所有权、支配权和使用权的分离，同农村土地的所有权、承包权和经营权的分离非常类似，使得资本产权同样具备提升生产要素的利用效率、促进新型业态发展等优势。

2.1.1.4 技术生产要素制度

马克思在《机器，自然力和科学的应用》中讲到，“每一项发现都成了新的发明或生产方法的新的改进的基础”。科学技术在当代生产力和社会经济发展中起着首要的变革作用。1988年9月5日，邓小平在会见捷克斯洛伐克总统时提出“科学技术是第一生产力”。随着科技的发展和知识产权制度的建立，技术也作为独立的要素用于西方经济学者的社会再生产分析之中，并形成了以“含有生产中的技能、技巧及其核心工具，以及工艺、程序和规则”为基础的生产要素概念。^③

^① 《资本论》第三卷（节选）#3，南京大学马克思主义社会理论研究中心，
<https://ptext.nju.edu.cn/b4/7e/c12196a242814/page.htm#:~:text=%E8%A6%81%E6%8A%8A%E8%87%AA%E5%BB%81%E7%9A%84%E8%B4%A7%E5%B8%81%E4%BD%9C,%E7%9A%84%E9%82%A3%E7%A7%8D%E4%BD%BF%E7%94%A8%E4%BB%81%E5%80%BC%E3%80%82>

^② 《娄澜：对“劳动产权”理论的几点质疑》，《当代经济研究》2022年第9期，
http://ie.cssn.cn/academics/thinktank_center/202212/t20221206_5568856.html

^③ 姚宇编著：《自由主义经济学的解读与批判：微观经济学讲义（修订版）》，第三章第一节，

就本质和属性而言，技术要素不同于其他常见生产要素，其往往具有依附性，大多需要依附于特定研发组织或科技人才而存在。因此技术要素常常无法如一般生产要素一样，可以剥离与依附者的关系进行价值交换，这是发展技术要素市场与发展土地、资本、劳动力和数据等要素市场的不同之处。

对 2019 年科技部火炬中心全国登记技术交易各类合同统计发现，仅有技术转让类交易可视作像一般商品一样完成了价值形态在依附关系上的剥离，但其占比仅为 9.8%，大量广泛存在的技术要素的流通和交易（如登记技术合同中的技术开发、技术服务、技术咨询）都需要有技术要素所依附的组织和人才载体参与才能发生。^①

《关于构建更加完善的要素市场化配置体制机制的意见》中明确“加快发展技术要素市场”，指出“深化科技成果使用权、处置权和收益权改革，开展赋予科研人员职务科技成果所有权或长期使用权试点”，将“所有权、使用权、处置权、收益权”作为构成技术生产要素产权制度的基本。该意见也指出目前我国技术要素开发利用不足，技术要素的各类科研人员、科研机构，与其所具备的技术之间权属界定仍有待完善。

随着我国经济转向高质量发展阶段，对知识、技术、管理等资源的需求增加，这些要素的稀缺度提高，市场对其贡

<https://www.zhihu.com/market/pub/120325903/manuscript/1536334502825066496>

^①《王胜光：发展技术要素市场的要义与命题》，深圳工业总会，2021 年 03 月 15 日，<https://new.qq.com/rain/a/20210315AOBOJK00>

献的评价就高，其在收入分配中的比例也会相应提高。^①技术生产要素的权属明确，对提升技术作为生产要素的流通利用十分关键。

2. 1. 1. 5 数据产权制度：去所有权化

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产方式、生活方式和社会治理方式。广泛意义上，数据是对事实、活动等现象的记录，可以是数字、字符、文字、图像等，^②也可以定义为“未经处理的事实或数值可供计算机（电脑）处理成为有用的信息”。^③按照《中华人民共和国数据安全法》中给出的定义，数据是指任何以电子或者其他方式对信息的记录。^④

数据的“收集”是使原始数据聚集在一起，“产生”则是将已有的原始数据进行加工，而派生出新的有价值的数据，这表明“收集”的数据和“产生”的数据是两类性质完全不同的数据。我国《数据安全法》和《个人信息保护法》关于数据处理行为的外延，包括数据的收集、存储、使用、加工、传输、提供、公开、删除等。“数据处理”的首个行为就是

^① 陈启清：《健全和完善生产要素参与分配机制》，共产党新闻网，2020年03月05日，<http://theory.people.com.cn/n1/2020/0305/c40531-31617679.html>

^② 夏征农、陈至主编，《大辞海：管理学卷》（2015年修订版），上海世纪出版有限公司，载于http://www.dacihai.com.cn/search_index.html?_st=1&keyWord=%E6%95%B0%E6%8D%AE&ite

^③ The Gartner Group Glossary of Information Technology Acronyms and Terms (May 2003), at 122, available at <https://www.gartner.com/en/information-technology/glossary/big-data> (原文为：Raw facts and figures that a computer processes into usable information.)

^④ 中华人民共和国数据安全法

<http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>

“收集”，数据处理中的“收集”主要是通过智能化方式对原始数据的获取和聚集，但是法定意义上的八个“数据处理”行为中并不包括数据的“产生”，数据的“产生”是对原始数据进行加工，而派生出新的数据价值。由此，数据的“收集”是“因”，而数据的“产生”是“果”，不同的数据处理方式，会产生不同的数据价值，这是数据生成的基本机理。

从数据生成的结构看，大致可划分为三种，即结构化数据、非结构化数据和半结构化数据。“结构化数据”的特征是可以用行为单位表现的数据，主要是由二维表结构来逻辑表达和实现的数据，其特征是严格地遵循数据格式与长度规范，如个人的身份证件（信用卡）号码、出行日期、电话号码、家庭地址等；“非结构化数据”的特征是结构不规则或不完整的数据，是一种很难用数据库二维逻辑表来表现的数据，如通过卫星收集的图像数据，通过摄像头、红外传感器、指纹传感器、麦克风等传感器收集的数据等；“半结构化数据”基本是介于结构化和非结构化之间，但趋向于结构化数据。

通过对上述原始数据的“收集”方式，以及经过加工“产生”的数据进行分析发现，在非结构化数据规模呈指数级增长的大趋势下，不可能出现组织或个人拥有数据所有权的命题。由此，数据产权制度最大的特征是“去所有权化”，不存在对数据的占有、使用、收益、处置的所有权问题。^①

^① 王春晖, 方兴东. 构建数据产权制度的核心要义[J]. 南京邮电大学学报(社会科学版):1-12.

数据作为新型生产要素与土地、劳动、资本、技术等传统生产要素相比具有明显的独特性。

第一，虚拟性，即非物理性。作为对物理世界的测量和记录，数据是人类思维活动的体现，本身并不具有物理属性。有学者认为，虚拟性的存在就意味着数据必须以其他生产要素作为载体才能发挥作用。在当前技术条件下，数据在大多数时候是存在于信息与通信技术（ICT）产品中的。虚拟性是数据与其他传统生产要素如劳动力、资本和土地的最主要差异。^①

第二，低成本复制性。数据可无限复制给多个主体同时使用，任何主体对数据的使用都不会影响其他使用者的利益。王春晖认为，数据作为关键生产要素与农业经济和工业经济时代的关键生产要素最大的不同是，后者面临着稀缺性的制约，前者的生产是无穷尽的，尤其是数据要素可复制和共享，从根本上打破稀缺性生产要素的制约。^②

第三，主体多元性。由于数字空间中的每条数据可能记录了不同用户的信息，而数据集的采集和汇聚规则又是由数据收集者设定，因此用户、收集者等主体间存在复杂的关系。同时，企业也可能对所用的数据资源进行一定程度的加工，而每一次增删改的操作都是对数据集的改变，所以这些加工

^① 徐翔等：数据生产要素研究进展

https://brgg.fudan.edu.cn/demo/articleinfo_3568.html

^② 数据交易是一种可以无限复制的增值式交易模式——专访王春晖

https://m.21jingji.com/article/20220805/herald/60157606f17b91937b7ff6b0aa313fb2_ths.html

者也是数据构建的参与主体。^①

第四，非竞争性。得益于数据能够被低成本复制，同一组数据可以同时被多个主体使用，一个额外的使用者不会减少其他现存数据使用者的使用，也不会产生数据量和质的损耗。如在各类数据分析、机器学习竞赛中，同一份数据可以被大量参赛者使用。非竞争性为数据带来普遍的使用效益与更大的潜在的经济价值。

第五，非排他性。数据持有者为保护自己的数字劳动成果，会付出较高代价使用专门的人或技术手段控制自己的数据，因而在实践中，数据还具有一定的排他性。然而，一旦数据持有者主动放弃控制或控制数据的手段被攻破，数据就将完全具有非排他性。排他性是界定产品权利的重要基础，土地、劳动、资本都有明显的竞争性和排他性，可以在市场中充分实现权利流转。而技术在当今专利保护制度下同样具有排他性，也可实现权利转让和许可。

第六，异质性。相同数据对不同使用者和不同应用场景的价值不同，一个领域高价值的数据对另一领域的企业来说可能一文不值。与数据形成鲜明对比的是资本，资本是均质的，每份资金都有相同的购买力，对所有主体同质。^②

第七，边际效应递增性。数据资源有边际报酬递增的效果，也就是说，当数据规模越大、种类越多时，它越能焕发

^① 中国信通院《数据要素白皮书》（2022年）第3页。

^② 中国信通院《数据要素白皮书》（2022年）第4页。

出强大的生产力作用。^①

2.1.2 数据产权区别于其他产权的独特性

数据产权是适应当代数据市场经济发展要求而出现的新兴经济范畴。目前，国家数据主权、企业商业利益和个人隐私保护等方面均面临确权困境。在谈及数据产权时，通常情况下会把所有权与产权混为一谈。需要指出，所有权不同于产权，所有权指对财产归属关系的权利规定，强调财产关系的物质属性；产权是基于财产权的一组权利的有机结合体，强调财产关系的社会属性。数据产权是持有和使用数据资源的权利，并不是对数据资源占有、使用、收益、处置的权利。

数据产权制度体系不属于要素制度体系，它是数据要素流通和交易制度体系、数据要素收益分配制度体系、数据要素治理制度体系三大类数据要素基础制度体系的根基，数据产权制度最大的特征是“去所有权化”。^②从农业经济的二维生产要素到工业经济的四维生产要素，再到数字经济的五维甚至更多维生产要素。与其他数据要素相比，数据具有明显的不同特征，因此，建立数据产权制度必须考虑到数据的不同特性。同时也要厘清产权与所有权的关系。

产权与所有权既有联系又有区别，两者的属性不同，产权是主要基于财产所有权为核心的一组权利的有机结合体，

^① 北京日报《越生产、越消费，数据资源越多，这与传统生产要素迥异——数据资源有边际报酬递增效果》2022年7月18日，

https://bjrbdbz.bjd.com.cn/bjrb/mobile/2022/20220718/20220718_010/content_20220718_010_3.htm#page9?digital:newspaperBjrb:AP62d46ef5e4b0647f1b15a996

^② 王春晖,方兴东. 构建数据产权制度的核心要义[J]. 南京邮电大学学报(社会科学版):1-12.

强调财产关系的社会属性；所有权指对财产归属关系的权利规定，主要强调财产关系的物质属性。正如科斯的《权利行使说》所表述的，产权体现的不是人与物的关系，而是人与人之间的关系。

因此，数据资源持有权、数据加工使用权、数据产品经营权的前提是制度安排，这种制度实质上是一种人们之间行使一定数据行为的权力。

数据产权是适应当代数据市场经济发展要求而出现的新兴经济范畴。在数据要素市场条件下，数据产权的属性主要有四大特征：一是数据产权具有经济特性；二是数据产权具有可分离性；三是数据产权流动具有独立性；四是数据的财产属性具有可复制性。数据要素与其他四大要素，如土地要素、劳动力要素、资本要素、技术要素最大的不同在于数据要素具有“非竞争性”特征，数据要素的生产是无穷尽的，尤其是数据要素的可无限复制性，导致其边际成本几乎为零，从根本上打破了稀缺性生产要素的制约。

数据产权制度的确立，最重要的是解决数据产权的两大清晰问题：一是数据在法律层面的清晰，这要求数据产权要有明确的法律地位，否则很难实现市场主体享有依法依规持有、使用、获取收益的权益；二是数据在经济层面的清晰，这要求数据产权的合法持有者对数据产权具有极强的约束力，这需要构建数据产权的约束依据，通过约束依据明确数

据产权的收益目标。^①

第二节 建立数据产权制度的重要性分析

2.2.1 数据产权制度是“四大制度”的核心

“数据二十条”指出要建立四大数据基础制度，对数据要素在生产、分配、流通、消费和社会服务管理等各个环节的贯通参与，具有重要推动意义。

“数据二十条”第二章提出，“建立保障权益、合规使用的数据产权制度”，要“探索建立数据产权制度，推动数据产权结构性分置和有序流通，结合数据要素特性强化高质量数据要素供给”。

数据作为新型关键生产要素，其特性决定了数据要素产权制度的新颖与复杂。数据要素权益的首要任务是界定产权，明确规定数据处理者可以做什么，然后通过权利交易达到社会数据总产品利用的最大化。^②

针对如何完善数据产权制度，国家发展和改革委员会指出，“推动数据产权结构性分置，跳出所有权思维定式，聚焦数据在采集、收集、加工使用、交易、应用全过程中各参与方的权利，通过建立数据资源持有权、数据加工使用权、数据产品经营权‘三权分置’，强化数据加工使用权，放活数据产品经营权”，点明数据生产要素产权制度由“持有权、

^① 《王春晖 | 解析“数据二十条”中的数据产权制度》，上海市法学会-东方法学公众号，<https://mp.weixin.qq.com/s/m9Q9QXbjmRzIYSEvwk1CcA>

^② 《王春晖 | 解析“数据二十条”中的数据产权制度》，上海市法学会-东方法学公众号，<https://mp.weixin.qq.com/s/m9Q9QXbjmRzIYSEvwk1CcA>.

使用权、经营权”的权属组成结构。^①

观察土地、劳动力、资本、技术和数据的产权制度发现（见表 4），各类生产要素都不同程度上出现了“权属分置”现象。一定程度上，所有权同使用权、经营权等要素加工使用和收益分配相关环节下的权利条件，进行了隔离安排。我国要素市场体量和要素需求量庞大，权属分置方式的产权制度，是符合我国国情、具备我国特色的产物，也是在统筹发展与安全的系统考虑结果。

表 4 五类生产要素产权制度组成

要素类别	产权制度组成
土地	所有权—承包权—经营权
劳动	所有权—支配权—使用权
资本	所有权—支配权—使用权
技术	所有权—使用权—处置权—收益权
数据	持有权—使用权—经营权

数据要素市场是数据流通交易分配的重要媒介和场所，对价值产生具有关键作用。据不完全统计，截至 2022 年底，国内由副省级以上政府牵头组建的数据交易场所已超过 30 所，全国各地积极建设各类数据交易机构，为数据要素更大规模全面流通奠定了较好基础。^②

数据产权制度的安全运行，还需要数据治理作为重要保障制度。数据要素安全治理作为数据基础制度的四大组成部

^① 《加快构建中国特色数据基础制度体系 促进全体人民共享数字经济发展红利》，《求是》，http://www.qstheory.cn/dukan/qs/2023-01/01/c_1129246978.htm

^② 刘园园：《“数据二十条”：以基础制度破解数据要素价值释放难题》，《科技日报》，2022-12-21，http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2022-12/21/content_546326.htm?di=v=-1

分之一，贯穿数据流通交易的各个环节，涉及数据要素市场培育的方方面面，发挥着不可替代的重要作用既有利于保障国家数据安全，也有利于维护企业、个人数字权益。可以说，只有建立健全安全可控的数据要素治理制度，才能真正实现数据要素市场的高质量发展。^①

2.2.2 确权是数据交易流通的前提

数据确权意为确定数据的权利属性，主要包含两个层面：第一是确定数据的权利主体，即谁对数据享有权利；第二是确定权利的内容，即享有什么样的权利。数据本身蕴含着个人、企业等主体的信息，会涉及相关当事人的物权、人格权、民事权、隐私权等多种权利，因此确认数据产权的权利归属的难度较大。^②

在制度层面，一系列政策的出台为数据在交易流通中明确数据权属指明了方向。2022年11月16日，国家发展和改革委员会发布《关于数字经济发展的报告》强调数字经济治理体系建设，明确指出推进公共数据、企业数据、个人数据分类分级确权授权使用，构建数据产权、流通交易、收益分配、安全治理制度规则，统筹推进全国数据要素市场体系。

“数据二十条”的发布，从数据产权、流通交易、收益分配、安全治理等方面构建数据基础制度，提出20条政策举措。

^① 周民：《完善数据要素治理制度，保障数据流通交易安全 《数据二十条》解读》，国家发展和改革委员会网站，2022年12月20日，

https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343659.html?code=&state=123

^② 《数据要素：全球经济社会发展的新动力》人民邮电出版社 2021.1/赵刚著 第三章 3.6.1 数据要素市场化配置的挑战 167页。

多项顶层设计政策文件的出台，对推动数据持有权、使用权等相关权利的有序分离，创新数据产权配置的路径，承认和保护数据要素各参与方的合法权益和义务，提出了明确的要求和规定。数据作为新型生产要素，对传统产权、流通、分配、治理等制度提出新挑战，而在数据交易流通环节所面临的一些数据确权问题仍需重点关注。

第一，产权界定清晰、权责明确，支持数据共享流通。构建数据确权基本框架时需考虑三项重点内容：一是明确公共数据的公有性质，所有权归国家所有；二是厘清数据所有权、使用权、运营权、收益权等权利，形成体系化的数据权利束；三是强化数据权利司法保护，依法保护权利人对数据控制、使用、处理、受益等合法权益。^①

第二，数据进场意愿不足，权属界定不清导致交易成本上升。合规交易的基础是清晰的产权归属。但数据所有权拥有者是产生数据的个人还是记录数据的企业，业界、学界和司法界莫衷一是，而以所有权为基础的使用权、处置权等更难以界定。^②

第三，数据分类分级确权授权制度亟待建立。从实践来看，公共数据和个人数据的权属问题相对清晰，企业数据方面则较为复杂。

^① 《人民政协报》（2022年05月18日第03版）

http://dzb.rmxzbx.com/rmxzbxPaper/pc/con/202205/18/content_24847.html

^② 南方都市报《京沪深等地数据交易机构共话数据交易新趋势推动协同监管机制建立 完善数据交易分级分类标准》（2022年4月6日GA15版），

http://epaper.oeeee.com/epaper/A/html/2022-04/06/content_6516.htm

一些数据交易场所迈开了破解“确权难”的第一步。从长远来看，根据数据来源和数据生成特征，国家层面的公共数据、企业数据、个人数据分类分级确权授权制度亟待建立，通过分别界定数据生产、流通、使用过程中各参与方享有的合法权利，为激活数据要素价值创造和价值实现提供基础性制度保障。^①

数据确权是数据交易流通的前提，在明确数据确权的基本原则和充分把握数据发展规律的前提下，才能推动数据确权的分类分级，满足不同类型数据的管理和使用需求。在探索更加精准的数据确权过程中，要坚持安全发展，处理好发展与安全的关系。

2.2.3 授权是数据交易流通的重要方式

数据授权是实现数据要素交易流通，促进数据价值释放的重要的方式。“数据二十条”明确指出，探索数据产权结构性分置制度。建立公共数据、企业数据、个人信息数据的分类分级确权授权制度。

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，推进非公共数据按市场化方式“共同使用、共享收益”的新模式，为激活数据要素价值提供基础性制度保障。数据

^① 人民日报：《数据交易如何更规范高效（经济时评）》（2023年01月09日 10版），http://paper.people.com.cn/rmrb/html/202301/09/nw.D110000renmrb_20230109_2-10.htm

分级分类授权机制可以推动数据快速进入数字经济的生产活动之中，不仅使各类数据主体对数据的获取和利用变得合理合法，也能减少数据的交易成本。^①

数据授权是数据产权制度建设的关键环节，也是促进数据交易流通的重要方式。加强公共数据的开放共享，打破“数据孤岛”；鼓励探索企业数据授权使用新模式，发挥平台企业的龙头作用，促进与中小微企业双向公平授权；积极探索个人授权，按照个人授权范围依法采集、持有、托管和使用，数据的分类分级确权，对于完善数据产权制度具有积极意义。

^① 《王春晖 | 解析“数据二十条”中的数据产权制度》，上海市法学会-东方法学公众号，<https://mp.weixin.qq.com/s/m9Q9QXbjmRzIYSEvwk1CcA>

第三章 主要发达国家数据要素产权发展介绍

第一节 当前数据要素的通用性国际规则介绍

当前，全球范围内各国均对数据要素加强研究和实践，了解主要发达国家、相关国际组织在数据要素产权的实践，尤其是在个人信息的定义、数据主体的权利、数据处理者权利义务和法律后果等方面的做法，有助于推进我国数据要素的发展。

3.1.1 各主要发达国家的相关法规政策

3.1.1.1 欧盟、美国对个人信息的界定

国际社会中，尤其是欧盟、美国等地区也在加快对数据要素的研究和立法过程。其中，欧盟的《通用数据保护条例》(General Data Protection Regulation，简称“GDPR”)和美国加利福尼亚州的《加利福尼亚消费者隐私法案》(California Consumer Privacy Act，简称“CCPA”)影响较大，尤其是其对个人信息数据方面的界定值得探究。

欧盟 GDPR 的第四条，对个人信息的定义为：个人数据是指与已识别或可识别的自然人（“数据主体”）有关的任何信息；可识别的自然人是指可以直接或间接识别的人，特别是通过参考诸如姓名、身份证件号码、位置数据、在线标识符等标识或与该自然人的身体、生理、遗传、精神、经济、文化或社会身份有关的一个或多个特定标志。

CCPA 的第 1798.140. 条 (v) 项，也对个人信息进行定

义：个人信息是指直接或间接地识别、关联、描述，或能够合理地联系到一个特定的消费者或家庭的信息。。

3.1.1.2 GDPR 对数据主体权利的界定

GDPR 中关于数据主体的权利内容，主要集中于知情权、查阅权、反对权、删除权、复制权等权利，涉及数据主体的权利条文共计 11 条，从第 12 条至第 23 条。

具体而言，第 12 条至第 14 条要求数据处理者必须提供透明完整的联系方式给数据主体，且在面对数据主体行使权利的诉求时不得无故拖延。数据处理者必须在取得数据主体的个人信息前或者取得个人信息后提供包括但不限于数据处理、存储的相关材料等；第 15 条规定了数据主体有权知悉数据处理者是否正在处理其数据；第 16 条规定了数据主体有权要求控制者对其不准确的个人数据做出更正，并不得无故拖延；第 17 条规定了数据主体有权要求数据处理者删除其个人信息的情形；第 18 条规定了数据主体有权限制数据处理者对数据的处理；第 21 条规定了数据主体有权拒绝其个人信息被数据处理者处理。^①

3.1.1.3 对法律后果的界定

在法律后果层面，欧盟、美国的相关法律主要涉及民事诉讼、行政责任、刑事后果等方面的内容。总体而言，欧盟 GDPR 的执行落地主要依靠行政规制，但仅仅在条文中认可诉

^① <http://www.dehenglaw.com/CN/tansucontent/0008/022406/7.aspx?MID=0902>

讼权利，在民事诉讼的实体性和程序性问题上，仍存在着诸多理论和实践障碍。美国没有专门的行政诉讼程序，而只有民事诉讼和刑事诉讼程序之分。

（1）民事诉讼

欧盟采取过错推定原则，美国采取过错原则。

从实体和程序上来说，CCPA 大大限制了个人信息违法行为的可诉性，更倾向于由检察长行使监管职权。CCPA 的第 1798.150 条明确规定了消费者的权利，即仅能在企业违反安全保障义务，致使消费者原始个人信息受到未经授权的访问和泄漏等情况下，才能提起民事诉讼。

GDPR 中认可民事损害赔偿机制，但是并没有规定统一的民事诉讼程序，而是授权适格法院适用其所在国的法律进行审理。由于 GDPR 项下的民事诉讼没有统一的审理机构，因此面临一系列程序上的问题，而且各成员国法院对某些实体法律问题的判断认定也并不完全一致，还需要欧盟法院进行统一。^①

（2）行政责任

整体来看，欧盟对具体的处罚数额或者处罚营业额占比作出了具体规定，美国法确立行政罚款一般都如 CCPA 一样仅规定罚款基准和公式。

GDPR 在第 83 条规定了针对数据处理者行政处罚的基本

^① See Data protection litigation on the rise: an area to watch out for,

<https://www.lexology.com/library/detail.aspx?g=c7d16841-667b-43f2-b3f2-22907de1d54>

原则，对于数据处理者进行行政处罚时应当考虑的因素，如侵权行为的性质、严重程度和持续时间，数据处理的性质、范围或目的等内容，同时 GDPR 还规定了罚款数额及标准。

CCPA 的 1798.155(b) 条规定，行政罚款的执行需要“总检察长以加利福尼亚州人民的名义提起民事诉讼”，在诉讼中，总检察长可以对罚款进行“评估和主张”。CCPA 规定的罚款为：企业每次违法行为的罚款最高为 2500 美元，每次故意违法的罚款最高为 7500 美元。

美国、欧盟均采取专门机构负责监管，其中欧盟采取数据保护监督机构（DPAs），美国由总检察长获得广泛的执法权，通过民事诉讼的方式进行罚款。

（3）刑事后果

针对刑事处罚方面而言，根据 GDPR 序言第 151 条针对丹麦和爱沙尼亚这两个成员国的例外规定，允许在丹麦通过刑事处罚的方式，在爱沙尼亚通过轻罪程序框架的形式来对违规主体及其高级管理人员进行惩罚。CCPA 则并无关于刑事责任的具体规定。

第二节 美国对数据要素、数据产权的做法解析

美国 1974 年的《隐私法》（U. S. Privacy Act of 1974）对政府机构持有的数据的权利和限制进行界定；1996 年的《HIPAA 法案》针对医疗保健和健康保险个人数据保护的情况，设定了健康数据的隐私保护标准；1999 年的

《Gramm-Leach-Bliley 法案》对财务非公开个人信息进行保护；2000 年《儿童在线隐私保护法》生效，保护了 12 岁及以下人群的个人信息。^①除此之外，还有 CCPA、《电子政务法》《信息技术管理改革法》《数据质量法》等与数据市场相关的法律法规。^②以下将着重介绍《美国数据隐私和保护法》和《加利福尼亚消费者隐私法案》。

2022 年 6 月 3 日，美国参众两院发布了《美国数据隐私和保护法》（American Data Privacy and Protection Act，简称“ADPPA”）草案，这是一项具有分水岭意义的隐私法案，将引入联邦标准。目前，行业特定法律和州法律共同构成了美国隐私法规和权利的支柱，因此，ADPPA 的颁布为美国的数据隐私权这一核心权利建立了一个统一的体系。^③

对于 ADPPA 来说，该提案由两项关键条款组成：联邦优先购买权和私人诉讼权（private right of action，简称“PRA”）。这是美国国会目前审议的唯一包含这两项条款的法案。且该法案借鉴了欧盟立法的许多关键原则，尤其是 GDPR 中的相关规定。具体如下：

首先，ADPPA 确立了联邦法优先于州法律，这意味着其条款将取代许多现有的州隐私法。然而，该法案排除了在 16

^① U. S. Privacy Laws: The Complete Guide, 2022 年 9 月 2 日,
<https://www.varonis.com/blog/us-privacy-laws>

^② 数据要素市场 须完善基础性制度, 2020 年 04 月 21 日,
http://www.qstheory.cn/llwx/2020-04/21/c_1125884656.htm

^③ Maybe This Time : Federal Government Proposes the American Data Privacy and Protection Act, 2022 年 6 月 8 日,
<https://www.dataprotectionreport.com/2022/06/maybe-this-time-federal-government-proposes-the-american-data-privacy-and-protection-act/>

个领域的优先购买权，包括州法律对公民权利、刑法、学生和员工隐私、数据泄露通知要求、面部识别以及财务和健康记录等方面的具体法规规定。

其次，该法案为违规行为创建了标准。例如，选择退出定向广告的互联网用户将有权起诉不当在线销售该用户数据的实体。

再次，ADPPA 要求公司尽量减少数据收集做法，只收集其业务运营所必需的数据。该法案还禁止实体向用户收取访问用户自身个人数据的费用（此处有例外，例如消费者忠诚度计划，或当使用财务数据完成交易时的情况等）。此外，该法案扩大了对未成年人隐私权的保护，包括禁止公司向 17 岁以下的用户传播有针对性的广告等。

根据现有的法案草案，用户也有权更正、访问或删除自己的数据。一旦用户修改了公司持有的数据，那么将由该公 司负责将任何变化通知给第三方。^①

相较于 2022 年刚通过的《美国数据隐私和保护法》，CCPA 是美国第一部也是迄今最具影响力的州级消费者隐私法。

CCPA 赋予了消费者更多对企业收集的其个人信息的控制权，并为如何实施该法律提供了指导。这项法律为加州消

^① Maybe This Time : Federal Government Proposes the American Data Privacy and Protection Act, 2022 年 6 月 8 日,
<https://www.dataprotectionreport.com/2022/06/maybe-this-time-federal-government-proposes-the-american-data-privacy-and-protection-act/>

费者的新隐私权提供了保障，包括了解企业收集的个人信息以及如何使用和共享的权利；删除从他们那里收集的个人信息的权利（有些例外）；选择不出售或不分享其个人信息的权利；行使 CCPA 权利时不受歧视的权利。受 CCPA 约束的企业有几项责任，包括响应消费者行使这些权利的请求，并向消费者发出解释其隐私做法的通知。CCPA 适用于许多企业，包括数据经纪人。^①

整体来看，CCPA 在关于隐私和数据安全部分，特别强调了“消费者隐私资源，身份盗窃，在线保护儿童，商务隐私资源，隐私执行、法律和立法，隐私报告，特别保护，数据泄露”等方面。

此外，美国还有一些针对特定行业或部分人群的需求而颁布的有关数据隐私的法律法规。如《儿童在线隐私保护法》（COPPA）规定网站管理者要遵守隐私规则，必须说明何时和如何以一种可以验证的方式向儿童家长索求同意，并且网站管理者必须保护儿童在线隐私和安全；《健康保险可携带性和问责制法》（HIPAA）确保患者所有医疗保健相关数据的保密性；《电子通信隐私法》（ECPA）防止政府未经允许接收和监听私人电子通讯。^②

从数据开放角度看，美国已建立起全国性的政府数据开放平台。例如早在 2009 年上线的美国 data.gov 网站，发布

^① California Consumer Privacy Act (CCPA), <https://oag.ca.gov/privacy/ccpa>

^② data privacy (information privacy), Stephen J. Bigelow, <https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy>

了农业、商业、气候、教育、能源等多领域的高质量公共数据，至今仍在不断更新。为保证公共数据开放质量，data.gov 开发开放数据仪表盘，设计数据质量自动评分与人工评分机制。政府、企业、公众均可查看开放政策数据进展、数据质量评分等内容，公共数据需求方可获得良好的服务体验。^①

第三节 欧盟对数据要素、数据产权的做法解析

近年来，欧盟在数据治理方面不断完善，打造单一数据空间以消除成员国政策碎片化，构建数据的保护与流动机制，形成垂直管理的治理体制，致力于提高个人数据保护水平，2018年5月正式施行的《通用数据保护条例》（GDPR）正是这一立法理念的代表产物。

为了发挥数据的重要作用，2020年2月，欧盟委员会正式公布了《欧洲数据战略》，其立法侧重从保护公民个人数据隐私转为促进数据流通利用，个人数据的定位亦发生了从人格承载向重要资产的转变。^②而《数据法案》《数据治理法》，均是践行欧洲数据战略的关键立法成果，代表了欧盟数据治理的最新发展趋向。

在大数据时代，怎样才能更好发挥数据资源的价值、促进数据要素市场培育，是建立数据基础制度需要考虑的重要命题，欧盟的相关做法可以为我国带来一定启示。

^① 中国信通院，数据要素白皮书，中国信息通信研究院，2022年，第一版，第17页。

^② 赵刚，数据要素，中国工信出版集团、人民邮电出版社，2021年，第一版，前言。

3.3.1 GDPR 规范数据要素

《通用数据保护条例》（GDPR）于 2018 年 5 月正式施行，该法旨在通过加强对数据控制者和处理者的规制，维护和扩大公民对其个人数据的控制权，被称为“史上最严”个人数据保护条例。^①

GDPR 条例的适用范围极为广泛，任何收集、传输、保留或处理涉及欧盟所有成员国内的个人信息的机构组织均受该条例的约束。GDPR 规定了个人同意提供数据的权利、组织必须将违规行为通知数据主体以及个人使用其数据的权利等领域。^②

整体而言，GDPR 主要突出数据私权至上的原则，极大地扩充数据主体的数据权利范围和保护机制，对数据控制者和处理者使用个人数据进行了严格的限制，加大了数据控制者和处理者对个人数据管理的法律责任，并对违反 GDPR 的行为，尤其是违反监管机构发布的命令，规定了极其严厉的惩罚措施。

其中第五条规定了数据控制人在进行数据处理的过程中应当遵循的基本原则，即合法性、公平性和透明性原则，目的限制原则，数据最小化原则，数据准确性原则，存储限制原则，诚实和保密性原则。

^① 人民法院报：《欧盟数据治理的新发展》（2022 年 11 月 4 日），
https://www.bj148.org/wh/b1/sy/202211/t20221104_1641219.html

^② data privacy (information privacy), Stephen J. Bigelow,
<https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy>.

第三十条规定了所有控制者和处理者及其代表，都应当保存数据处理活动的记录。从公司层面来说，需要保存个人信息被收集和处理的原因，以及对该信息本身的描述及相关处理结果的说明文件。如，当用户请求访问他们的个人数据并验证公司处理了与他们有关的哪些个人数据时。企业必须确认正在处理与的他们有关的个人数据，并提供副本（例如姓名，联系方式，交换的消息和图片）。同时，还须向他们提供处理的信息（通常这些内容在企业的服务隐私声明中）。

总体而言，GDPR 大致赋予了数据主体七项数据权利，包括知情权、访问权、修正权、删除权（被遗忘权）、限制处理权（反对权）、可携带权和拒绝权等。

在实践中，如果个人想了解哪些公司知道或者掌握了自己的个人信息，可以通过主体查阅请求（Subject Access Request，简称“SAR”）要求相关公司提供信息。当数据主体提出主体查阅请求后，就有权从控制者处获得有关其个人数据是否被处理的确认信息，以及有权在该种情况下访问个人数据和相关的其他补充信息。公司必须在一个月内回应这类请求，并说明处理这些个人信息的原因，以及将来该如何使用这些信息和对该信息的保留时间。

3. 3. 2 《数据治理法》《数据法案》对数据确权授权的规范

2022 年 2 月 23 日，欧盟委员会发布《数据法案》（Data Act），以促进欧洲数据价值释放为目标，明确了多项数据

流通共享举措。2022年6月23日，欧盟《数据治理法》正式生效，旨在通过增强对数据中介的信任，增强整个欧盟数据共享机制，来提升数据的可用性。两部法案均围绕促进欧洲数据价值释放这一目标，内容分别侧重于公共部门与私人部门所持有数据的共享利用。

（1）《数据治理法》相关内容

《数据治理法》共9章38条，主要内容包含“公共部门数据的重用条件”“数据中介服务监督框架”“数据利他主义”三方面。

其中“重用”是指自然人或法人对公共部门所持有的某些数据的重新使用，该使用需基于公共任务之外的商业或非商业目的。《数据治理法》规定，重用应遵循非歧视性、透明、合比例和客观合理等条件，这些条件不应被用来限制竞争。公共部门应对数据进行安全处理，确保数据在其提供或控制的安全处理环境中被访问和重用，确保数据所承载的其他受保护利益，如个人数据、商业机密、知识产权等，不因重用而被损害。

数据中介服务提供者是指在数据持有者与潜在数据使用者之间提供技术、实现数据共享的从业者。《数据治理法》规定，数据中介服务提供者应向数据中介服务主管部门告知其服务提供及相关信息。相关主管部门应对数据中介服务提供者是否符合法定条件予以确认，对数据中介服务提供者的

合规情况进行监督。

而数据利他主义是指为公共普遍性利益，数据主体自愿无偿共享其个人数据，或数据持有者自愿共享其非个人数据而不寻求或获取超出数据收集成本的补偿。《数据治理法》规定，成员国可以通过在组织或技术方面的安排以促进数据利他主义。被认可的数据利他主义组织应履行保障数据主体和数据持有者数据权益的义务，并由相关主管部门予以合规监管。^①

（2）《数据法案》相关内容

《数据法案》的具体措施主要包含四点，一是允许连接设备的用户访问由其生成的数据，及与第三方共享此类数据，以提供售后市场或其他数据驱动的创新服务。通过支付与传输相关成本并禁止在与其产品直接竞争中使用共享数据，激励制造商投资于高质量数据生成。二是防止滥用数据共享合同中的不平衡，重新平衡中小企业谈判权力。欧委会将制定示范合同条款，以帮助这些企业起草和谈判公平的数据共享合同。三是允许公共部门在特殊情况下访问和使用私营部门持有数据。特别是在发生洪水、野火等公共紧急情况下，或在执行法定任务但无法以其他途径获得数据的情况下。四是允许客户在不同云数据处理服务提供商之间进行有效切换，并针对非法数据传输采取保护措施。

^① 人民法院报：《欧盟数据治理的新发展》（2022年11月4日），
https://www.bj148.org/wh/b1/sy/202211/t20221104_1641219.html

根据《数据法案》规定，消费者和企业将能够访问其设备的数据，并可以将其用于售后和增值服务，如预测性维护等。通过获得更多的数据，消费者和用户将能够做出更好的决定，例如购买更高质量或更可持续的产品和服务，从而为绿色交易目标作出贡献。工商界人士将获得更多的可用数据，并从竞争激烈的数据市场中受益。售后服务提供商将能够提供更个性化的服务，且可以与制造商提供的同类服务平等竞争，同时数据也可以组合起来帮助开发全新的数字服务。^①

《数据法案》中引入了互联产品这一对象。互联产品作为一种与互联网相连的设备，能够收集和共享在用户使用过程中产生的海量个人数据与非个人数据，在大数据时代的应用范围非常广泛，包括机动车、医疗设备、工业设备和智能包装等。《数据法案》中制定了涵盖公私主体的“互联产品数据”访问与使用规则，主要内容包括数据持有者向私人部门的数据共享和向公共机构的数据共享两部分。

这意味着互联产品与相关数字服务的用户享有访问、使用互联产品数据和要求数据持有者向第三方提供数据的权利，即“数据可携带权”。因此数据持有者具有应用户要求共享互联产品数据的义务，但为避免因数据共享损害数据持有者竞争利益，特规定了用户或接收数据的第三方关于数据使用和披露的限制和义务。

^① Data Act: Commission proposes measures for a fair and innovative data economy, 2022年2月.

另外，关于互联产品数据是公共机构为公共紧急情况的应对、预防或从中恢复等基于公共利益的特殊需要使用的情况，收到公共机构数据使用请求的数据持有者有义务及时提供数据。但如果请求提供的数据涉及个人数据，数据持有者应当对数据进行假名化处理。而且除应对公共紧急情况外，公共部门机构基于其他特殊需要使用互联产品数据的，数据持有者有权获得补偿。^①

第四节 RCEP、DEPA 等区域性组织的数据规则

3.4.1 RCEP 中数据要素的章节

2020 年 11 月 15 日签订的《区域全面经济伙伴关系协定》（简称“RCEP”）拟在亚太主要经济体之间建立全球最大的自由贸易区，促进区域经济的一体化，提高域内经济体抵御重大风险的能力。自由贸易区的重要特征是货物、资金、人员等要素在区域内流动的障碍得到消除或大幅减少，而区内贸易和投资成本显著降低。RCEP 则围绕货物贸易零关税、原产地累积规则、服务贸易开放、投资市场准入和保护、自然人流动等角度，提出了详细而具体的规定，将为贸易和投资的自由化带来积极效应。

目前，RCEP 缔约国的数据保护规则基本上都遵循欧美所倡导的“合法、正当、必要、最小化”等原则，严格限制对数据的收集、转移及利用。然而，各国的数据保护规则内涵

^① 人民法院报：《欧盟数据治理的新发展》（2022 年 11 月 4 日），

https://www.bj148.org/wh/b1/sy/202211/t20221104_1641219.html

仍存在较大的差异，加上各国执法上的自由裁量权，极容易形成新型的贸易壁垒。

网络安全和数据保护水平，已日益成为国家乃至地区竞争力的重要力量。RCEP 作为一个现代、全面、高水平和互惠的贸易协定，在数据保护的国际化方面付出了很大的努力。欧盟是 RCEP 缔约国的最重要贸易伙伴之一，为了避免本国企业遭受欧盟的严苛处罚，并且确保本国企业与欧盟之间的正常数据交流，RCEP 缔约方也不得不向 GDPR 看齐，努力提升本国的数据保护水平，争取获得欧盟的充分性认定。RCEP 中与数据要素相关的内容具体如下：

第一，RCEP 肯定数据治理的必要性，其第十二章“电子商务”第八条第一款规定，“每一缔约方应当采取或维持保证电子商务用户个人信息受到保护的法律框架”。

第二，RCEP 关注过度监管对数据流动的妨碍。其第十二章第十条第二款规定，“每一缔约方应当努力避免对电子交易施加任何不必要的监管负担”。第十二章第十五条第二款规定，“任何缔约方不得阻止其他缔约方的投资者为进行商业行为而通过电子方式跨境传输信息”。

第三，RCEP 试图减少数据存储本地化对跨国投资者的负担。其第十二章第十四条第二款规定，“缔约方不得将要求涵盖的人使用该缔约方领土内的计算设施或者将设施置于该缔约方领土之内，作为在该缔约方领土内进行商业行为的

条件”。

第四，为了提高数据监管的透明度，RCEP 第十二章第八条第四款规定，“缔约方应当鼓励法人通过互联网等方式公布其与个人信息保护相关的政策和程序”；其第十二条则进一步要求每一缔约方尽快公布与电子商务有关的监管措施。

第五，在数据监管规则的协调和统一方面，RCEP 建议缔约方借鉴现有的国际规范。其第十二章第八条第二款规定，“在制定保护个人信息的法律框架时，每一缔约方应当考虑相关国际组织或机构的国际标准、原则、指南和准则”；第十条第一款规定，“每一缔约方应当在考虑《联合国国际贸易法委员会电子商务示范法（1996 年）》《联合国国际合同使用电子通信公约（2005 年）》，或其他适用于电子商务的国际公约和示范法基础上，采取或维持监管电子交易的法律框架”。换言之，缔约国期望，各方应努力使本国的数据监管法律框架与国际普遍通行的规范靠拢和兼容，以提高监管措施的可预见性与稳定性，降低商业主体的合规成本。^①

综上所述，在数字经济与数据资本日益发展的背景下，RCEP 的签署生效对我国来说是积极参与全球规则构建的新起点，这些规定对于进一步完善我国关于数据跨境流动的国内法制，促进形成全球数字贸易协定共识，具有启示意义。

^① RCEP 能否促成亚太版 GDPR，《中国外汇》2021 年第 19 期，作者：曾磊

3.4.2 DEPA 数据要素相关的内容

《数字经济伙伴关系协定》(Digital Economy Partnership Agreement, DEPA)由新加坡、智利、新西兰三国于2020年6月12日线上签署生效,该数字贸易协定旨在加强三国间数字贸易合作并建立相关规范。^①

DEPA的具体内容包括16个模块:初步规定和一般定义、商业和贸易便利化、数字产品及相关问题的处理、数据问题、广泛的信任环境、商业和消费者信任、数字身份、新兴趋势和技术、创新与数字经济、中小企业合作、数字包容、联合委员会和联络点、透明度、争端解决、例外和最后条款。其中模块4提到了个人信息保护、通过电子手段进行的跨境数据流动、计算机设施的位置等数据要素相关内容,此外,DEPA还提出了一系列创新性的数据议题,为全球数据治理提供了最新的关注点。

(1) 模块4中数据相关内容

在DEPA的模块4中,与数据要素相关的内容包括个人信息保护(第4.2条)、跨境数据流动(第4.3条)和计算设施的位置(第4.4条)部分。

在个人信息保护部分,DEPA构建了10条规则,从倡导性规则、构建个人信息保护相关法律应该考虑的关键原则、非歧视性原则及信息保护公开、信息保护机制的兼容性和数

^① 刘向东. 积极加入DEPA,中国打造数字贸易新引擎[J]. 中国报道,2023,(02):64-65.

据保护信任标志等方面，对缔约方在个人信息保护方面提出了全面且兼具深度的承诺要求。虽然提出了“限制收集、数据质量、目的规范、使用限制、安全保障措施、透明度、个人的参与、问责制”八个关键原则，但在个人信息跨境流动的限制问题上做了保留，没有规定对个人信息跨境流动进行限制要遵守必要性原则。^①

在跨境数据流动的问题上，DEPA 通过三项规定，承诺有约束力的跨境数据自由流动。第一项采用授权缔约国对跨境数据流动有本国的监管要求。第二项和第三项要求缔约国既要允许跨境数据流动，也可以在不构成“不合理歧视或贸易限制”或“过度采取管制”的前提下，采用出于“合法公共政策目标”的跨境数据流动管制措施，这保留了缔约方对“跨境数据自由流动”进行管制的自主空间。^②

在计算设施的位置问题上，DEPA 采用了富有约束力的措辞进行承诺，要求不得强制将数据存储设施设置在当地，并规定了监管例外和公共安全例外。与此同时，该款项提出缔约方在以下特定情况下可以限制履约，一是考虑各方监管要求^③，二是不得禁止出于“合法公共政策目标”的制约行为。

（2）创新性数据议题

^① 靳思远. 全球数据治理的 DEPA 路径和中国的选择[J]. 财经法学, 2022, (06):96-110.

^② 陈寰琦, 陆锐盈. DEPA 数据安全规则解析及对中国的启示——基于和 CPTPP/USMCA/RCEP 的比对[J]. 长安大学学报(社会科学版), 2022, 24(02):22-31.

^③ 该项采用软性措辞“may”，不具备强制约束力.

首先，在数字贸易便利化方面，DEPA 首倡电子发票、物流和快递等议题，提倡缔约国努力实现数据交换系统的互联互通，努力构建国际公认的数据开放标准，以提升数字贸易的效率、降低交易成本。

其次，DEPA 要求缔约方认识到在个人或企业数字身份方面的合作将有利于区域和全球互联互通，构建数字身份的安全和可互操作的标准会使消费者因数字身份被欺诈案件减少，企业受益于电子方式可以进行更高效的交易。

再次，跨界数据流动和数据共享能够实现数据驱动的创新，DEPA 鼓励缔约国通过监管“沙盒”等方式进行合作，实现跨国界的数据驱动创新以促进新产品和服务的开发。中小企业也应当通过创建免费且可公开访问的网站实现跨国企业之间信息的互联互通，通过举办数字中小企业对话等活动促进企业合作。

最后，DEPA 鼓励缔约国开放政府数据，为公众获取和使用政府信息提供便利，并可促进经济和社会发展、竞争力提升和创新。^①

3. 4. 3 CPTPP 与数据跨境流动相关的规则

全面与进步跨太平洋伙伴关系协定（简称 CPTPP），是美国退出跨太平洋伙伴关系协定（TPP）后该协定的新名字。2018 年 12 月 30 日该项协定正式生效，截至 2023 年 1 月，

^① 靳思远. 全球数据治理的 DEPA 路径和中国的选择 [J]. 财经法学, 2022, (06):96-110.

签署国家有日本、加拿大、澳大利亚、智利、新西兰、新加坡、文莱、马来西亚、越南、墨西哥和秘鲁。

CPTPP 是全球范围内最早生效的新一代数字贸易规则，确立了限制数据本地化、保护个人信息、鼓励数据跨境自由流动、保护源代码等高标准规则。这些规则体现了 CPTPP 旨在遏制数据保护主义、鼓励数据自由流动，代表着保护和促进数字贸易的高水平。

CPTPP 中与数据跨境流动有关的规则主要包括第 14.13 条“计算设施的位置”、第 14.11 条“通过电子方式跨境传输信息”和第 14.8 条“个人信息保护”。其中，第 14.13 条是关于限制数据本地化措施的规定，第 14.11 条直接以数据跨境流动为规制对象，第 14.8 条则涉及数据流动中的个人信息保护问题。^①

在对数据本地化存储的规定方面，CPTPP 第 14.13 条第 2 款规定不得将计算机设备或数据储存器设施置于本国领土作为从事经营的条件，因而被称为禁止数据本地化条款。禁止缔约国要求他人或其他缔约国提供软件中源代码，以此作为进口、销售或使用该软件的条件，强化对大众市场软件源代码知识产权的保护。^②但基于缔约方“合法公共政策目标”，14.13 条的第 3 款做出了例外规定，从目的、方式、限度三个维度衡量缔约方，只有在同时满足规定时可以采取

^① 黄秋红, 李雅颖. 对接 CPTPP 数据跨境流动规则研究[J]. 南海法学, 2022, 6(01):115-124.

^② 全毅. CPTPP 与 RCEP 协定框架及其规则比较[J]. 福建论坛(人文社会科学版), 2022, (05):53-65.

或维持数据本地化措施。

在对数据跨境流动的要求方面，CPTPP 规定，每一缔约方应允许通过电子方式跨境传输信息，包括个人信息，如这一活动用于涵盖的人开展业务。^①第 3 款则与数据本地化措施限制例外一样，缔约方可以在符合目的、方式、限度的基础上，实施或维持限制数据传输的措施。

个人数据作为跨境流动数据的重要组成部分，数据流动必然涉及个人信息的保护问题。根据 CPTPP 第 14.8 (2) 条，缔约方应承担制定或维持电子商务用户个人信息保护法律框架的强制性义务。考虑到不同缔约方之间的文化差异和立法水平，CPTPP 允许缔约方采用不同的法律方式，例如制定个人信息、个人数据保护专门法或涵盖隐私保护的特定部门法等法律框架。^②但缔约方在个人信息保护规则设置上应参考相关国际机构的指南和原则和强化不同信息保护体制之间的兼容性。^③

^① 孙南翔. CPTPP 数字贸易规则:制度博弈、规范差异与中国因应[J]. 学术论坛, 2022, 45 (05) : 44-53.

^② 黄秋红, 李雅颖. 对接 CPTPP 数据跨境流动规则研究[J]. 南海法学, 2022, 6 (01) : 115-124.

^③ 董静然. 数字贸易的国际法规制探究——以 CPTPP 为中心的分析[J]. 对外经贸实务, 2020, (05) : 5-10.

第四章 探索建立数据产权制度、推进技术发展

根据数据的属性和数据生成来源，数据主要分为公共数据、企业数据、个人数据。以上数据要根据其来源和生成特征，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。数据产权制度最大的特征是“去所有权化”，淡化数据所有权，强化数据产权，聚焦数据资源持有权、数据加工使用权和数据产品经营权的“三权分置”的数据产权制度，促进公共数据、企业数据、个人数据分类分级确权授权使用机制。因此，应重点建立数据资源持有权、数据加工使用权、数据产品经营权，“三权分置”的产权运行机制。

数据在不同的应用场景、不同的生产环节中起着不同的作用，也会衍生出不同的权利，很难用一种单一的标准对所有场景下的数据进行统一的确权。由此，有必要设计数据产权结构性分置制度，以达成不同场景、不同层次下清晰的数据权属共识。

“数据二十条”明确提出，要探索数据产权结构性分置制度。主要是建立公共数据、企业数据、个人数据的分类分级确权授权制度。数据分级分类授权机制可推动数据快速进入数字经济的生产活动之中，不仅使各类数据主体对数据的获取和利用变得合理合法，也能减少数据的交易成本。

同时，“数据二十条”对数据产权的技术提出更高的要求。公共数据方面，提出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、核验等产品和服务形式向社会提供。个人信息数据方面，要求创新技术手段，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。

借助数字技术工具进行一系列的采集、筛选、分析、计算等复杂工作流程，才能助力不具备价值形态的杂乱零散的原始数据形成数据要素资源，而数据产权的技术发展将推动数据产权制度的建立。

第一节 推动实施公共数据确权授权机制

4.1.1 公共数据的界定及使用

4.1.1.1 公共数据的定义

作为一个技术型、工具性概念，公共数据并不存在固有的内涵和外延^①。目前，国家立法层面也尚未对公共数据进行明确界定。不过随着地方政府相继出台公共数据共享开放的规范或政策，研究的不断加深，企业不断探索实践，人们对于公共数据初步形成共识。以《上海市数据条例》^②为例，公共数据被定义为：本市国家机关、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

^① 沈斌,黎江虹.论公共数据的类型化规制及其立法落实[J].武汉大学学报(哲学社会科学版), 2023 (1):67-77.

^② 上海市人民政府：《上海市数据条例》(2021-11-29)，
<https://www.shanghai.gov.cn/nw12344/20211129/a1a38c3dfe8b4f8f8fcba5e79fbe9251.html>

过程中收集和产生的数据。整理深圳^①、浙江^②等地出台的政策发现，对于公共数据的认定基本类似，主要采取以下复合标准：

一是主体要件，收集和产生公共数据的机构应当具有公共属性，“公共数据”的持有者（主体）包括政府、管理公共事务的组织和提供公共服务的运营机构等；二是行为要件，公共数据是前述机构在履行公共管理和服务职能过程中所收集和产生的（政府部门、水电燃气企业等采集的数据大多符合前述标准，而互联网平台企业掌握的数据则不属于公共数据）；三是目的要件，公共数据的共享、开放、授权经营或交易，必须有利于促成公共利益，而不是谋取个人或少数群体的利益（“数据正义性”，公共数据更充分地为广大人群所获取和利用能够更多维度地实现数据资源的价值同时有利于防范数据的“部门化”和“权力化”）；四是公共数据从数据的收集到经过加工产生的数据，需经过管理相对人和接受公共服务运营组织提供公共服务产品的多方利益相关主体的参与，其中包括各级党政机关、个人、企业和其他组织。

从公共数据服务的范围看，公共数据主要有两大类，一类用于公共治理和公益事业的公共数据；另一类是用于产业

^① 深圳市人民政府：《深圳经济特区数据条例》（2021-06-29），
http://www.szrd.gov.cn/szrd_zlida/szrd_zlida_flfg/flfg_szfg/content/post_706636.html

^② 浙江省人民政府：《浙江省公共数据条例》（2022-01-21），
https://www.zj.gov.cn/art/2022/2/11/art_1229641548_59709272.html

发展和行业发展的公共数据。前者主要是基于公益目的，应当无偿使用和分享，后者是与社会经济发展有关的数据，可以探索有偿使用。为此，“数据二十条”提出，推动用于公共治理、公益事业的公共数据有条件无偿使用，探索用于产业发展、行业发展的公共数据有条件有偿使用。

因此，公共数据应包括以下几层含义，国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、供气、公共交通等公共服务运营单位，在依法履行职责或者提供公共服务过程中收集、产生的数据，并且相关数据的共享、开放、授权经营或交易，必须有利于促成公共利益。

4.1.1.2 公共数据、政府数据及政务数据概念解析

公共数据、政府数据、政务数据这三个概念是在公共数据开放法律文件和开放实践中较为常见的相似概念，三者概念范围存在交叉重叠，并且各地的相关数据开放法规、规章对上述概念均有采用。

目前，我国关于公共数据与政府数据的概念范围主要存在两种观点：一是，以季统凯为代表的学者认为政府数据是公共数据的一部分，“ $\text{公共数据} = \text{政府数据} + \text{公共机构数据}$ ”，“政府数据是各级人民政府及其职能部门以及依法行使行政职权的组织在其管理或提供公共服务过程中制作、获得或拥有的数据，不包括提供自来水、电力、公共交通等公共机构的数据”，将提供公共服务、履行公共管理的企事业单位

排除在外^①；二是，以郑磊为代表的学者认为政府数据有狭义和广义之分，广义的政府数据即为公共数据。“狭义的政府数据是指行政机关依法履职过程中制作或者获取的数据资源，广义的政府数据还包括企事业单位中与政府项目和服务相关、并具有重大公共利益的数据”^②，契合开放的价值追求，地方政府数据开放文件中也较多采用“公共数据”概念。政府数据在主体要件上更狭窄一些，比如公共事业单位的数据不是政府数据，但可能是公共数据。

政务数据主要是指有关行政机关主动在履行职责过程中收集、存储和管理的具有公开性的政务信息数据，不包括自然汇聚而成的具有免费公开性的政府数据^③。政务数据比政府数据的范围更小，政务数据、政府数据、公共数据三者的概念范围递增，属于被包含关系。王春晖认为，从数据服务的社会属性看，“公共数据”的内涵更丰富，而政务数据相对狭窄，“公共数据”的外延比较广，其中就包含了“政务数据”，因此使用“公共数据”的概念更符合公共数据服务的社会属性和公益目的。

4.1.1.3 公共数据使用的主要方式：共享、开放利用及授权运营

^①季统凯、刘甜甜、伍小强：《政府数据开放：概念辨析、价值与现状分析》，《北京工业大学学报》2017年第3期，第328页

^②郑磊：《开放不等于公开、共享和交易：政府数据开放与相近概念的界定与辨析》，《南京社会科学》2018年第9期，第86页

^③李爱君：《数据权利属性与法律特征》，《东方法学》2018年第3期，第67页

“数据二十条”指出，加强公共数据汇聚共享和开放开发。在公共数据的使用方面，梳理各地相关实践发现，公共数据使用的主要方式有三种：公共数据共享、公共数据开放与利用、公共数据授权运营。

截至 2022 年底，我国多地已将数据要素市场建设列入“十四五规划”，北京、上海、广东、贵州等二十余地制定了“数字经济发展规划”或“数字经济行动计划”，推动数据要素市场培育，促进数据要素价值释放。在立法方面，各地在国家数据立法框架下充分发挥试点优势，截至 2022 年底，已有 23 个省市公布了数据相关的条例或草案，不断从法律层面探索数据权益保障、数据流通利用、数据安全管理等环节的解决思路，同时密集发布的政策文件也为公共数据的探索注入活力（见表 5）。

表 5 部分地方立法条例或管理办法

时间	地区	政策
2021 年 1 月 28 日	北京市	《北京市公共数据管理办法》
2021 年 6 月 29 日	深圳市	《深圳经济特区数据条例》
2021 年 11 月 25 日	上海市	《上海市数据条例》
2021 年 11 月 25 日	广东省	《广东省公共数据管理办法》
2021 年 12 月 14 日	江苏省	《江苏省公共数据管理办法》
2022 年 1 月 21 日	浙江省	《浙江省公共数据条例》

数据来源：部分省份政府官网

（1）公共数据的共享：无条件共享、受限共享和不共享数据

公共数据共享，即公共数据在政府体系内部不同部门、不同层级之间的流动。各地关于公共数据共享方面，基本以共享为原则，不共享为例外。《浙江省公共数据条例》规定，公共数据按照共享属性分为无条件共享、受限共享和不共享数据。其中，列入受限共享数据的，应当说明理由并明确共享条件。列入不共享数据的，应当提供明确的法律、法规、规章或者国家有关规定依据。《上海市数据条例》规定，建立以共享需求清单、责任清单和负面清单为基础的公共数据共享机制。对未列入负面清单的公共数据，可以直接共享，但不得超出依法履行职责的必要范围。对未列入公共数据目录的公共数据，市级责任部门应当在收到共享需求之日起十五个工作日内进行确认后编入公共数据目录并提供共享。

（2）公共数据的开放：无条件开放、有条件开放和非开放

公共数据开放与利用，即各级政府面向社会免费开放公共数据，属于公共数据向政府体系外部流动。各地关于公共数据开放基本遵循分类分级、需求导向、安全可控等原则，在法律、法规允许范围内最大限度开放。同时，公共数据按照开放类型分为无条件开放、有条件开放和非开放三类。涉及个人隐私、个人信息、商业秘密、保密商务信息，或者法律、法规规定不得开放的，列入非开放类；对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据，

列入有条件开放类；其他公共数据列入无条件开放类。一些地区依托城市大数据中心建设统一、高效的公共数据开放平台，组织公共管理和服务机构通过该平台向社会开放公共数据，根据公共数据开放类型，提供数据下载、应用程序接口和安全可信的数据综合开发利用环境等多种数据开放服务。

（3）公共数据的授权运营：国有资本运营公司、特许经营

公共数据授权运营，即政府授权一定主体通过市场化方式运营公共数据，促成外部主体的使用。多地提出建立公共数据授权运营机制，提高公共数据社会化开发利用水平，组织制定公共数据授权运营管理辦法，明确授权主体，授权条件、程序、数据范围，运营平台的服务和使用机制，运营行为规范，以及运营评价和退出情形等内容。梳理相关文件还发现，目前很多地方都是通过国资公司开展政府数据授权运营，运行模式存在差异。北京、贵州、山东、广东等地采取了国有资本运营公司方式，海南、浙江等地采取了特许经营方式，江苏、福建等地采取了以上两种方式。

4.1.2 公共数据现有产权机制现状

4.1.2.1 公共数据产权机制的探索成果

探索公共数据的有条件有偿使用，是赋予公共数据要素价值，激活公共数据价值的重大举措。公共数据的有条件有偿使用，应重点聚焦实体经济领域和民生服务领域，如生产

制造、科技研发、金融服务、商贸流通、航运物流、现代农业，以及公共卫生、医疗卫生、文化旅游、交通物流、健康养老等。无论是公共数据的无偿使用还是有偿使用，均要附带一定的条件，如需要经过公共数据提供部门的审核同意，并与公共数据提供单位签订公共数据无偿或有偿使用协议，明确公共数据利用的方式、使用范围，以及安全保障等。

（1）公共数据开放平台建设方面取得良好成效

建立公共数据开放平台是各地推进数据开放的主要手段。近年来，各地在公共数据开放平台建设方面积极推进，取得了良好成效。《中国地方政府数据开放报告（2022）》数据显示，截至2022年10月，我国已上线了208个政府数据开放平台，其中省级平台21个（含省和自治区，不包括直辖市和港澳台），城市平台187个（含直辖市、副省级与地级行政区）（见图3），我国74.07%的省级（不含直辖市）和55.49%的城市（包括直辖市、副省级与地级行政区）已上线了政府数据开放平台。

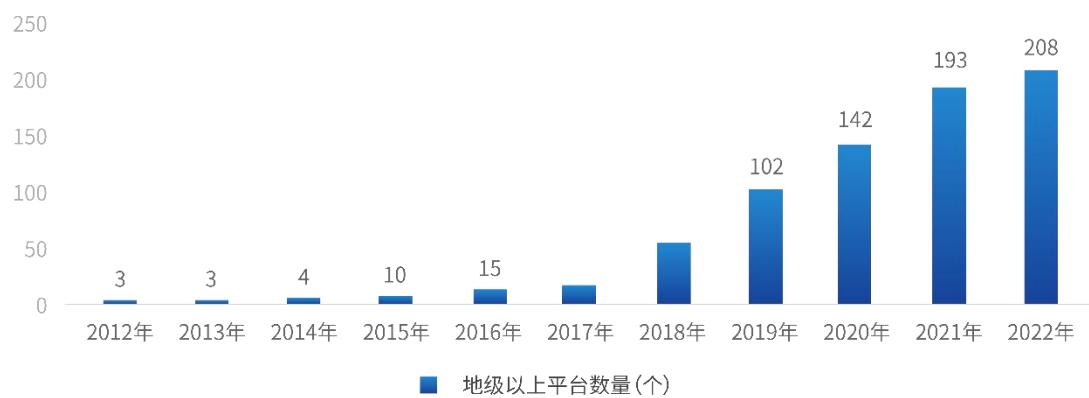


图 3 我国地级以上数据开放平台数量

数据来源：《中国地方政府数据开放报告（2022）》

各省市的数据开放平台建设逐渐完善，数据开放程度逐年提升。根据部分地区公共数据开放平台官网数据显示，截至 2023 年 1 月 11 日，北京市公共数据开放平台已开放 115 个单位，16021 个公共数据集，582444 个数据项（其中无条件开放共计 576673 个数据项，有条件开放共计 5771 个数据项），71.86 亿条公共数据；上海市公共数据开放平台已开放 50 个数据部门，131 个数据开放机构，5356 个数据集（其中 2244 个数据接口），67 个数据应用，43908 个数据项，20.09 亿条公共数据；深圳市公共数据开放平台已开放 50 个市级部门/区，开放目录总量 3360 个，数据项总量 30465 项，14.27 亿条公共数据。

（2）各地数据交易所相继成立、升级优化

大数据交易所是数据市场化流通的重要载体，发挥促进资源整合、规范交易行为、增强数据流动性、推进标准制度建立的关键作用。2020 年以来，北京、上海、深圳、广州等一线城市的 data 交易所陆续成立（见表 6），贵阳大数据交易所也重组升级，新型数据交易所从之前主要扮演“撮合交易”的角色向全生命周期的服务平台转型，同时普遍采用国有资本入股、政府指导、市场化运营的方式，既可以发挥政府政策和资源优势，有利于保障数据的权威性和安全性，也能够确保市场化机构的参与积极性。

表 6 我国数据交易所相关信息

挂牌	交易所	定位
----	-----	----

时间	名称	
2021年3月	北京国际大数据交易所	打造国内领先的数据交易基础设施和国际重要的数据跨境交易枢纽，助力北京市在数据流通、数字贸易、数据跨境等领域发挥创新引领作用，成为全球数字经济的标杆城市。
2021年11月	上海数据交易所	重点培育发展“数商”新业态，围绕打造全球数据要素配置的重要枢纽节点的目标，构建“1+4+4”体系：紧扣建设国家级数据交易所“一个定位”；突出准公共服务、全数字化交易、全链生态构建、制度规则创新“四个功能”；体现规范确权、统一登记、集中清算、灵活交付“四个特征”。
2022年9月	广州数据交易所	采用“一所多基地多平台”体系架构运营，为区域数据交易服务设立多基地，鼓励各类中小企业、高新技术企业、服务创新企业的数据产品与服务，数字资产，以及算力资源等数据能力，基于“无场景不交易”的要求进场交易。
2022年11月	深圳数据交易所	以建设国家级数据交易所为目标，构建数据要素跨域、跨境流通的全国性交易平台，探索适应中国数字经济发展的数据要素市场化配置示范路径和交易样板。

数据来源：部分数据交易所官网

（3）公共数据的授权运营模式涌现多项创新举措

随着公共数据从以开放为中心到以开放和利用为中心的转变，平台（网站）开发利用与协议开发利用都无法为市场主体提供高价值的数据开放和高品质的数据供给，为社会化、市场化的公共数据利用提供充足的制度供给，亟需引入一种新的制度来破局，授权运营制度应运而生。公共数据授权运营制度作为一种创新性的公共数据社会化、市场化利用方式，一方面，以公共数据运营平台为载体，确保高价值的数据利用风险可控；另一方面，给公共数据“提质”，为市场主体提供高品质的数据利用供给。

我国公共数据授权运营已经形成三种主要模式：一是行业主导模式，主要由垂直领域行业管理部门授权和指导其下

属机构承担本领域公共数据运营平台建设、场景开发和市场运营；二是区域一体化模式，主要由地区数据管理机构以整体授权形式委托数据运营机构整体开展区域内公共数据运营平台建设和市场运营；三是场景牵引模式，主要由地区或行业数据管理机构在公共数据资源统筹管理基础上，基于特定应用场景通过针对性、专业化分类授权引入专业数据运营机构，分领域、分场景激活公共数据价值的运营模式。

场景案例 1

（1）场景背景

公共数据的授权运营模式的应用，以公共数据为载体，建设平台，将公共数据与产业相结合，推动当地产业的发展。湖北省秭归县为推动脐橙全产业链联动、高质量发展，与人民数据合作，定制化开发“脐橙数据库及大数据平台”。实现公共数据与产业的融合，也为公共数据的利用带来了新的模式探索路径。

（2）场景建设

秭归脐橙数据库及大数据平台实现成果数字化、数据资产化、投融资数据化、产业可视化，达到“一张图看懂秭归县脐橙产业发展”的精准化、精细化管理目标，也实现政府与柑农“面对面、键对键”，强化乡村治理。

脐橙数据库及大数据平台包括展示系统、辅助决策系统以及后台管理系统。展示系统展示脐橙种植分布、品种、产

量、长势、种植适宜区、种植区域耕地质量、核心主产区以及新型经营体等数据；辅助决策系统能够监测气候变化、脐橙价格，为秭归县相关部门制定应对措施提供数据支撑；后台管理系统可以促进全县脐橙的标准化管理，政府部门可利用大数据平台发送技术培训、通知公告等相关信息，确保柑农及时接受到消息，提高效率，也可在 web 端上传新数据。



图 4 秭归脐橙大数据平台展示

(3) 场景成效

秭归脐橙大数据平台聚焦秭归核心脐橙产业，将农业土地资产、农产品、农户等数据要素资产化，推进秭归农业农村数据资产管理稳定实施；推进农业农村数据资源以通促产的方式转变，激活农业数据资产的融资潜能；推进空天地一体化技术在农业生产中的应用，提升数字化生产能力。

秭归脐橙大数据平台还入驻人民数据联合农业农村部大数据发展中心共同研发的农业农村大数据公共平台基座。通过农业农村的大数据管理服务平台，对“智慧农业”业务

数据进行全面梳理，从脐橙产业出发，建立起覆盖，实现数据全采集、业务全监测、主体共分享，推进秭归脐橙产业高质量发展，为全国数字化赋能农业产业链探索“秭归样板”。

各地探索公共数据授权运营的实践中推出多项创新举措：一是以地方法规形式构建公共数据授权运营的基本规则。比如，上海、北京、浙江等诸多地区在地方数据条例或者数字经济条例中明确提出“建立公共数据授权运营机制”，并从制定具体管理办法、公共数据使用范围、所形成的数据产品和服务的交易规则、安全要求及合规评估等方面进行初步规定。二是探索公共数据资源管理制度。比如，广东启动公共数据资产凭证化改革试点，发布全国首张公共数据资产凭证，探索和拓展公共数据资产凭证的应用场景，推动公共数据资产登记与评估，初步形成以凭证来承载资产、声明权益、治理数据、保障合规的数据资产凭证解决方案。三是，探索建立首席数据官或数据专员制度，通过赋予负责本地区或本部门的统筹数据管理和融合创新、数据运营机构建设、数据技能与安全培训等职责，形成上下贯通的首席数据官组织体系，提高数据治理和数据运营能力。

公共数据授权运营也加快了产业数字化转型。数字经济与实体经济融合的过程也是数据与传统产业融合的过程，公共数据授权运营将释放数据的倍增叠加效应，为经济发展注入活力源泉。

场景案例 2

(1) 场景背景

为解决因信用数据缺失导致的信息不对称的小微企业融资难、融资贵难题，北京创新打造了“金融公共数据专区”，依托北京市大数据平台，汇聚了企业税务、社保、医保、公积金、政府采购等 20 多亿条政务数据，涉及近 30 个部门，帮助小微企业获取金融“活水”。

(2) 场景建设

金融公共数据专区是北京市大数据平台的组成部分，作为金融公共数据汇聚的核心载体、运营管理的平台和社会应用的统一接口，承担金融公共数据统进统出、制度化管理、创新社会应用的职能。北京市金融公共数据专区主要提供信用信息查询、准入分析、风险洞察、竞争力分析、企业守信分析等七大类公共数据产品与服务。



图 5 北京市金融公共数据专区场景案例展示

(3) 场景成效

从运营绩效来看，北京金融公共数据专区累计为银行等金融机构提供服务 5000 多万次、支撑 30 余万家企业申请金融服务金额超 2000 亿元。同时，作为北京市大数据平台的组成部分和数据输出应用的“统一接口”，北京市金融公共数据专区的实践创新，也为全国各地推进公共数据共享应用，促进公共数据授权运营加速发展、探索市场化机制和培育数据要素市场提供了借鉴。^①

4.1.2.2 推进公共数据产权机制存在的难点

(1) 公共数据确权面临困境

公共数据与其它社会产品相比，带有显著的公共资源特征，数据的开放和共享符合公共利益，为了活跃大数据市场，多地采取与平台合作的方式，将数据投放到数据平台，推动公共数据开放。大数据交易中，公共数据起着举足轻重的地位，是数据确权中绕不开的话题。目前，学界对数据权利的成立与否存在学术争议，否定论者认为数据不是一种民事权利客体，肯定论者认为公民对其个人数据享有人身性权利和财产性权利^②。根据公共数据权利理论，“公众享有对政府数据知情或知悉的权利、对政府数据开放请求的权利和对政府数据使用的权利”。^③

^① 穆勇.：《数据要素流通交易保护》(2021-09-13)，https://www.sohu.com/a/489565973_121124373

^② 何渊：《数据法学》，北京大学出版社 2020 年版，第 81 页

^③ 朱峰：《政府数据开放的权利基础及其制度构建》，《电子政务》2020 年第 10 期，第 119 页

在公共数据所有权的实践方面，各地常常把公共数据作为政府资产进行管理和运营，在事实上将公共数据归政府所有。但是现有法律和制度文件中并没有明确公共数据属于国有资产。自 2016 年以来，福建、重庆等地先后通过出台管理办法的方式，明确政务数据资源归属国家或当地人民政府所有。其中，《重庆市政府数据资源管理暂行办法》第 4 条第 1 款规定“政务数据资源属于国家所有”，《福建省电子政务建设和应用管理办法》第 9 条规定“应用单位在履行职责过程中产生的信息资源……属于国家所有。”

然而，关于公共数据的归属问题，对于公共数据，个人、法人和其他组织分别享有哪方面的权利，各权利主体如何行使自己的权利和保护自己的利益，以及如何获得数据要素的合理报酬等问题，目前尚未有国家层面的法律予以明确。同时，我国公共数据权属立法的市场基础还比较薄弱，市场上具有指导性意义的数据权利归属案例不足且局限性较大，公共数据领域案例更是鲜见。

在公共数据使用权的实践方面，虽然各地能够自主使用自身收集和产生的数据，但是仍面临两方面困境：一是政府部门使用其他部门提供数据的可使用程度尚未明确。按照现有的公共数据共享政策逻辑，公共数据应尽可能实现在部门之间的最大程度共享，政府部门以保护商业秘密和个人隐私

为由不进行数据共享并不符合政策要求。但是，目前也确实存在公共数据共享滞后，主管部门难以有效掌控等问题。由于主管部门需要对数据的安全负责，共享后出现问题也需要承担责任，进一步加剧了部门不愿意共享数据的现象。二是政府部门在开放数据时参照的标准依据尚未明确。按照现有的公共数据开放政策逻辑，开放数据不能涉及国家秘密、商业秘密、个人隐私，大大减少了可供开放的数据数量。尽管可以通过脱敏方式推进数据开放，但需要增加投入，因此进一步降低部分部门的积极性。

（2）公共数据开放不足、范围不清

第一，数据开放有限、生态难以形成。公共数据开放的目标是在安全可控的前提下尽可能多地开放，但是公共数据的实际开放数量并不理想。2021年，复旦大学数字与移动治理实验室发布的《中国地方政府数据开放报告（指标体系与城市标杆）》给出了十个标杆城市，指数得分最高的上海市，为67.75分。分析四个一级指标的失分比例发现：数据层失分占比最高，其中最高得分是济南市（29.31分），最低得分日照市（22.92分），将近比数据层总分45分少一半。^①数据层能够直接反映公共数据开放的数量和质量状况，表明目前公共数据开放的最大困境是开放有限。

^① 复旦大学数字与移动治理实验室：《中国地方政府数据开放报告（指标体系与城市标杆）》（2021年7月26日），<https://xueqiu.com/1987269200/192280382>

第二，公共数据目录普遍处于不公开状态，导致公共数据开放陷入“口惠而实不至”的境地。数据目录是公共数据的“元数据”，是分级分类管理的核心，制定公共数据目录、采取分级分类管理和差异化开放的策略是实践中的通行做法。通过数据目录，可以一目了然地了解到公共部门在履职过程中以及委托第三方收集和产生了哪些数据。数据目录结构中一般还包括数据来源、更新频率、安全分级以及共享开放属性等关键要素信息。其中，数据开放属性又可细分为非开放、有条件开放和无条件开放等（一般来说，涉及商业秘密、个人隐私，或根据法律法规不得开放的，归入非开放类。对访问者的数据安全和处理能力要求较高，以及数据时效性较强或者需要持续获取的情况，则列入有条件开放。除此以外，属于无条件开放类）。^①

但是，数据目录并不是数据开放清单（数据开放清单主要包括数据开放范围、开放类型、开放条件和更新频率等），地方数据立法中不乏制定、公布数据开放清单的相关规定，但鲜有地方立法把公共数据目录作为公开的对象。开放清单的信息量、重要性远不及数据目录。地方政府手中握有大量公共数据，但数据目录的具体情况仍处于混乱不清或刻意保密的状态，公众无从知晓究竟存在哪些公共数据资源，更无

^① 《浙江省公共数据开放与安全管理暂行办法》第14条，《深圳经济特区数据条例》第48条等

法监督是否有该开放而未开放的情况。如此一来，便极易滋生暗箱操作和权力寻租等问题。

（3）公共数据授权运营面临障碍

第一，公共数据授权范围不明确。公共数据授权运营牵涉数据著作权的许可、转让等产权流转问题，且哪些数据可以授权运营并没有明确的规定。目前仅有贵州、浙江、天津等少数地方提出开展政府数据分类分级，且分类分级工作刚刚起步，尚未实施落地。虽然有的政策提出以分类方式开展数据差异化授权，但实践中仍采取单一的授权方式，大多数平台没有制定授权协议。如何科学分类，明确数据授权范围，成为阻碍公共数据授权运营的一大障碍。

第二，数据授权与隐私保密难平衡。20世纪60—80年代，美国、英国、德国等西方发达国家开始出台关于信息公开、数据保护等方面国家层面的法律，强调公民有权利要求政府机构提供相关信息，同时政府也有义务保护公民的个人隐私信息。^①在数据开放与隐私保护两者之间的冲突方面，我国制定《个人信息保护法》保护个人信息隐私，但在国家层面公共数据开放利用的法律还有待进一步完善，大多是一些导向性的文件或者非约束性的政策意见，在公共数据授权运营的实践过程中，存在数据授权与隐私保密平衡难的问题。

^① 宋卿清，曲婉，冯梅红：《国内外政府数据开发利用的进展及对我国的政策建议》，《政策与管理研究》，2020（35），742—750页

第三，公共数据授权运营监管机制亟需完善。授权运营的风险来自公共管理和服务机构将公共数据的管理开发权限交由私人主体。人们既担心公共管理和服务机构会不断将其责任转交给私主体，甚至沦为其实行垄断的工具，也担心市场主体的“利己主义”会妨碍公共管理和服务机构所代表的公共导向性能^①。要建立与授权运营相配套的监管机制仍需要重点解决以下两个问题：一方面，公共管理和服务机构的监管定位问题。另一方面，公共管理和服务机构与其他监督主体之间的制度安排影响着监管效能的提升。虽然目前部分地方规定了公共管理和服务机构以及利益相关者的数据安全保护义务，但是并未说明公私主体间如何避免监督上的交叉重叠，进而形成监管合力。

4.1.3 公共数据产权机制应遵循的原则

4.1.3.1 践行“原始数据不出域、数据可用不可见”

“数据二十条”提出：“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、核验等产品和服务形式向社会提供。”这主要是依托联邦学习以及多方安全计算等隐私计算技术，形成“原始数据不出域，数据不动价值动”的数据增值开发利用新范式，这些新范式可以实现以模型、核验等

^① 塔格特 M：《行政法的范围》，中国人民大学出版社，2006，4—5页

产品和服务形式向社会提供有价值的数据，这是公共数据融合创新利用的新方向。

（1）安全是数据流通的重要前提

公共数据流通面临保障个人隐私、数据安全的忧虑，数据的安全流通与数据可信交付成为数据要素市场发展的必要条件。中央政策文件明确提出“原始数据不出域、数据可用不可见”要求，如2022年1月，国务院办公厅发布《关于印发要素市场化配置综合改革试点总体方案的通知》^①，提出要探索“原始数据不出域、数据可用不可见”的交易范式；“数据二十条”指出，要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，对不承载个人信息和不影响公共安全的公共数据，推动按用途加大供给使用范围。政策层面对保护公共利益、数据安全和数据来源者合法权益的重视程度可见一斑。

“原始数据不出域”要求数据持有者保障通过合法手段采集的数据在流通中不脱离掌控，以避免隐私泄露、数据安全隐患。“数据可用不可见”是对于“原始数据不出域”的解决方案，即数据使用者可对原始数据进行加工处理，利用数据价值，但不获得、不掌握原始数据。

（2）对互信难题提出解决办法

^① 中华人民共和国中央人民政府网《国务院办公厅关于印发要素市场化配置综合改革试点总体方案的通知》（2022年01月06日），http://www.gov.cn/zhengce/content/2022-01/06/content_5666681.htm

“原始数据不出域、数据可用不可见”是一道互信难题。针对这一问题，政府部门与行业机构均作出了有效探索：

一是提出“三权分置”的数据产权框架制度。数据产权问题是一直制约数字经济发展的难题，“数据二十条”提出的“三权分置”的形式受到学界和业内的高度评价，新产权运行机制或将给个人、企业和政府部门带来新机遇。中国人民大学信息资源管理学院副教授朝乐门认为，“三权分置”将改变数据流上下游主体之间的竞合关系，从而影响部分数据持有者在产业链中所扮演的角色，并有助于数据加工使用者和数据产品经营者的增加，进一步优化市场竞争机制^①。

二是隐私计算是数据安全流通的技术解法。隐私计算可以通过加密、分片、不传递原始数据等方式大大降低数据泄露和被滥用的风险，是平衡数据利用与安全的重要路径，2022年10月国务院办公厅印发的《全国一体化政务大数据体系建设指南》^②提出“探索利用核查、模型分析、隐私计算等多种手段，有效支撑地方数据资源深度开发利用”。

隐私计算的技术探索和行业应用均已有成果。《隐私计算白皮书（2022年）》指出，2022年，隐私计算在多方安全计算、联邦学习、可信执行环境等被业界视为三大主流技术中迎来了一系列创新与突破：多方安全计算技术可用性进

^① 人民网《数据产权归谁？专家：“三权分置”开创数据要素市场新局面》（2023年1月6日），<http://finance.people.com.cn/n1/2023/0106/c1004-32601274.html>

^② 中华人民共和国中央人民政府网《国务院办公厅关于印发 全国一体化政务大数据体系建设指南的通知（国办函〔2022〕102号）》（2022年10月28日），http://www.gov.cn/zhengce/content/2022-10/28/content_5722322.htm

一步提升，性能优化与场景扩展；联邦学习领域，2022年涌现出大量优秀研究成果，性能、安全、模型效用等关键方向持续探索创新；可信执行环境方面，通过对现有算法协议改造、结合硬件加速能力等方式，实现了数倍到数十倍的性能提升，提高了可用性^①。

在应用层面，近年来，上海数据交易所等交易所对数据沙箱技术均有应用。这一技术属于隐私计算中数据不流出、集中计算路径的代表技术——可信计算平台^②。可信计算平台包括可信执行环境（Trusted Execution Environment，TEE）和数据沙箱技术。国家发展和改革委员会在《加快构建中国特色数据基础制度体系 促进全体人民共享数字经济发展红利》^③中也有所提及：“要建立有效的‘数据沙箱’机制防范化解重大风险。”但隐私计算并非数据产权机制安全保障的全集，《隐私计算白皮书（2022年）》指出，单纯使用隐私计算技术并不能免除取得授权同意义务、达到绝对的匿名化或满足目的限制要求，它并不是为了帮助履行《个人信息保护法》的合规义务而设计的合规工具，而是对于增强数据处理安全性具有积极意义的技术手段^④。

4.1.3.2 建立负面清单制度 “非禁止即允许”

^① 中国经营网《隐私计算产业快速增长 2025年国内市场规模将达百亿元》（2022年12月30日），<http://www.cb.com.cn/index/show/zj/cv/cv135191751265>

^② 经济参考网《“隐私计算”四大技术路径解析》（2021年9月6日），http://www.jjckb.cn/2021-09/06/c_1310171566.htm

^③ 求是网《加快构建中国特色数据基础制度体系 促进全体人民共享数字经济发展红利》（2023年1月1日），http://www.qstheory.cn/dukan/qs/2023-01/01/c_1129246978.htm

^④ 新京报《白皮书：隐私计算可以大大降低数据泄露和被滥用的风险》（2022年12月28日），<https://www.bjnews.com.cn/detail/1672231777168304.html>

关于公共数据的开放，“数据二十条”要求：“依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场，保障公共数据供给使用的公共利益。”因此，政府、管理公共事务的组织和提供公共服务的运营机构要定期制定公共数据开放的重点清单，凡涉及国家安全数据，个人信息，尤其是敏感个人信息，以及企业商业秘密数据，或者法律、法规规定不得开放的数据，均应列入非开放类公共数据清单。

（1）建立负面清单制度的原则

负面清单制度的运行前提是公共数据应无条件共享，共享为原则，不共享为例外。建立负面清单制度助力平衡数据保护与开发的关系，明确公共数据共享的底线和红线，配合“非禁止即允许”原则，增强公共数据产权机制的灵活性。

为便于负面清单制度的运行，让制度规范市场的同时，促进市场活力，建立负面清单制度应遵循以下几个原则：

一是类目需全面，规定需详细。公共数据可能涉及的数据类型包括个人信息、国家信息、商业信息及其他，公开级别包括禁止共享、限制共享和开放共享。负面清单应梳理不同信息类别、不同公开层级的数据范围，为公共数据流通明确规则。上海社会科学院信息研究所副研究员范佳佳认为负面清单应包括：涉及个人隐私的敏感性个人信息；国家安全信息；商业秘密；其他数据等。

二是公开发布，及时更新。为保障数据安全，畅通市场流通，数据管理部门需公开发布负面清单，保证清单可获取、易获取。公开发布方式可参考现行政府信息披露的形式，在政府官网、政务新媒体等平台进行权威公开，保证有需要的行业有关企业和从业者可以低门槛获取负面清单。更新方式有滚动更新和定时更新两种，滚动更新即负面清单随时更新，定时更新即按照既定周期进行调整，考虑到数据市场变化的迅捷，滚动更新更有利于保障数据安全。

（2）负面清单制度的探索

负面清单制度在公共数据领域的开发利用中已有探索。我国首部数据领域的综合性专门立法《深圳经济特区数据暂行条例（草案）》设计了共享负面清单制度^①；2021年6月29日通过的《深圳经济特区数据条例》^②中明确实行公共数据目录管理制度，纳入公共数据共享目录的公共数据，应当按照有关规定通过城市大数据中心的公共数据共享平台在有需要的公共管理和服务机构之间及时、准确共享，法律、法规另有规定的除外。

公共数据共享目录由市政务服务数据管理部门另行制定，并应及时调整。《关于印发要素市场化配置综合改革试点总体方案的通知》也提出“探索制定大数据分析和交易禁

^① 南方新闻网《深圳将出台国内数据领域首部综合性立法 拟设公共数据共享负面清单制度》（2020年12月29日），https://news.southcn.com/node_54a44f01a2/73eeae9197.shtml

^② 《深圳经济特区数据条例》（2021年6月29日），<http://www.sz.gov.cn/attachment/0/980/980196/9835431.pdf>

止清单”。目前的探索中，负面清单不仅有禁止类目，也有限制类目。如《江西省公共数据管理办法》^①明确，对涉及国家安全、商业秘密、保密商务信息、个人隐私、个人信息，或者法律、法规、规章规定不得开放的公共数据，列入不予开放类；对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据，列入有条件开放类；其他公共数据列入无条件开放类。

第二节 推动建立企业数据确权授权机制

“数据二十条”明确要求要推动建立企业数据确权授权机制，对各类市场主体的权责明确界定，为企业数据的流通、交易指明方向。

“数据二十条”提出：“对各类市场主体在生产经营活动中采集加工的不涉及个人信息和公共利益的数据，市场主体享有依法依规持有、使用、获取收益的权益，保障其投入的劳动和其他要素贡献获得合理回报，加强数据要素供给激励。”上述内容有三层含义，一是企业作为市场的主体，在生产经营活动中采集加工的数据，依法享有依法依规持有、使用、获取收益的权益；二是在企业在生产经营活动中收集的数据，除了生产运营有关的数据，还包括个人信息和公共利益数据，但是企业依法持有、使用和获取收益的数据，不应包括个人信息和公共利益数据；三是企业对收集的数据要

^① 《江西省公共数据管理办法》（2022年1月12日），
http://www.jiangxi.gov.cn/art/2022/1/21/art_71157_333.html

进行加工处理才具有要素价值，因此企业要投入资本和人力要素，按照“市场评价贡献、按贡献决定报酬”的原则操作，而国家应依法保障企业投入的劳动和其他要素贡献获得合理回报。^①

根据“数据二十条”要求，聚焦企业数据概念及特征、企业数据现有的产权机制现状，企业数据产权机制运行规则及坚守的原则，企业数据分类分级发展现状及使用原则，助力企业数据释放更多价值。

4.2.1 企业数据的内涵及要点

企业数据是企业赖以生存与发展的重要战略资源，来源于企业运行的各个环节，通过使用者控制、加工、整理、分析、处理，发挥着支撑企业经营决策、服务企业开拓创新的作用，表现出低成本复制性、非消耗性、非排他性、可再生性、可交易性、可联接性等特性。在公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等八大重要行业和领域，企业数据得到一定发展。一些数据交易场所已逐步形成数据登记等确权模式，走出破解“确权难”的第一步，但仍存在相关确权授权法律不够完善、数据流通环节中的各参与主体的利益分配不均衡等问题，以及企业数据难以适用传统的财产权保护制度、过度商业秘密易导致数据垄断等现象。对此，《关键信息基础设施安全保

^① 王春晖,方兴东. 构建数据产权制度的核心要义[J]. 南京邮电大学学报(社会科学版):1-12.

护条例》对八大行业或领域关键信息基础设施的范围、各监管部门的职责、运营者的安全保护义务以及安全检测评估制度提出了更加具体、操作性更强的要求，特别是金融数据和汽车数据领域，需要积极贯彻信息共享、数据安全保护、保障关键信息基础设施安全稳定运行等要求。

4. 2. 1. 1 企业数据的概念及特征

广义上，企业数据是公司概况、产品信息、经营数据、研究成果等信息的集合。这些企业数据一部分由权威部门统一发布，例如统计局、工商局的数据显示，一部分由企业内部整理分析，支持企业运营，以及由外部第三方机构收集、加工、销售，为其他需求方提供有效信息，具备交易价值。狭义上，企业数据是企业在生产、经营、管理各个环节，经过控制、加工、整理、分析得出的有效信息，不涉及个人信息和公共利益，用以支撑企业经营决策，服务企业开拓创新。

从类型上来看，企业数据主要分为公开的企业数据、部分公开的企业数据、非公开与商业机密类的企业数据三种形式。其中，公开数据统一面向社会公众，一般不存在对企业造成经营上的影响和成本问题，不为企业所独占，企业不具备排他性的权利，仅可对恶意竞争、违法违规获取或使用企业数据的行为做出制止。但此类数据仍需要法律的合理保护，解决确权授权问题，保障公平竞争、合规行为和权益主体，以促进更多的企业公开数据共享，激发市场活力。部分公开

的企业数据往往以数据库的形式储存和获取，仅对少部分群体开放，企业享有经营此类数据的合法权益，同样不具备排他性。涉及到保密性质的非公开的企业数据，往往受到商业秘密的法律保护。

值得注意的是，法律对非公开或部分公开数据提供充分的法律保护，确定企业主体持有、使用和收益的权利，保障企业主体投入的劳动资本能够获得合理回报，完善企业确权授权机制，有利于促进这两类数据转化成可流通数据，加速企业数据在市场的流通和应用。

从特性上看，国家发展和改革委员会发布的《加快构建中国特色数据基础制度体系 促进全体人民共享数字经济发展红利》^①指出，与其他生产要素相比，数据具有可复制、非消耗、边际成本接近于零等新特性，打破了自然资源有限供给对增长的制约，能够为经济转型升级提供不竭动力。

企业数据将数据的特性进一步放大，除具备数据本身的低成本复制性、非排他性等性质外，还具备可再生性、可交易性、可联接性等特征：

第一，企业数据具有可再生性。产生核心价值的企业数据来源于用户，在服务客户和互动运营过程中，数字资产不断被整合优化，在更新迭代中驱动业务精进。

第二，企业数据具有可交易性。清华大学社会科学学院

^① 《加快构建中国特色数据基础制度体系 促进全体人民共享数字经济发展红利》，《求是》，2023年01期，http://www.qstheory.cn/dukan/qs/2023-01/01/c_1129246978.htm.

经济学研究所所长汤珂指出，数据可交易性是数据作为生产要素的前提。^①企业数据不仅可以依法被征用，用以满足公共需求，而且为企业主体持有、分配。同时，企业在依法依规交易企业数据的过程中享有获取收益的权益。

第三，企业数据具有可联接性。企业数据对外开放，能够便利企业数据汇聚、流通，并可与其他主体共生共建共创，实现互联融合网络。但由于企业经营能力、发展规模、技术能力等方面的差异，使得企业数据质量不均衡。完善行业龙头企业、互联网平台企业与中小微企业的双向公平授权，尤其是对中小微企业的重点保护，对企业数据之间紧密联接、杜绝数据垄断与数据封锁局面有较强推动作用。

企业数据作为数据这一新型生产要素的分支，与资本、劳动、土地等传统生产要素持续融合更新，在大数据、人工智能、区块链等新一轮信息技术的加持下，能够不断释放服务价值，提高企业经营的创造力，对于企业发展革新、市场经济建设起到举足轻重的作用。而企业数据确权授权机制的建立有利于维护市场经营秩序、加强社会公共利益保护、促进数字经济公平、高效发展。

4.2.1.2 八大重点领域企业数据概况简析

企业数据的确权授权涉及面广，情况较复杂。当前企业数据确权授权集中在关键信息基础设施关涉的八大领域，分

^① 激活数据要素推动城市发展——数字城市分论坛观察，《福建日报》，2022年7月25日，http://mag.fznews.com.cn/h5/fzrb/mobile/2022/20220725/20220725_004/content_20220725_004_4.htm

别为公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业。这些领域关键信息基础设施企业运行过程中存储或传输的信息数据大量集中或极其敏感，其中涉及的企业数据往往关系到国家安全、国计民生、公共利益，成为相关监管部门及广大民众关注的重点。

随着数据要素价值的释放，八大领域的企业数据得到一定发展。总体而言，距离释放企业数据要素价值的客观要求还存在一定差距。主要体现在两方面：

一是相关确权授权法律不够完善，数据流通环节中的各参与主体的利益分配不均衡。就金融业而言，当前，我国在金融确权及数据权利保护方面存在不足和障碍，金融数据的生产者、使用者以及消费者之间利益协调与平衡尚未形成统一认定标准，金融数据权益分配上常出现权利归属冲突情形。此外，金融数据在流动与使用中也存在数据非法采集、隐私侵权、数据非法不当使用乃至数据垄断等问题，加强个人信息数据与信息安全、隐私保护和数据确权方面立法和制度完善是关键。^①

二是企业数据难以适用传统的财产权保护制度，过度商业秘密保护易导致数据垄断。数据常常被视为数字经济时代的石油，正因如此，用排他性的财产权保护企业数据，一直被认为是企业数据保护的方案之一。但在实际操作中，企业

^① 参考黄国平，我国金融数据治理体系的创新与发展，中国金融新闻网，2022年6月18日，<https://baijiahao.baidu.com/s?id=1735906412737571581&wfr=spider&for=pc>

数据财产权保护并不能完全适用，首先，企业的公开数据难以适用绝对的财产权保护；其次，半公开或部分公开的企业数据也不适合绝对化的财产权保护；最后，企业非公开数据或商业秘密类数据的保护也不是“绝对性、排他性”的。基于此，以分类分级为基础，探索适应企业数据特点的产权保护制度成为当前的重点工作。除此之外，部分企业数据在传统财产权保护下，通过商业秘密保护企业数据可能导致企业隐藏数据，形成数据垄断。^①

4.2.1.3 《关键信息基础设施安全保护条例》提出更高要求

2021年7月30日，国务院印发《关键信息基础设施安全保护条例》，对关键信息基础设施的范围、各监管部门的职责、运营者的安全保护义务以及安全检测评估制度提出了更加具体、操作性也更强的要求，为开展关键信息基础设施的安全保护工作提供了重要支撑。该条例指出，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。同时，该条例强调，关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基

^① 参考丁晓东，企业数据如何分类保护：“数据要素市场”解读，微信公号“腾云”，2020年4月23日，<https://mp.weixin.qq.com/s?src=11×tamp=1673653079&ver=4287&signature=uMmuBxfCa1T14P3MJGWFHibLAvrj289svue095SRzfWBE1CC1sMVDp0k21WavxxVmZs1MpSgyKZUd6ePRhPZCuRS1Gw5ceSOBB1Zx4Pyy0qvrszpmv8fUh03300kmQ&new=1>

础设施运营者主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

当前，银行金融数据、非银行金融数据、汽车数据与广大民众密切相关，备受关注，结合《关键信息基础设施安全保护条例》要求，三方面值得重点关注：

一是及时、准确报送数据信息，促进有关部门、保护工作部门、运营者等之间的信息共享。2022年11月，中国银行保险监督管理委员会官网信息显示，因“EAST数据漏报及报送不一致、数据错报以及其他与数据报送相关的违规问题”，北京农商银行被北京银保监局处以630万元的行政处罚。2022年3月，中国银行保险监督管理委员会也曾严肃查处一批EAST数据质量领域违法违规案件，对政策性银行、国有大型银行、股份制银行等共21家银行机构依法作出行政处罚决定，处罚金额合计8760万元。商业银行的频频被罚，或暴露出其在风险管理、内部控制等方面存在不同程度的问题。基于此，商业银行应当充分发挥主体责任，进一步提升数据报送质量的合理化、规范化和标准化；监管部门则应继续加强对监管数据报送违法违规现象的查处力度，严肃市场纪律，提高违规成本，引导并督促商业银行切实发挥监管标准化数据在防范金融风险、提升内控水平等方面的作用。

二是履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度。对于金融机构来说，金融数据关

系其生存与发展，金融数据一旦被非法获取，会影响金融市场的稳定与秩序。金融机构应当履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度，并对关键信息基础设施设计、建设、运行、维护等服务实施安全管理。2022年，中国裁判文书网披露了一起有关非法获取计算机信息系统数据、非法控制计算机信息系统、内幕交易、泄露内幕信息的二审刑事判决书。一男子在2004年至2016年间，利用木马病毒非法入侵几十家金融机构，获取交易指令，进行牟利。此案对金融机构负责本单位的关键信息基础设施安全保护工作具有警示作用。

三是防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行。2022年12月，蔚来汽车收到一封勒索邮件。勒索者声称其掌握了蔚来汽车2021年8月之前的部分用户基本信息和车辆销售信息，并以泄露数据要挟蔚来汽车支付225万美元等额比特币。值得一提的是，车企被勒索早已有之，2016年，优步公司被黑客窃取了5700万名乘客和司机的个人数据；2018年，网络安全公司UpGuard安全研究员发现包括通用汽车、菲亚特克莱斯勒、福特、特斯拉等在内的100多家车企的机密数据在Level One Robotics的公共服务器上曝光；2021年12月，沃尔沃透露研发数据被窃取，可能会对公司运营产生影响；2022年10月，丰田汽车表示，在其T-Connect服务中约有29.6万条客户信息可

能被泄露……对此，汽车企业可以依照有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。同时，在面临重大安全威胁时，汽车企业也应当按照有关规定向保护工作部门、公安机关报告。

4.2.2 企业数据现有产权机制现状

长期以来，数据的权属问题一直备受争议。针对企业数据，“数据二十条”强化供给激励，发挥国有企业带头作用，探索国有企业数据授权运营新模式。在数据由谁管的问题上，企业纷纷在内部成立数据治理部门，通过建立科学的数据管理机制、明确数据治理统筹部门、制定流程细节，通过建立组织构架，明确职责，制定系统化的制度和规章，在明确权属授权基础上，确保数据高效、安全运行，充分挖掘企业数据价值。

在数据权利属性、权利主体与权利内容的确定问题上，目前，北京、上海、浙江等全国多地通过建立数据交易所、数据确权平台等第三方机构或平台，展开积极探索。

从业务模式来看，数据交易所也从最初的中介撮合到数据加工，再到以数据条例为支撑，探索数据确权、数据价值评估等法律制度，以及包括交易撮合、数据加工甚至数据资

产交易在内的数据交易体系，基本以点对点的交易或通过服务合同的交易为主。

从数据定价来看，目前，产业领域存在两种较为普遍的数据定价机制：一是互联网服务商等推出的以自身为主的数据服务平台或产品；二是数据交易平台结合数据质量、完整性、稀缺性等对数据集标价。由于多数数据产品的了解过程与使用过程重叠，数据有用性无法事先确定，导致买卖双方对数据价值有“双向不确定性”，加之数据具有高固定成本低边际成本、产权不清、结构多变等特征，定价难度远大于其他产品。^①

为解决数据资源流通问题，上海、广东、深圳先后推出“数据资产登记”“数据产品登记”“数据资产凭证”“数据生产要素统计核算”等数据资产登记制度。但目前在实践中，对于数据资产登记的概念和内涵、数据资产登记的意义和价值仍认识不清，相关制度建设几近空白，数据资产登记的系统平台分散且功能弱少，标准缺失，参与登记的企业和机构数量不多。整体来看，目前我国尚未形成统一、明确的企业数据确权体系。在法律法规、合规抓取信息、数据垄断等方面存在亟需解决的问题。

4. 2. 2. 1 探索企业数据产权机制取得的成果

关于数据产权的表述，“数据二十条”在强调国家统筹

^① 黄倩倩、王建冬、陈东、莫心瑶：超大规模数据要素市场体系下数据价格生成机制研究，《电子政务》2022年第2期

布局的基础上，提出推进企业数据的分级确权授权，并明确支持第三方数据服务发展。

随着大数据等技术和产业发展，全社会数据资源分布格局正在从过去政府数据资源占 80% 转变为以互联网、金融、电信等企业数据资源为主的“倒 28”格局。^①近年来，企业从未对于数据的权责管理停止探索：一是调整组织架构，成立相关数据治理部门，统筹协调数据管理；二是加强数据人员管理，越来越多的企业任命高级管理人员来负责整个企业的数据管理和监督工作。此外，各地也以提高企业数据战略意识为导向，推行试点企业首席数据官制度，提升企业数据管理能力，明确企业的战略管理方向，使企业数据的管理权责与边界更加清晰。

企业数据的价值离不开数据的流通，为加快数据要素的价值转化，各地陆续建立数据交易平台。据不完全统计，截至 2022 年底，国内由副省级以上政府牵头组建的数据交易场所超 30 家，由政府或企业建立的数据交易平台超 80 家。随着数据交易机构的陆续成立，各地纷纷提出“数字经济中介”“数据经纪人”“数据服务商”等新型服务生态，这些机构和服务体系在数据交易相关规则制定、数据产权制度方面取得了一定成果：

一是完善数据规范体系，提升业务效率。上海数据交易

^① 国家发展改革委员会高技术司，探索数据产权登记新方式，加快构建全国一体化数据要素登记体系，国家发展改革委员会官网，2022 年 12 月 21 日，https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221220_1343700.html?code=&state=123

所首发数商体系，涵盖数据交易主体、数据合规咨询、质量评估、资产评估、交付等多领域，培育和规范新主体，率先针对数据交易全过程提供一系列制度规范，涵盖从数据交易所、数据交易主体到数据交易生态体系的各类办法、规范、指引及标准，确立了“不合规不挂牌，无场景不交易”的基本原则，帮助企业更好的整理、处理和管理数据、改善业务。北京国际大数据交易所将中介服务功能与数字经济特点相结合，建立国内首个数字经济中介产业体系，形成涵盖数据收集、治理、加工、确权、评估、定价、交易等数据要素服务商体系，促进交易效率提升。

二是推进数据跨境服务，促进跨境安全流通。为解决企业在数据跨境流通中面临的困难，北京国际大数据交易所在全国率先以服务数据跨境场景为着力点，试点开展跨境数据合规托管工作；深圳市积极推进“数据海关”试点，开展跨境数据流通的审查、评估、监管等工作，推进跨境数据交易。

三是探索数据产权登记新方式，加快构建一体化登记体系。贵阳大数据交易所通过建设数据要素登记 OID (Object Identifier, 对象标识符) 服务平台，面向全国提供数据产品登记、数据资产登记、数据交易登记等服务，为全国一体化数据要素登记体系建设探索路径。

四是控制数据流通风险，建立数字信任。企业可通过授权“数据经纪人”等数据交易配套机构行使权力，促进数据

流通中的风险控制和价值挖掘。在“数据经纪人”监管领域，广州市引入“监管沙盒”模式，通过与试点企业签订“信任协议”来兼顾安全可控与创新突破。

近年来，国家出台《网络安全法》《数据安全法》等一系列关于数据安全和网络安全的法律法规。《大数据白皮书（2022年）》显示，自2021年以来，我国数据安全体系建设进程明显提速，驱动力主要来源于政策与技术两个方面，数据安全法律政策逐步细化，政策环境不断完善，为企业数据安全建设提供政策引领，在技术层面，数据安全技术产品蓬勃发展，数据安全培训、数据安全评估等方面需求开始爆发式增长。^①

在破解数据安全问题上，区块链、隐私计算等互联网信息技术的应用也不断促进数据要素的安全可信流通。以内容生产领域为例，相关企业将区块链技术作为解决网络版权问题的新型内容科技，有效化解传统数字资产保护领域确权难、维权难、用权难的三大难题，如北京人民在线网络有限公司打造的“人民版权”平台，通过版权授权交易生成数字作品的专属价值链，为版权方提供文字、图片、视频等多种媒体形式作品登记，实现区块链登记、版权监测等相关版权保护。

场景案例 3

（1）场景背景

^① 《〈大数据白皮书（2022年）〉发布》，《人民邮电报》，2023年1月5日第3版，https://paper.cnii.com.cn/article/home_16306_314579.html

针对“信息的影响力无法强化版权媒体的影响力”的问题，人民版权平台依托区块链、人工智能、大数据分析、云计算等前沿技术，为知识产权保护提供创新的解决思路。面向广大媒体单位，人民版权为文字、图片、视频等多种类型原创作品提供原创内容自动确权、侵权实时监测、授权交易和维权诉讼的全流程线上服务。建立版权保护和版权收益分享机制，打造全内容的版权生态；以版权影响力强化媒体影响力，助力媒体差异化定位，赋能融媒体协同发展。

人民版权从行业需求出发，利用区块链、自然语言处理技术、视频基因提取与AI图像识别技术、打通原创内容自动存证、原创转载实时监控、侵权转载快速取证、侵权行为线上维权全业务流程，实现存证、维权、诉讼每一个环节无漏洞保护。确保每一条资源版权“身份唯一”、来源可靠，实现精准溯源，探寻传播途径，从而达到净化版权市场，支持内容原创，提升版权价值与优化舆论生态的目的。解决溯源难，人工识别效率低，传统比对耗费大，检索识别准确率过低，检索速度慢的多重难题。

（2）场景建设

人民版权平台具有原创作品登记上链、全网原创作品侵权监测、原创内容比对自查、多场景取证、高效维权、版权交易、智能大屏等功能，其中，智能大屏功能是人民版权平台依托人民在线强大的全网信息采集能力和自然语言处理

能力，可提供定制化的数据可视化服务，如内部生态自有作品传播、登记等情况，通过数据可视化展示，帮助用户全面、宏观、整体地了解自身动态数据。



图 6 人民版权智能大屏

(3) 场景成效

作为对知识产权保护的实际应用探索，人民版权平台与中广电传媒有限公司、西部国家版权交易中心、北方国家版权交易中心等多家单位开展合作，还有全国近百家媒体单位正在对接接入中。其中，人民版权平台打造“北京云·融媒体”省级技术平台，以“聚合、开放、分析、赋能”为目标，对全网数据采集，反馈最真实的舆情动态；通过宣传指挥调度平台灵活指挥调度，实现全市宣传队伍协同作战；通过建立内容共享和分发平台，构建“一次采集、多元生产、多元传播”工作格局，进行统一资源内容管理，共建版权联盟，推动内容共享。

为兼顾数据安全保护与实现数据价值，如何通过前沿科技升级数据安全体系、基于科技创新提升数据安全能力成为

企业考量的重点。有互联网银行结合区块链和多方安全计算的优势推出多方大数据隐私计算平台 WeDPR-PPC，从联合报表、联合计算、隐私查询等技术场景切入，在联合风控、反欺诈、反洗钱等议题中，促进隐私数据有序流通，实现跨域价值融合创新，全方位保障用户隐私安全。中国信息通信研究院云计算与大数据研究所所长何宝宏表示，以隐私计算平台为代表的多方安全计算环境，有望成为数据合规流通基础设施的关键一环，在保证安全的前提下有效持续释放数据要素价值，促进数字经济高质量发展。^①

4.2.2.2 推动建立企业数据产权机制存在的难点

在数字经济时代，数据成为越来越重要的生产要素。当下大量经由获取、交易而被企业主体掌握的数据，通过开放、共享、交易、携带与抓取等形式得以流通。然而，实践表明，我国企业数据产权机制建设在法律法规、合规抓取信息、数据垄断、专业人才供给及数据交易等方面存在待解决问题。

一是企业数据确权仍存在法律空白。为推动数据要素市场发展，相关政策陆续出台，《“十四五”大数据产业发展规划》提出，健全数据要素市场规则，发展数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系。《要素市场化配置综合改革试点总体方案》提出，探索“原始数据不出域、数据可用不可见”的交易范式。近些年，《数据安全

^① 中国信息通信研究院云大所所长何宝宏：隐私计算 + 区块链：让数据真正成为生产要素，《人民邮电报》，2021年9月15日，https://www.cnii.com.cn/rmydb/202109/t20210915_309386.html

法》《个人信息保护法》等数据安全相关法律法规也陆续出台实施。但是，在数据确权、数据流通等环节，支撑性的法律法规基本处于空白状态。

二是违规抓取信息问题。包括企业超范围抓取信息、不正当手段获取信息等。数字经济时代，数据资源已成为市场主体的核心竞争力，部分市场主体为了获取更多的数据资源，通过实施不正当数据抓取行为，违法获取其他市场主体具有商业价值的数据资源的现象时有发生。2022年，上海警方发现一互联网站售卖知名直播平台主播数据，据此循线深入侦查，侦破一起非法获取计算机信息系统数据并公开售卖获利的案件。2016年，脉脉不当抓取微博用户信息，被判定脉脉构成对新浪微博的不正当竞争，赔偿新浪微博经济损失200万元。

三是数据垄断问题。互联网时代，平台在重塑社会生活的同时，也会通过垄断损害他人的合法权益，主要表现为“大数据杀熟”、排他性交易等。2016年至2022年，脸书、谷歌、亚马逊等互联网公司在欧盟受到的反垄断诉讼始终不断。在国内，尽管某些企业声称自己没有数据垄断，但中国人民银行科技司相关负责人曾在2017年6月公开表示：“一些规模较大的机构通过开展综合业务，大量汇集信息流、资金流与产品流，加之基于网络的云存储技术使金融数据高度聚集，数据寡头已经产生。”

四是专业服务机构和专业人才储备与市场需求存在较大供需缺口。在我国，数据要素、数据确权是新生的事物。国内高校开展数据要素、数据确权人才培养的时间并不长，市面上具备数据要素、数据确认能力和经验的人才亦很少。这也造成数据确权、数据治理、资产评估、创新应用等方面缺乏自我造血能力，导致数据要素对于数字经济的赋能不足，并对我国数据经济发展造成了严峻的挑战。

五是企业数据场外交易量大，质量安全无法保证。目前，国内已经建立的各类数据要素交易市场超过 30 家，但 90% 以上的国内数据交易却来自于“场外交易”，并且以实现数据控制权从 A 到 B 的转移作为主要的交易目的，这直接导致了数据交易的目的与场景不可控、数据交易标的质量无法保障、侵权与维权工作难以展开、数据交易价格与数据要素价值严重不匹配、数据资产配置滞后、交易后市场服务缺失、政府数字经济促进政策触达低等诸多问题，这也间接造成数据交易“黑灰色地带”多发且无法有效管理等问题。

4.2.3 企业数据产权机制运行要求及原则

“数据二十条”提出“发挥国有企业的带头作用，引导行业龙头企业、平台企业与中小微企业的双向公平授权”，通过倡导双向公平授权，让企业数据开放、流通告别野蛮生长，推动数据产业生态繁荣，保障数字经济高质量发展。本部分内容将围绕企业数据产权机制运行要求及原则进行探

讨，对不同企业间数据双向公平授权、第三方数据服务机构权责与使命、企业采集个人信息应该遵守的原则等提出基本遵循。

“数据二十条”在“工作原则中”强调，坚持共享共用，释放价值红利。合理降低市场主体获取数据的门槛，增强数据要素共享性、普惠性，激励创新创业创造，强化反垄断和反不正当竞争，形成依法规范、共同参与、各取所需、共享红利的发展模式。同时，鼓励探索企业数据授权使用新模式，着力发挥国有企业带头作用，引导行业龙头企业、互联网平台企业发挥带动作用，促进其与中小微企业双向公平授权、共同合理使用数据，以此赋能中小微企业数字化转型。

4.2.3.1 推动大型企业与中小微企业双向公平授权

(1) 大中小微企业共同发展

据国家工业信息安全发展研究中心测算，预计到 2025 年，中国数据要素市场规模将突破 1749 亿元，整体进入高速发展阶段。企业是发展数据要素市场的根本力量。企业数据由简单的信息升级转变为重要的经济资源，形成企业的核心资产。如何管理、利用好企业数据，寻求竞争之外的更大价值成为时代的“必修课”。

大型企业数据向中小微企业合理开放，提升数据供给质量。目前对于双向公平授权，打破市场中的潜在垄断控制成为破局关键。数据成为决定着企业竞争优势的重要因素，海

量数据集中在行业头部企业，特别是大型国有企业、大型互联网公司、电信运营商、银行以及电力、交通运营企业。平台龙头在先期发展中积累了大量数据，通过利用这些数据更有针对性地提供服务，增加用户留存，加强竞争优势，限制其他企业从数据中找准发展通路，间接对新进入市场的竞争平台形成进入壁垒。

龙头企业在数据分析和挖掘技术上也具有优势，更容易将累积的数据资产转化为实际利益。数据垄断造成数据的获取和运用明显不对称、知识不对称、技术不对称，有悖于数字经济的运行逻辑。行业龙头企业、平台企业与中小微企业的双向公平授权意味着更加健全的合规流通途径，带来更高质量的数据供给，对利用数据加强竞争优势、侵害消费者权益、破坏竞争秩序等数据垄断行为起到抑制作用。

企业间数据流通以供需合作为前提，较多企业通过协商约定互相提供数据。数据市场离不开规则，其核心是建立合理、公平的确权授权机制。《欧洲数据法案》提出，为防止大企业滥用竞争优势地位，提高中小企业在数据共享谈判中的议价能力，大企业应向中小企业提供公平、合理和非歧视性的合同条款，禁止数据共享合作中强加的单方面合同条款。

双向公平授权赋能中小微企业，推动数字经济高质量发展。当前中小微企业在双向授权中处于不对等地位，主要原因之一是缺乏数据，不少企业数字化程度明显不足。尤其是

自身具有一定数据资源的中小企业，担心商业机密被泄露或失去数据控制权，不愿向大型企业授权开放数据资源，盲目追求独立经营，形成数据孤岛。“双向公平授权”的提出对中小企业加快数字化转型起到重要的促进和引领作用。赋能中小微企业数字化转型是我国数字经济高质量发展的具体表现。

针对中小微企业无数可用、数字化转型程度不深等问题，应以数字化、网络化、智能化技术作为支撑，围绕中小企业生产、流通、服务各应用场景提供数据服务，建设中小企业数字化赋能生态体系，王春晖指出，应当优先推动中小微企业正当合理合法地收集数据和利用数据资源，再逐步促进大型企业与中小微企业双向公平授权，共同挖掘和利用数据价值。^①另外，引导部分率先实现数字化转型的中小企业应在自身数据安全、商业安全的基础上，积极提供数据授权，借力大型企业的技术优势和分析优势，深度参与数字经济市场。

在确保大型企业、平台企业不实行数据垄断，保证对高质量数据有巨大需求的中小企业有大量数据可用并能公平使用数据的同时，小企业也不能无序搭便车，应让双方在创新、发展的基础上，双向赋能、合作共赢。

（2）推动企业数据开放的探索建议

^① 王春晖，解析“数据二十条”中的数据产权制度，微信公号“上海市法学会”，2022年12月22日，https://mp.weixin.qq.com/s?__biz=MzUxMzUyMzk10A==&mid=2247749205&idx=1&sn=30115a11bb7a7ae4a145a0b8cb42e059&chksm=f95ea7ccce292eda5cd53cbddaac78598fdef40a1ba619233a9e2ab3a5bccfef55195d509f26&scene=27#wechat_redirect

分类分级实施数据开放，跨领域、跨平台授权促进数据要素流动。大型企业与中小微企业双向合理公平授权机制的建立尚处于“摸着石头过河”阶段。企业数据跨领域、跨平台授权可以促进数据要素流动，但因缺乏统筹规划、数据流通渠道不畅、利益分配争议等瓶颈问题面临重重挑战。推动企业数据开放，可从以下几方面进行探索：

一是明确授权边界，制定分类分级标准。实施分类监管，区别指导，精准监督，为龙头企业、平台企业带动中小企业发展提供良好的政策和市场环境。明确责、权、利的边界，根据不同规模平台的义务责任施行数据分类分级保护制度，细化数据授权—确权的基本制度和行业制度。监管机构需要进一步明确超级平台在反垄断、反不正当竞争层面的特殊义务，明确超级平台、大型平台、中小型平台的规模划分标准，以便明确不同规模、不同行业在数据流转交易过程中的数据安全保障义务，在保护企业利益的同时创造新的数据价值。

二是平衡保护与发展，携手共促公平授权。商业数据跨平台流动对促进竞争与创新发展有积极作用；企业数据综合了技术法律以及经济政策多领域的问题，需要依靠政策、企业、用户等多方力量携手共促。平台企业之间通过屏蔽外部链接等方式各自打造生态“护城河”，缺乏合理的数据接口授权模式。虽然有利于平台的短期商业利益，却有损中小企业与用户的权益，一些互相屏蔽问题给消费者带来了使用成

本增加等问题。同时，也不利于整合资源和互联场景，激发高质量发展活力。有关部门持续监管互联网平台间恶意封禁行为，推动平台开放外链、促进互联互通。

三是打通数据链上下游，释放多元价值，实现跨区域、跨平台授权。企业在数字经济的发展中，跨领域合作为创新突破带来更多可能，通过访问外部数据资源，释放不同信息的多元价值，有助于打通数据链上下游产业。以导航地图公司的数据为例，政府部门需要了解一部分用户数据来改善道路交通状况，智能汽车制造商、保险公司也需要分析相关数据来保障行车安全或有针对性地提供保险服务。在医疗行业中，大数据的应用促进新药研发，同时，健康风险管理也依赖于数据要素的支撑，例如：利用数据对于重点人群的疾病早筛和干预。另外，电力行业的数据几乎穿透所有行业，客观上需要跨领域的数据流动、联通。

4.2.3.2 探索数据经纪人等模式 推动第三方机构发展

近年来，广东、上海、北京等多地实践探索第三方机构的参与机制，推行“数据经纪人”“数商”等业务模式。2021年7月，《广东省数据要素市场化配置改革行动方案》印发，提出探索建立“首席数据官”“数据经纪人”制度等，定义数据经纪人是政府监管下具备开展数据经纪活动资质的机构。广州海珠区将“规定动作”和“自选动作”相搭配，以“规定动作”聚焦电力、金融、电子商务等重点领域，推动

数据流通规范化；以“自选动作”立足行业特色，创造性地探索数据经纪业务试点工作。

与之类似，上海数据交易所在2021年推出“数商”概念，涉及数据交易主体，数据合规咨询，质量评估，资产评估、交付等多领域。北京国际大数据交易所也提出类似数字经济中介服务商概念，实践建设数字经济中介产业体系，包括“数据收集、治理、加工、确权、评估、定价、交易、审计、资产证券化等新型数据要素服务商”。和“数商”相比，“海珠模式”下的数据经纪人服务范围更广，涵盖场内交易和场外交易双空间。

实践中数据经纪人更多充当撮合的角色，但从企业数据确权授权要求来看，数据经纪人的职能不能只是撮合，需要更多发挥整合和分析作用，更大程度挖掘数据应用场景，充分激活数据要素市场活力。在企业数据处理上，数据经纪人需更多考量数据利用的效率和效益，重在实现数据价值的充分挖掘和资产化；对公共数据的处理，则着力于促进数据开放，提高数据驱动的决策质量，侧重数据发展的责任和安全。

数据经纪人应解决数据供给和需求之间的断层，维护数据安全与应用的平衡体系。例如，人民数据承担起数据“经纪人”角色，发挥“中间人”作用，承揽优质、可公开的政务数据，以特定、有偿方式向第三方市场主体开放。人民数据对接多个行业的全国全量数据，以平台和产品的形式向地

方政府、市场主体等需求方提供数据支持。

“数据二十条”明确要求支持第三方机构、中介服务组织加强数据采集和质量评估标准制定工作，推动数据产品标准化，发展数据分析数据服务等产业。第三方机构和中介服务组织将成为推动数据采集和质量评估标准制定的重要主体，基于第三方机构的职责使命，更好地让第三方机构参与到企业数据确权授权机制中，可以重点从三方面发力：

一是建立权责明晰的第三方机构标准。“打铁还需自身硬”，第三方机构作为数据采集和质量评估标准制定主体，其自身的标准也亟待明确。目前，在国家层面还未建立第三方机构的相关标准，监管部门还不明确。基于企业数据确权授权的客观需求，建立第三方机构标准需要明确一些重点，如由谁来制定第三方机构标准，谁来保障标准执行，标准需要明确的权责内容，标准是否对第三方机构建立退出机制等。

二是明确第三方机构的许可要求。在实践中，一些银行、保险公司等拥有大量数据的企业，缺乏数据加工能力，直接进行数据授权不能满足其他企业对高质量数据的需求，这就要求有数据处理能力的第三方机构支持介入。但能够介入支持的第三方机构需要明确第三方机构的许可要求。该要求需要明确第三方机构具备的资质，承载企业数据确权授权需求、保障数据安全等。业内专家建议，设立国有第三方机构、有央企背景的企业等，如大数据交易所，大数据局产品检验检

测、分级、治理、数据资产化配置等机构，有助于确认数据权属问题。相关企业在积极探索以第三方机构的身份，助力数据要素发展。

三是探索建立对企业数据违规行为认定的第三方机构。在数字经济时代，数据是企业的核心竞争力，数据合规是企业健康可持续发展的基石。但企业数据合规面临着多重现实困境，包括数据应用违规频发，企业合规成本高昂，企业内外数据泄露严重，数据处理不当处罚严重，部分企业合规意识淡薄。基于当前处于企业数据确权授权的探索阶段，结合企业数据违规多发的现状，在给企业数据流通树标准的同时，也需要探索建立对企业数据违规行为认定的第三方机构，为企业数据正常流通立规矩。

在探索建立对企业数据违规行为认定的第三方机构时，也需要注意：一是认定企业数据违规的机构具有权威性、公正性，在行业内有话语权，这既可以是企业自身具有这些属性，如探索标准规矩，拥有广泛民意渠道和研究基础的央国企，同时也可以是得到相关监管部门授权的机构或组织。二是有明确的认定标准和规范，包括按照党中央、国务院对数据要素发展的指导要求，遵循相应的法律法规、条例规章、地方法规标准等，能够做到客观、公平认证，为企业数据合规营造良好的流通环境。三是具备打造征集线索、发现问题、促进专项行动、完善政策法规的闭环能力，真正做到及时发

现问题，推动相关部门快速处理，并上升到差缺不差，完善相关规章制度。

4.2.4 企业数据分类分级发展现状及使用原则

无论是产生的还是收集的企业数据，均需要分类分级才能授权使用。分类分级是企业数据授权流通的前提，探讨企业数据分级分类标准现状、面临的挑战及企业合法合规使用数据，享受相关权益的原则，有助于推动企业数据产权制度的实际落地。

4.2.4.1 推动企业数据分类分级政策措施

企业数据的分类分级是完善数据确权制度、促进数据共享流通、保障数据安全的基础之一。近年来，国家陆续出台相关政策，指导数据使用主体开展分类分级工作，推动数据分类分级治理。《网络数据分类分级指引》提出了常见的数据分类维度，包括公民个人维度、公共管理维度、信息传播维度、行业领域维度以及组织经营维度。2022年9月发布的《信息安全技术 网络数据分类分级要求》（征求意见稿）提出了通用的数据分类分级原则和方法，用以解决缺乏国家统一的数据分类分级规则问题，推进数据分类分级保护制度落地实施。

该要求指出，数据按照先行业领域分类、再业务属性分类的思路进行分类。由于不同行业数据类型差异较大，在该要求提出的统一明确的数据分类方法指引下，各行业需要根

据实际情况确定适合各自领域的分类标准，指导企业在相关法律政策指引下开展数据分类分级工作。

当前，我国工业、电信业、金融业、医疗业和汽车行业等部分行业领域均已出台了针对性的数据分类分级指南或技术规范，开展了数据分类分级保护工作。《工业数据分类分级指南（试行）》要求工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。《汽车数据安全管理若干规定（试行）》指出利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽车数据保护，依法履行数据安全义务。《证券期货业数据分类分级指引》提出在解决业务分类问题、确定数据管理主体的基础上，进行数据归类，形成以交易、监管、信息披露等一级子类以及子类下 13 个具体数据类别。《基础电信企业数据分类分级方法》将电信行业的数据划分为用户相关数据与企业自身相关数据两大类，并对其细分。

数据分类管理为不同水平下数据分级的防护打好根基，有助于对不同类别不同级别的数据采取相应的安全防范措施。《信息安全技术 网络数据分类分级要求》将数据从高到低分为核心、重要、一般三个级别。各行业企业需要参考数据分级规则，对数据进行定级（见表 7）。

表 7 数据分级确定参考规则

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	重要数据
社会稳定	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织利益、个人权益	一般数据	一般数据	一般数据

《信息安全技术 网络数据分类分级要求》按照数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对个人、组织合法权益造成的危害程度，将一般数据从低到高分为1级、2级、3级、4级四个级别。此类级别标准视各行业实际安全情况而定，例如《工业数据分类分级指南（试行）》将数据分为三级，《基础电信企业数据分类分级方法》按敏感程度分为四个安全级别，《金融数据安全 数据安全分级指南》根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度分为五级，《信息安全技术健康医疗数据安全指南》根据数据重要程度、风险级别、对个人健康医疗数据主体可能造成的损害和影响分为五级。

4.2.4.2 企业数据分类分级面临的挑战

企业数据分类分级也面临四方面挑战：一是数据资产识别梳理难。企业数据分类分级的前提是明确企业的数据资产。在实践中，企业数据往往分布较分散，可能存在于PC端、云端、移动端和外部处理供应链等，加上，企业数据规模庞

大，这些均会增加数据资产识别与梳理的难度。

二是标准不统一，落地实践难。从数据分类分级的政策文件及已经明确的行业相关标准来看，缺乏相对统一的数据分类与分级标准问题较突出，数据的分类与分级各自均具有自身的交叉性，按照不同的标准可将数据划分为不同的类别与级别，且分类与分级两者之间也存在交叉，进而对同一数据存在不同的规范管理制度，可能导致不同的领域、行业、执行主体等在具体适用中混乱与不协调。

此外，即使有些行业有标准，但这些标准仍不够精细化，执行人员较难着手处理。对于已经做好分类分级处理的数据，由于缺乏相关流程制度及平台，分级分类后，面临如何落地使用问题。这也是造成当前各行业、各地区缺乏优秀实践案例的重要原因。

三是缺乏数据分类分级技术支撑。基于企业数据的量级以及其重要性，高效率的企业数据分类分级工作需要人工干预与人工智能等技术支撑，从目前的实践看，现有的企业数据分类分级工作仍然以人工制定规则和标准为主，智能处理较弱，导致企业数据的认定识别成本高、更新慢等问题。

四是专业数据人才供不应求。企业数据分类分级需要专业人才，当前，专业数据人才较少，国家互联网信息办公室会同相关部门研究起草《网络数据安全管理条例（征求意见稿）》中明确要求，国家支持数据开发利用与安全保护相关

的技术、产品、服务创新和人才培养。未来，专业数据人才，同时能够运用人工智能等技术将备受数据市场欢迎。

基于企业数据分类分级面临的挑战，明确企业数据分类分级法律法规，形成相对统一的企业数据分类分级标准，梳理并推荐优秀落地实践案例，完善数据分类分级技术和方法，培养更多适应企业数据分类分级需求的专业人才，将是推动企业数据分类分级工作的重点。

4.2.4.3 企业数据合法合规使用原则

在大数据时代背景下，企业数据成为企业之间竞相争取的重要生产要素，企业数据的使用渗透在经济、社会、生活的方方面面。但由于缺乏明确的数据利用标准，不正当使用企业数据的行为时常出现。为此，在实际使用过程中，企业应把握以下两大原则：

一是兼顾安全与发展。作为网络空间安全的基础，数据安全不仅会对公民的个人隐私和经济利益产生影响，还会对公共利益和国家安全产生影响。因此，在使用和发展企业数据过程中，需要牢牢守住安全底线。在总体国家安全观的指导下，企业要兼顾安全与发展，具备更高的安全保护意识，增强数据保护能力，筑牢数据安全屏障，使其数据安全治理工作不仅满足基本商业竞争与发展需要，还要与国家安全、公共利益、个人合法权益需求相匹配。

二是合法合规正当收集数据。企业数据合法合规使用的

前提是数据的获取需要合法合规正当。一直以来，数据收集是数据监管部门重点关注的问题之一。在获取数据时，企业要认真落实告知知情同意原则，在明示并征得用户同意后，才能获取相关信息。另外，在利用爬虫手段收集信息数据时，企业要遵守目标网站设置的爬虫协议，依法依规地使用数据收集技术。在源头上保证获取数据合法合规，才能为后续使用数据，享受相关收益，奠定良好的基础。

第三节 建立健全个人信息数据确权授权机制

4.3.1 个人信息数据的界定

“数据二十条”提出：“对承载个人信息的数据，推动数据处理者按照个人授权范围依法依规采集、持有、托管和使用数据，规范对个人信息的处理活动，不得采取‘一揽子授权’、强制同意等方式过度收集个人信息，促进个人信息合理利用。”上述内容明确了“推动数据处理者按照个人授权范围依法依规采集、持有、托管和使用数据”。关于“授权”是指数据处理者接受个人信息主体的委托处理其个人数据的行为，上述授权的范围包括四项内容，即依规采集数据、持有数据、托管数据和使用数据。

上述“授权”行为可以参照《个人信息保护法》第二十一条有关委托处理个人信息的规定，一是个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利

和义务等，并对受托人的个人信息处理活动进行监督；二是受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；三是委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留；四是未经个人信息处理者同意，受托人不得转委托他人处理个人信息。上述规定中的“个人信息处理者”，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

4.3.1.1 关于个人信息的法定规范和定义

个人信息不仅关系到个人的生命财产安全，更关系到社会的稳定和国家的安全。数字经济时代更加注重对个人信息的保护。关于个人信息，国内外都对其有较为详尽的描述，以求对个人信息进行更加全面的保护。

我国相关法律法规对个人信息进行了明确的定义：《民法典》第一千零三十四条规定：“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等”。《网络安全法》第七十六条第（五）项规定：“个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识

别信息、住址、电话号码等”。《个人信息保护法》第四条规定：“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”。

我国对个人信息的定义中，“以电子或者其他方式记录”的方式，强调了电子与其他方式系并列关系。有专家指出，实际上，这句话表达的意思为：“任何方式”，除了“电子”以外的个人信息，都可以归类为“其他”。^①

个人信息可以分为两类：一是个人信息是可识别的信息，具有可识别性；二是匿名化处理后的信息不属于个人信息。

第一，可识别性。个人权益与个人身份紧密相关，因此控制、规范身份识别问题是个人信息保护的重要内容。我国《民法典》《网络安全法》和《个人信息保护法》都强调了个人信息是“可识别”自然人身份的信息，说明了“识别性”是个人信息基本功能。

一般而言，按照信息可识别性，个人信息大致可以划分为直接标识符和间接标识符两类，直接标识符信息是指可以识别的包含个人识别符号的信息，如基因序列、生物特征、护照号码、驾照号码、居民编号、法律规定的其他可以识别个人的符号；间接标识符信息是指信息中所包含的姓名、生日及其他可以间接识别特定个人的信息。

^① 个人信息保护法与 GDPR——横向比较不同法域下对个人信息的保护，德恒律师事务所官网，2021年08月31，<http://www.dehenglaw.com/CN/tansuocontent/0008/022406/7.aspx?MID=0902>

个人信息保护既包括对直接标识符信息的安全保护处理，也包括对间接标识符信息的保护。华东政法大学法律学院教授高富平认为，从识别行为的目标角度，广义的识别行为可以分为两类：一是识别自然人的身份；二是识别自然人的行为习惯、兴趣爱好或者经济、健康、信用状况等个性特征。以自然人身份为目标的行为是狭义的识别行为，《个人信息保护法》中的“识别”即指狭义识别。以勾勒自然人的个性特征甚至是群体特征为目标的识别分析行为（也称为画像）也属于广义识别行为，但区别于狭义识别行为，在《个人信息保护法》中被称为“分析、评估”。^①

第二，“匿名化”。《个人信息保护法》中强调了个人信息不包括匿名化处理后的信息。其第七十三条规定，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。

《中华人民共和国网络安全法》第四十二条规定，个人信息匿名化至少满足以下要求：一是个人信息必须经过技术处理存储，二是被处理后的个人相关数据无法识别到特定个人，三是不能通过处理后的数据复原原始个人信息。如将具体年龄属性值“20”“22”等值匿名化为区间值“20~30”，具体地址位置匿名化为“XX市XX区”，具体薪资或纳税额值2118、19080等匿名化为“1000~1万”“1万~10万”

^① 数字法治|高富平：基于规范目的的个人信息治理规则，《中国应用法学》2022年第6期，<https://www.163.com/dy/article/HRUHAIUJ0514AGAB.html>

等。匿名化处理后的个人数据不可逆，即要求在任何情况下都无法通过自身存储或其他渠道获得的额外信息完成特定个人主体识别或者关联，也无法复原出原始个人信息。

将“匿名化”与“非匿名化”作为判断信息是否属于个人信息的标准极大地促进了信息的自由流通、交易与共享，对于指引企业进行个人信息保护、加强数据安全监管起到重要作用，对信息产业的发展存在积极意义。

从技术层面看，数据匿名化通常指从数据集中删除个人身份信息（标识符）的过程，但受限于技术、成本、时间等因素，将个人数据完全做到匿名化处理仍存在困境。“匿名化”与“去标识化”的区分也成为学界及业界讨论的重点。

根据《个人信息保护法》第七十三条，去标识化是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。去标识化的目标是通过对直接标识符或间接标识符进行删除或变换，使得攻击者无法根据去标识化个人数据识别出特定主体。以身份证号去标识化为例，具体身份证号“440401（年月日）1768”可以使用“440401*****1768”或者“GG44M6801”替代，变换前后的编码标识是可逆的。

虽然匿名化和去标识化均对个人信息进行保护处理，但两者关注的重识别主体和处理后信息的性质有着根本的不同：一是去标识化强调在“不借助额外信息”的情况下无法

重识别特定个人主体，二是去标识化后的个人数据仍属于个人信息，因为任何信息处理者有可能获取还原标识符的“额外信息”，进而反向复原或重识别出特定个人，因此仍需保证去标识化数据的安全。^①

综上所述，去标识化没有匿名化的要求严格，实现匿名化的加工方法都可以满足去标识化的要求。在利用个人信息分析评估个人的行为习惯等个性特征时，如果只是将信息指向某个个体，但不识别该个体的真实身份，就可以在合理、合法的情况下利用信息，用数惠民。例如，在利用医疗保障数据进行个性分析时，不必得知参保个人的身份，仅通过国家医疗保障部门为每位参保个人配备的唯一编码，即可将关于该参保个人的各方来源的信息匹配起来并进行分析评估。

4.3.1.2 个人信息数据属于消极权利

在法律上，承认自然人对个人信息数据的民事权利之后，要明确该权利的内容并将其与既有的民事权利相区分，从而确立相应的保护方法。自然人对个人信息数据的利益必须具有一定程度的社会可识别性，这就意味着该利益是稳定的、持续的，值得信赖的。而这一利益并非是自然人对个人信息数据的财产利益，因为绝大多数情况下，个人信息数据对于自然人来说是没有经济价值的。

^① 关于去标识化、匿名化等概念简析及思考，<https://mp.weixin.qq.com/s/eeMa4jQK5bTWhCCy6BiWg>

清华大学法学院党委副书记程啸教授认为，个人数据可以成为民事权利的客体，可以通过私权制度对其加以规范和保护。自然人对个人数据的权利旨在保护其对个人数据的自主决定利益，从而防御因个人数据被非法收集和利用而侵害既有的人格权与财产权。自然人对个人数据的权利并非物权等可以积极利用的绝对权，只有在该权利被侵害而导致其他民事权利被侵害时，才能得到侵权法的保护。因此，自然人对个人数据的权利是一种消极的防御性的权利，不是积极的、绝对的。

王春晖指出，在大数据和云环境下，个人信息从一开始处就在与自然人主体的分离状态，自然人根本无法了解自己的个人信息在何时、何地、被何人、以何种方式收集、存储、使用、加工、传输、提供、公开等。因此，个人信息权益处在一种消极状态，无法积极行使。^①只有规范个人信息处理行为，才能保障个人信息权益。

《个人信息保护法》明确了个人在信息处理活动中的权利包括：

- (1) 知情同意权。收集和使用公民个人信息必须遵循合法、正当、必要原则，目的必须明确并经用户的知情同意。
- (2) 决定权。有权限制、拒绝或撤回他人对其个人信息的处理。

^① 《数字社会与数据权益》，王春晖，2021年10月10日，“数据治理与隐私保护”高端研讨会暨网络空间治理与数字经济法治（长三角）研究基地启动仪式。

(3) 查阅复制权。个人有权向个人信息处理者查阅、复制其个人信息。

(4) 个人信息转移权。个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

(5) 更正补充权。个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

(6) 删除权。在以下五种情形下，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：①处理目的已实现、无法实现或者为实现处理目的不再必要；②个人信息处理者停止提供产品或者服务，或者保存期限已届满；③个人撤回同意；④个人信息处理者违反法律、行政法规或者违反约定处理个人信息；⑤法律、行政法规规定的其他情形。

(7) 规则解释权。个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

以上七项权利大多属于个人信息保护请求权，是个人信息处理者在对自然人的个人信息的收集、储存、使用、加工、传输、提供、公开等过程中，自然人所享有的请求权，其中大部分是包括排除个人信息的处理者违法侵害的消极请求权，很少有个人控制、支配个人信息的积极请求权。

我国《个人信息保护法》第四章的名称为：“个人在个人信息处理活动中的权利”。从上述名称可以看出，自然人的个人信息权是，个人信息处理者在对自然人个人信息的收集、储存、使用、加工、传输、提供、公开等过程中，自然人所享有的请求权，包括七项权利：知情权、决定权（限制、拒绝和撤回权）、查阅复制权、个人信息转移权、更正补充权、删除权、规则解释权。以上请求权大部分是包括排除个人信息的处理者违法侵害的消极请求权，很少有个人控制、支配个人信息的积极请求权。

因此，“数据二十条”确立的“健全个人信息数据确权授权机制”的前提，是严格规范平台企业处理个人信息的行为。从我国《个人信息保护法》立法目的看，主要包含两大功能：一是“保护个人信息权益”，二是“促进个人信息合理利用”，但“规范个人信息处理活动”则处于《个人信息保护法》的核心地位，只有夯实“规范个人信息处理活动”这个关键环节，才能确保实现保护个人信息权益和促进个人信息合理利用之目的。

综上所述，在传统的法律体系中，自然人既有的权利通过对这种权利本身赋予绝对权的保护请求权或者损害赔偿请求权就足以得到保护。然而，在大数据时代，个人既有的权利面临着新的风险，既然自然人对个人信息数据的权利是一种消极的防御性的权利，确立个人信息权，就要确立自然

人在信息社会中的主体地位。大数据时代下，通过个人信息保护规则，明确个人信息权，最终目的是突出自然人在信息社会的主体地位，突出自然人既有利益的应受保护性。

4.3.1.3 涉个人信息违规行为的认定

《网络安全法》《个人信息保护法》与《数据安全法》被称为护航网络信息安全的“三驾马车”，这三部法律对于个人信息违规行为均有涉及：《网络安全法》规定，“网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息”。“网络运营者不得泄露、篡改、毁损其收集的个人信息”等；《数据安全法》中指出，“任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据”；《个人信息保护法》不仅在总则中明确了“处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息”。“收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。”等原则，对个人信息处理的禁区有了基础的说明，还在第二章、第三章中，具体解释了敏感个人信息、国家机关处理个人信息、个人信息跨境提供等特殊的信息处理中应遵守的规则。

《个人信息保护法》还将国家网信部门、国务院有关部门和县级以上地方人民政府有关部门规定为履行个人信息保护职责的部门，在不同范围内负责个人信息保护工作和监督管理工作，具体职责包括接受、处理与个人信息保护有关的投诉、举报；组织对应用程序等个人信息保护情况进行测评，并公布测评结果；调查、处理违法个人信息处理活动等。

当前，在具体的个人信息数据确权和违规行为认定方面，还缺乏一定的标准和规范。“数据二十条”指出要“畅通举报投诉和争议仲裁渠道，维护数据要素市场良好秩序。”对于个人信息数据的滥用，在采取惩罚措施的同时，也应建立相应个人信息数据滥用的认定及相关标准规范，如建立对个人信息数据违规认定的第三方机构等。

4.3.2 个人信息数据产权机制现状

4.3.2.1 探索个人信息数据产权机制取得的成果

（1）我国个人信息数据法律体系和法治环境不断完善

第一，国家立法与地方立法体系逐渐建立健全。具体表现如下：

在国家立法领域，一方面，我国个人信息保护的基础性法律制度已形成。党的十八大以来，国家高度重视个人信息保护领域的立法，在《消费者权益保护法》《网络安全法》《电子商务法》《民法典》《数据安全法》等立法中，均确立了个人信息保护的主要规则，特别是2021年1月1日起

施行的《民法典》，将个人信息受法律保护作为一项重要民事权利写在了《总则》，在《人格权编》明确了个人信息处理的原则和条件、确立了个人信息主体的权利、强化了信息处理者的信息安全保障义务等，为个人信息保护立法奠定了基础。^①另一方面，近年来国家层面的立法和政策监管还呈现专门化、行业化的新趋势。2022年9月通过的《反电信网络诈骗法》成为我国首部专门聚焦打击电信网络诈骗领域的法律。而《个人信息保护法》实施一年多以来，国家网信办、工信部、国家卫健委、银保监会等多部委纷纷出台了部门立法，持续织密个人信息数据的行业“保护网”。

在地方立法领域，2021年以来，以《深圳经济特区数据条例》《上海市数据条例》为代表的地方数据立法密集出台，明确了数据的人格权、财产性权益。沪深数据立法关注个人信息、数据安全，既与当前三大上位法律^②相衔接，又综合考量了个人信息保护与数据开发利用的法益平衡。具体而言，二者的立法意义又有异同之处：在个人信息保护方面，沪深立法都设置了“个人数据”或“个人信息特别保护”专章，都提出了“数据财产权益”，但区别在于深圳仅规定了数据产品和服务的财产权益，而上海则将保护范围拓展至原始数据，即组织和个人在数据处理活动中形成的合法财产权益。此外，沪深立法均凸显了对消费者权益的保护，进一步规范

^① 三大上位法律，指《网络安全法》《数据安全法》《个人信息保护法》。

^② 《专家解读|上海市数据条例与深圳经济特区数据条例对比分析》，CCIA数据安全工作委员会，<https://mp.weixin.qq.com/s/mJ91jCweoYQgnR1pGkyfk>

基于个人信息的自动化决策和个性化推荐的使用，有力规范“大数据杀熟”等乱象；在个人信息利用方面，《深圳经济特区数据条例》是国内数据领域首部综合性立法，首次对个人信息进行立法确权；上海数据立法则对数据产权进行了开放性的制度安排，“在数字经济发展中有关数据创新活动取得的合法财产权益”被认为有利于激活数据要素的经济价值。

第二，行政执法监管愈发重视个人信息数据保护。针对数字经济发展进程中出现的数据安全和个人信息侵权问题，行业监管机构也逐渐加大了行政执法力度。如监管机构对“滴滴”的处罚等。

第三，互联网司法构筑个人信息数据保护与规范处理的屏障。司法顶层设计层面，最高法、最高检积极出台了一批司法解释及办案指引，并发布个人信息侵权案件办理方面的典型案件，精准助力大数据时代的个人信息司法保护。^①司法实践层面，伴随中国互联网司法的不断进步，以脉脉擅自搜集使用新浪微博注册用户的个人信息案、数据特洛伊之战的“头腾案”、大众点评诉百度案为代表的典型案件，从个人信息数据保护与数据商业利用等层面，为个人信息数据权属的司法认定积累了探索经验。^②与此同时，检察机关在《个人信息保护法》出台后，探索开展个人信息保护领域公益诉

^① 有关司法解释包括《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《检察机关办理侵犯公民个人信息案件指引》等等。

^② 安柯颖：《个人数据安全的法律保护模式——从数据确权的视角切入》，《法学论坛》2021年3月，第2期。

讼，取得积极成效。据统计，2021年，检察机关共办理个人信息保护领域公益诉讼案件2000余件，同比上升近3倍。^①

(2) 大数据产业在个人信息合规保护与合理利用上取得一定成果

第一，平台企业更加重视建立健全个人信息数据合规管理机制。以《个人信息保护法》的实施为重要转折点，国内平台企业尤其是“超级平台”在立法规制和社会监督压力下，更加重视对“大数据杀熟”“算法黑箱”“隐私后门”等热门问题的治理。当前，我国大型平台企业普遍设置了数据安全合规工作机制，头部企业普遍将“个人信息安全和隐私保护”纳入公司企业社会责任或ESG（环境、社会与管治）年度报告中，在个人信息权益保护方面的企业责任感较之此前逐步提升。

场景案例 4

(1) 场景背景：

2017年底，业界首次提出个人数据中心（Personal Data Center，PDC）的理念。经过业界技术专家的不断探讨和迭代，逐步形成了关于个人数据中心PDC的共识，即，个人数据中心是以“还数于民”为核心理念，以区块链底层技术作为安全保障，以分布式存储和计算为基础，以“二次数据”

^① 个人信息保护领域公益诉讼是指检察机关聚焦重点领域、重点行业、特定群体办理公益诉讼案件，对于承担一定公共管理职能和重要社会责任的网络运营者、电子商务平台经营者，探索以民事公益诉讼检察建议方式督促整改，如未及时落实整改，再向人民法院提起民事公益诉讼。

为理论根据，是促进个人数字身份和个人数据资产的确权、流转及二次开发的新型信息基础设施。

（2）场景建设：

世纪互联数据中心有限公司探索个人信息数据产区机制，其个人数据中心具备以下功能：

数据资产化

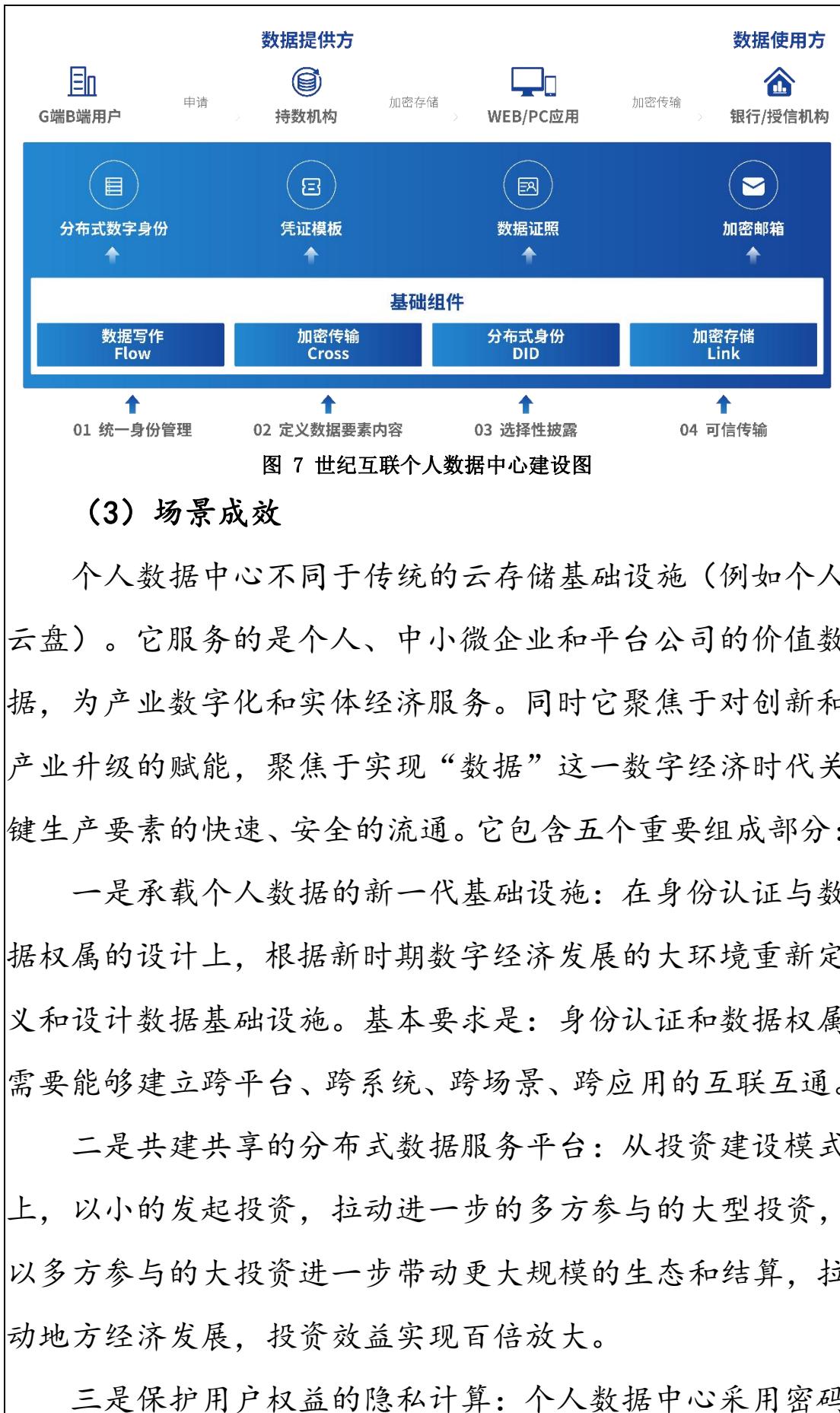
在数据治理的基础上进行数据资产管理。围绕“场景+算法+数据”形成服务型金融资产，并对数据资产进行估值，促进企业数据利用内循环，同时也可成为市场化运营的数据要素产品。

数据确权

实现数据要素从产生、融合、分配、交易、再创造等不同过程中的数据资源持有权、数据加工使用权、数据产品经营权的登记管理，形成可溯源体系。

数据产品交易流通

基于隐私保护的可信数据要素流通技术底座，依托数据要素流通服务管理机制，结合数据应用场景打造面向全国的数据产品流通生态市场。



学技术，包括可验证计算、同态加密和安全多方计算。比如，在同态加密和安全多方计算下，对外提供数据时采取密文而非明文形式，从而使数据具备排他性。这些密码学技术支持数据确权，使得在不影响数据所有权的前提下交易数据使用权成为可能，并构建数据交易的产权基础。区块链技术用于数据存证和使用授权，也在数据产权界定中发挥重大作用。

四是基于共识的数据交换体系：通过安全、可靠、防篡改的技术体系提高数据的质量，通过存证确权、产权溯源保障数据的权利，通过隐私计算保障数据安全，通过监管的机制保障数据的过程可追溯。

五是建立个人大数据协作社群：去中心化商业模式的理念为个人数据的生态建设提供了借鉴和参考。社群的开创精神可真正做到让数据参与价值分配，让数据得到价值量化。通过各界开放合作、加入个人大数据协作社群，形成围绕个人数据研究的开放合作机制，推动国内乃至全球个人数据的政策、技术研究和产业落地。



图 8 世纪互联个人数据中心各部分联系示意图

第二，第三方机构通过探索个人信息保护与确权服务助力“还数于民”。“数据二十条”中的第六条提出探索建立个人信息数据的“受托者制度”，即由受托者代表个人利益，监督市场主体对个人信息数据进行采集、加工、使用的机制。这无疑是促进个人信息数据市场化授权流通的重要利好。相关企业也在积极探索。

场景案例 5

（一）建设背景

《关于构建更加完善的要素市场化配置体制机制的意见》明确要加强数据资源整合和安全保护，提出要研究根据数据性质完善产权性质。该意见是全方位推进要素市场化改革的纲领性文件，将数据与土地、劳动力、资本、技术等传统生产要素并列。数据成为关键生产要素，数据被确定为生

产要素就面临着分配，生产要素的分配就会涉及到交易，而数据交易的正常进行必须以明晰的数据产权为基础。

数据确权要明确数据主体拥有数据产权的边界，区分和界定个人、企业及社会组织、国家等各群体对于数据的权益，这将关系到公民权利、企业竞争、国家安全和全人类福祉等多个方面。

（二）场景建设

2022年6月，人民数据打造了我国首个个人信息保护与确权服务平台“人民数保”，通过公开透明规范协议接口的方式，打通与各大互联网平台的“壁垒”，从而真正实现数据服务于人民、服务于平台、服务于政府。

在技术上，人民数保形成了独特路径：利用区块链技术，将已有协议和服务转换成为PDC的基础组件，形成快速整合和系统集成能力，而非构建一个全栈闭源技术体系。其核心主要有三点：二次数据、一人一链、数据确权。

二次数据是第三方记录并认证的数据。其特点主要有：
1. 权责清晰，认证的记录公开可查；2. 跨角色使用，数据的真实性可以被多方验证；3. 保护用户隐私，避免不合理的重复审核数据。

一人一链是指任意一个人在网络空间内均可利用区块链技术，开辟并拥有一条属于个人的链式结构数据库。该链式数据库具有单向增加、永久存在、可供查询、但不可修改

的特征。用户通过该链及其智能合约对分散在网络空间内的个人数据，开展存储、确权、迁移、交换、分析等全生命周期管理和应用。

数据确权由数字签名和时间戳技术保证，包括：1. 通过在数据发布的过程中，声明利益相关方的权益，来实现数据确权；2. 数字签名。人民数保参与方使用数字身份中所关联的密钥进行数字签名，任何拿到签名数据的人都可以校验签名的真实性，数字签名能够有效的表达利益相关方的权益。3. 时间戳。根据区块链不可篡改的特性，数据一旦上链，记录的时间便被锁定，任何人无法修改区块的发布时间。因此，区块链可以从技术角度有效保证表示一份数据在某个特定时间之前已经存在的、完整的和可验证的“标记”。



图 9 Nexus 手机：第一款基于人民数保的示范产品

（三）场景成效

人民数保在保护个人数据不被非法乱用的同时，对个人有权向个人信息处理者复制的、可携带的个人信息提供确权、上链、存证、存储、治理、流通、收益分配等服务，实现数

据精准确权、授权、流转及二次开发，将个人信息数据权利还归个人，让数据真正取用于民、造福于民，让广大人民群众共享数字化红利。

通过实践和探索，人民数保还助力以下四个方面取得一定成效：

一是为个人用户搭建可信的个人数据迁移和存储服务。人民数保为个人用户提供其在平台公司上原始数据的迁移，通过公开透明规范协议接口的方式打通各大互联网平台，将“原始数据”转换为“二次数据”，为个人用户搭建起一个可信的个人数据迁移通道。由人民云或城市人民云，为每个人提供独立的个人数据中心（PDC）。

二是为平台机构提供数据确权、和数据增值服务。人民数保协助平台公司参与第三方存储的搭建，从而使得个人数据迁移对个人用户和平台公司的双向透明，允许平台公司通过规范化的第三方存储，向个人用户继续提供符合双方利益的增值服务。

三是为政府提供数据归集、数据监管工具。人民数保为地方政府归集政府无法掌握的城市数据提供了新型服务能力，同时为监管部门针对个人数据的统计分析和流转变迁提供了统一的查询和检索入口。赋能监管部门对个人数据的身份、内容、流转、操作等维度进行筛查和审计，有助于构建更为规范的数据市场秩序。

四是确保数据消费过程中的权责清晰。人民数保基于数据权限管理和资源调度机制，利用区块链技术，既防止数据滥用/盗用/泄露，又提供了数据共享的酬劳分配机制。确保了数据消费者在请求、授权和行权过程中的责权清晰，从而促进数据消费者对所授权数据的利用和价值挖掘。

（3）社会组织与行业协会积极打造个人信息数据“治理共同体”

近年来，社会组织与行业协会对于个人信息数据产权机制的探索持续增多，积极打造“数据治理共同体”：科协、互联网协会、大数据协会等社会组织加大了与个人信息保护有关的政策解读、科普宣传，并通过制定行业自律公约来强化对个人信息商业化利用的规范。^①此外，金融、软件信息等重点行业开始探索制定指导性文件，加大对企强化个人信息保护合规管理能力的行业指引。

4.3.2.2 个人信息数据产权机制存在的痛点

（1）执法落地性、精细化与新风险为个人信息数据法治环境带来多重挑战

第一，立法修法层面，执法惩戒标准的模糊性与落地性有待强化。综合当前立法与司法实践中出现的问题与争议，针对《民法典》《个人信息保护法》等已有立法，在个人信

^① 《党的十八大以来我国网络法治建设的成就与经验》，中国法学网，http://iolaw.cssn.cn/zxzp/202208/t20220810_5470349.shtml

息数据保护和利用方面存在如下两类问题，有待进一步通过修法或司法解释加以完善细化：

其一，少数法律法规的原则性较强，为落地实施带来一定难度，个别规则适用标准尚待统一、具体行业规制标准尚待细化。例如，《个人信息保护法》第二十八条第二款规定的敏感个人信息处理原则，条文原文为“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息”，其中的“特定的目的”和“充分的必要性”较为抽象，规则的具体适用仍需细化。

《个人信息保护法》未给出证明做到绝对的“无法识别”或“不能复原”的标准，这方面仍倚赖于具体行业、场景中个人信息处理规范的不断完善。

其二，个人信息侵权责任有待进一步明确，执法惩戒和经济赔偿力度（尤其是隐私侵权）考虑酌情加大，精神损害赔偿方面，《民法典》中规定的侵害人格权“禁令制度”尚需在司法实践中被“激活”。^①

第二，执法机构层面，设置隐私保护专门机构期待高。当前，《个人信息保护法》第60条规定了个人信息的监管机构，但该条中的“有关部门”与“职责范围”并不明晰，隐私权保护的监管机构仍然不明，导致出现主管部门“重前期部署，不重事中与事后督促指导”；主管部门与等级保护

^① 《数字时代个人信息权益司法保护的现状与完善》，《人民法院报》2022年12月29日，第8版。

管理部门沟通机制不畅通，导致出现监管真空。^②此外，缺乏专门的数据管理和隐私保护机构来通过制定相关法规，明确数据权属，强化协同监管，规范数据采集。^③

第三，运用“分级分类”激发个人信息数据产权机制活力需重点强化。分类管理层面，个人信息数据包括敏感数据、隐私数据、身份数据和生物数据，类型庞杂决定了其产权机制的探索必须加以区分类型。有专家呼吁，人格权关系越紧密的隐私数据应禁止流动、与财产权关系紧密的身份数据可以有限制的流动。但是，类型化、场景化的法律保护模式在我国仍有较大的立法完善空间；分级管理层面，虽然金融等一些行业开始探索实施行业性的个人信息分级共享制度，但尚未实现重点行业重点领域“全覆盖”，精细化治理程度有待强化。^{①②}

第四，暗网交易、生物信息泄露、网络虚拟财产权属模糊等新型挑战不容忽视。其一，新型侵犯公民个人信息权益的违法犯罪行为层出不穷，暗网交易、网络“黑灰产”对执法带来新挑战。在暗网数据非法交易中，涉及金融行业的最多，占比高达 34.3%。^③其二，生物识别技术引发的个人信息泄露风险持续攀升，“戴头盔看房”一度引发社会热议。虽

② 《数字时代个人信息权益司法保护的现状与完善》，《人民法院报》2022 年 12 月 29 日，第 8 版。

③ 贾文山、赵立敏：《数据经济时代的个人数据保护》，《首都师范大学学报（社会科学版）》2022 年 12 月，第 5 期。

① 管洪博：《数字经济下个人信息共享制度的构建》，《法学论坛》2021 年第 6 期。

② 安柯颖：《个人数据安全的法律保护模式——从数据确权的视角切入》，《法学论坛》，2021 年第 2 期。

③ 《国家互联网应急中心发布 2019 年中国互联网网络安全报告》，央广网，
<https://baijiahao.baidu.com/s?id=1674712213845645606&wfr=spider&for=pc>

然最高法已发布办理“人脸识别”民事案件司法解释，但类似风险仍将带来“个人信息保护和利用之争”方面的执法难题。^④其三，网络虚拟财产引发的新型数据司法权属争议越来越多。以数字藏品领域为例，有关 NFT 的法律属性以及 NFT 发行者、平台经营者、平台用户的数据权利与义务边界，目前未有统一的执法标准。

（2）平台企业隐私保护、第三方机构从业资质有待产业链创新机制和厘清标准

第一，平台经济统筹发展与安全仍是个人信息数据产权机制探索的重中之重，具体表现如下：

从商业模式与合规机制来看，平台经济难逃为逐利而大量收集用户个人信息数据的现象，面对大型数字平台的优势地位，处于弱势地位的个人要实现对个人信息的决定权，尚待“超级平台”夯实个人信息保护合规制度。而对“超级平台”而言，针对《个人信息保护法》要求其成立主要由外部成员组成的独立机构，有专家认为缺乏第三方组织履行对平台个人信息处理活动的独立监督职能。^①

从授权模式和隐私保护来看，目前多数平台企业过度索要授权，“所有权转移模式”条款、“无限授权模式”条款、“可再许可”类条款、“不可撤销”类条款与用户个人信息

^④ 此处指《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》。

^① 王春晖：《个人信息保护法最大亮点是“两个最小”原则》，《人民邮电报》2021年9月
<https://baijiahao.baidu.com/s?id=1709755074784278790&wfr=spider&for=pc>

权利冲突，损害用户对个人信息的自决权。^①值得注意的是，平台企业中的各类数据承载了大量的隐私信息和肖像信息，该类数据的原始权利归数据主体所有，平台以格式条款概括授权的方式不利于用户人格利益的保护。此外，伴随电子商务和直播电商平台发展，所衍生的侵犯消费者隐私类网络消费纠纷层出不穷。业内认为，隐私保护作为个人信息数据产权机制运行的重要前提，平台企业尚未将其贯穿至数字产品研发到使用的全生命周期，从而缺乏持续性的监督和评估。最高法指出，将推进民法典侵权责任编的解释，加强隐私权和个人信息保护，依法惩治网络侵权行为。未来，在新的数字法治环境中，平台企业如何强化履行个人隐私数据保护的责任和义务，预计还将受到更多关注。

我国《个人信息保护》第十六条规定：“个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。”该条有两项规定，第一项是禁止性规定，即不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；第二项是除外性规定，即信息属于提供产品或者服务所必需的除外。至此，用户不同意 APP 收集个人信息，就无法使用 APP 将视为违法，且收集个人信息也必须限定在“必要个人信息范围”，只要超过“必要个

^① 胡丽，何金海：《互联网用户协议中用户数据授权模式实证研究——以 40 个互联网平台用户协议为样本》，《河北法学》，2022 年 10 月第 10 期。

人信息范围”的收集和处理行为，均属于超范围收集个人信息，必须严格予以禁止和惩处。

从数据流通交易与合理使用来看，未来以“数据二十条”为新契机，平台企业如何以数据安全为前提，尽到保障用户个人信息人格权与个人信息数据财产权的企业责任，同时借助隐私计算等新技术推进对个人信息数据的合理使用，从而释放更高质量的数据要素价值，已成为国内平台经济创新发展所面临的新命题。

第二，第三方机构尚需在实践中丰富“受托者制度”内涵。“数据二十条”中的第六条提出探索建立个人信息数据的“受托者制度”，也为日后的个人信息数据产权机制提出了新问题——受托者、第三方机构一般要具备什么资质、如何承载需求？这些方面尚需经过探索实践来明晰准入资质和从业标准。

（3）社会组织和行业协会、公民需在个人信息保护与利用上形成更大社会合力

个人信息数据产权机制的探索实施还离不开社会力量的协同参与。一方面，重点行业的个人信息分类分级保护管理标准还需要更多社会组织和行业协会参与制定或完善；另一方面，我国当前的个人信息保护意识和隐私侵权维权意识整体不高。不少民众对各参与主体的权利义务边界不甚了解，对个人信息数据与公共数据、企业数据的权属边界认知也就

无从谈起。未来，尚需通过普法宣教在个人信息保护和利用的基本原则上形成更广泛的数字社会共识。

4.3.3 个人信息数据产权机制处理规则与原则

4.3.3.1 对个人信息采集的原则

网络时代，海量的数据和信息以聚合形式存在于社交网络、电子商务、移动智能终端等网络平台，特别是一些大型的网络运营商已经形成对个人数据和信息的实际控制和垄断，公民作为数据内容的主体完全不能控制自己的个人数据和信息，根本无法了解自己的信息和数据在何时、何地、被何人、以何种方式非法收集、使用、加工、传输。事实上，个人信息保护的核心不在于“个人信息”本身，而重点在于如何规制第三人对公民个人信息的收集、使用、加工、传输等行为。因此，公民行使信息权利的基础，是基于公民作为信息内容的主体有权决定其个人信息在何时、何地及以何种方式被何人收集、使用、加工和传输。

企业在采集个人信息时，要以保护个人信息为前提。在2022年底，字节跳动公司内部调查发现有员工不当获取了少量美国TikTok用户的数据，包括两名美国记者的TikTok用户数据，引发舆论质疑TikTok的隐私和数据安全问题。企业如何合法合规采集个人信息，保护信息安全备受关注。

从相关法律法规要求及企业在数据采集时集中暴露的问题看，企业需要坚持精准化、最小化、知情自愿等原则，

才能更好地做到合规，规避风险。

一是坚持精准化原则，不能“一揽子授权”和强制同意，企业在采集个人信息数据中，不得采取“一揽子授权”，而是要根据双方或多方基于合作目标约定的授权进行精准采集，同时，如果被授权主体发生变化，需要授权方与被授权方重新授权。“数据二十条”提出：“对承载个人信息的数据，推动数据处理者按照个人授权范围依法依规采集、持有、托管和使用数据，规范对个人信息的处理活动，不得采取‘一揽子授权’、强制同意等方式过度收集个人信息，促进个人信息合理利用。”个人信息处理者在处理个人信息时确需授权且授权信息中含有个人隐私要素且涉及两者及两者以上时（个人隐私要素包括但不限于个人联系方式、地理位置、相机相册、浏览数据、设备信息、订单信息等个人信息数据授权；向个人进行信息推送、商业营销；数据处理自动化决策等），应该为个人提供不同的授权方案。个人信息数据应该分级、分类授权，不能“一揽子授权”，允许个人针对具体使用情况授权不同的个人信息数据内容，改变一键授权的模式。

2022年12月26日，国家市场监督管理总局依据反垄断法对同方知网（北京）技术有限公司做出行政处罚规定，业内人士分析称，知网滥用市场支配地位，本质是权属问题不清。因此，企业在采集个人信息数据过程中，需要坚持精准

化原则，单面授权，避免“一揽子授权”。

二是最小化原则，即企业只能采集业务相关的信息数据，避免过度采集。据消费者个人信息保护调查报告显示，消费者个人信息被过度采集现象严重。国家计算机网络应急技术处理协调中心、中国网络空间安全协会发布的《App 违法违规收集使用个人信息监测分析报告》显示，App 超范围收集个人信息的问题目前主要包括七种情形：敏感权限声明超出必要范围、权限索取超出必要范围、收集数据的敏感性超出必要范围、收集数据的具体内容超出必要范围、收集方式超出必要范围、收集频率超出必要范围、收集场景超出必要范围。王春晖指出，关于 App 超范围收集个人信息的情形，主要有三类：一是 App 收集无关信息；二是 App 强制收集非必要信息；三是 App 收集频率不合规。

国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局等部门多次对企业超范围采集行为进行通报、查处，起到了一定的震慑作用，但是超范围收集和使用个人信息等行为依然存在。《常见类型移动互联网应用程序必要个人信息范围规定》明确对“必要个人信息”做出了定义：必要个人信息是指，保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。基于该定义及实践，立法明确企业采集个人信

息的界限，规定“最小化原则”呼声越来越高。

三是以“告知—知情—同意”为核心，知情自愿原则，即企业在采集数据时，告知被采方采什么数据、数据用途等，明确被采集方已对数据采集和用途知情，被采方自愿同意授权采集方使用采集的数据。《个人信息保护法》不仅确立了以“告知—同意”的个人信息处理规则，而且构建了以“告知—知情—同意”为核心的个人信息处理规则体系。个人信息处理者“告知”的目的是为了确保被告知者的充分“知情”，只有被告知者在充分知情的前提下才能自愿明确地做出决定。此外，《个人信息保护法》第14条明确规定：基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出，法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。^①

越来越多的平台企业、第三方机构在个人信息数据产权机制方面开启进一步探索，并提供多种解决方案。

场景案例 6

（一）建设背景

当前，私人数据隐私保护面临的以下几个问题：1. 用户隐私授权粗暴一刀切，要求用户一键授权全部信息，收集信息过量（如手电筒搜集用户通讯录信息）；2. 隐私政策描述太过专业，用户看不懂或者不能理解；3. 用户端对于授权后

^① 王春晖，中国个人信息保护立法这十年，微信公号“上海市法学会”，2022年10月26日，<https://mp.weixin.qq.com/s/y-116L8BHAV0928guQTzdQ>

的风险，并无明显感知（不清楚我都确认过什么，我都交出了什么）；4. 用户隐私授权不确认无法继续，及无规范与监管。

（二）场景建设

针对私人数据隐私保护存在的问题，人民数据联合隅西科技从授权、确权、行权三个层面为平台企业提供解决方案。在授权方面，改变一键授权的模式，设计多种用户隐私政策权限选择方向及对应权限，允许授权不同的内容和信息。并留有入口，允许用户取消已授权内容。

在确权方面，人民数据联合隅西科技构建提供三种告知及引导方式：第一是调查问卷。供个人针对性了解该授权信息对应的权限，根据个人调查问卷的反馈内容，给个人提供最适合的授权方案的建议；第二是授权风险手册的讲演。通过案例讲解或视频呈现，保证个人从实际案例的学习中对授权个人信息的风险点知情；第三是法务咨询。提供咨询入口，一对一解答个人信息数据安全相关问题，保障个人知情权。在处理个人信息时需基于个人同意，且该同意是在个人充分知情的前提下自愿、明确作出，保障个人同意权。

授权 用户隐私政策权限选择方向示意及对应权限



图 10 用户权限授权场景示意图

基于个人同意处理个人信息的，个人有权撤回其同意，个人信息处理者应当提供便捷的撤回同意的方式，如为个人提供“授权管理—取消已授权内容”的入口，且入口应明显、便于操作。在行权方面，使用智能化处理方式。通过标识系统，一键接入客户的数据，根据客户的需求，收集用户数据，并进行监督。此外，还可根据用户授权的不同的隐私信息内容，划分分组，在合法合规符合用户需求下触达。

(3) 场景成效

通过该场景的建设，一方面保护个人信息，另一方面充分利用个人信息的海量数据，达到以下几个方面作用：

深改革：通过改革，切实打通数据，深耕于数据，实现数据开放共享。

明数权：加强数据要素基础制度建设，保障数据安全性，把握政府与市场的关系，建立数据标准和制度，推动政府、企业和社会多方协同。

搭平台：通过搭建平台，为政府、企业和社会服务。为各地政府、各类企业提供精准招商和产业数据服务。

享红利：数字时代应共享数据红利。

4.3.3.2 处理与应用个人信息的原则

个人信息具有财产属性，但是个人信息主要涉及的是自然人的人格权，这其中就包括大量的个人隐私信息。我国《民法典》“人格权编”（第四编）第六章专门就个人信息中私密信息的保护作出规定，即“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。”为了保障使用个人信息数据时的信息安全和个人隐私保护，“数据二十条”建议，要创新技术手段，推动个人信息匿名化处理。我国《个人信息保护法》第四条规定：“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。”

《个人信息保护法》关于个人信息的定义，与我国《民法典》《网络安全法》、最高法、最高检《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》以及欧盟的GDPR关于个人信息的内涵最大的不同在于增加了“不包括匿名化处理后的信息”。

这从法律层面上确认，个人信息经匿名化处理后，数据处理者采集、持有和使用的信息就不属于个人信息，无须适用个人信息保护法的相关规定。《个人信息保护法》第七十

三条（四）将“匿名化”定义为：“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。”将经过匿名化处理后的个人信息排除在个人信息保护法的框架之外，对于促进个人信息的合理利用具有巨大的数据要素价值。

（1）遵循合法、正当、必要和诚信原则

《消费者权益保护法》第二十九条、《网络安全法》第四十一条均有明确规定，经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。此外，《个人信息保护法》还强调了诚信。其第五条规定，处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。该原则对企业利用大数据分析、评估消费者的个人特征用于商业营销的行为进行了约束。

以“大数据杀熟”为例，一些电子商务平台经营者利用大数据分析、算法等技术手段，根据消费者或者其他经营者的偏好、交易习惯等特征，基于成本或正当营销策略之外的因素，对同一商品或服务在同等交易条件下设置不同价格。这种行为严重损害了消费者的权益，也违反了合法、正当、必要和诚信的原则。

（2）处理个人信息应当遵循公开、透明原则

《个人信息保护法》第七条规定，处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目

的、方式和范围。结合其第十七条、第三十条规定，明示的内容至少包括：第一是个人信息处理者的名称或者姓名和联系方式；第二是个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；第三是个人行使本法规定权利的方式和程序；第四是法律、行政法规规定应当告知的其他事项；第五是如果涉及敏感信息处理，需明示处理敏感个人信息的必要性以及对个人权益的影响。在实践中，此等明示义务通常可通过《个人信息保护规则》（或称《隐私政策》）、弹窗单独告知等形式实现。

（3）应当保证个人信息质量原则

《个人信息保护法》第八条至第九条规定，处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响，同时个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。基于以上法规内容，信息处理者在处理个人信息时应当以保证个人信息质量为原则。

一是在准确性方面，个人信息处理者应综合考虑所收集个人信息的目的，开展必要的个人信息完整性和准确性审核。二是在可问责性方面，《个人信息保护法》第五十二条规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

三是在数据安全性方面，《个人信息保护法》第五十一条规定，个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等制定内部管理制度、实行分类管理、采取安全技术措施、确定个人信息处理的操作权限、定期进行安全教育和培训、制定并组织实施个人信息安全事件应急预案。

（4）应遵循匿名化原则

敏感个人信息一旦泄露或者被非法使用，极易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。个人信息处理者在处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息时，应当遵循匿名化原则。原因有两点：一是保护个人信息权益，二是促进个人信息的合理利用。

对于“个人信息”的定义，《网络安全法》《民法典》《个人信息保护法》中均强调了“已识别或者可识别的自然人有关的各种信息”内涵。但是，在《个人信息保护法》中，增加了“不包括匿名化处理后的信息”的补充，明确了经匿名化处理后的信息不属于个人信息，无须适用个人信息保护法相关法规。这体现了《个人信息保护法》的实质目的是在保护个人信息权益的基础上，促进个人信息合理利用。^①

《个人信息保护法》第七十三条（四）对“匿名化”的

^① 《王春晖：“个保法”一周年，对十一个亮点和展望的思考》，中国工信产业网，https://www.cnii.com.cn/rmydb/202210/t20221031_424615.html

定义为：“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。”但从操作层面来看，《个人信息保护法》未给出证明做到绝对的“无法识别”及“不能复原”的标准，个人信息处理者可根据具体行业、场景中的相关数据处理规范实施。例如，国家互联网信息办公室等5部门发布的《汽车数据安全管理若干规定（试行）》第八条指出，因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。

（5）应遵循可被遗忘原则

随着大数据与人工智能的发展，智能设备、传感器等应用无时无刻记录着人们使用电子设备的行动轨迹，大量的用户痕迹数据被记录，同样面临随时被泄露的风险。被遗忘原则就是指数据主体应享有个人对数据的控制权，享有对自身不同形式留下的数据痕迹的可删除，取得被遗忘的基本权利。

随着“数据生命周期”与人自身生长周期的变化，数据保存的实际效应也会随着数据本身的准确性和有效性不断递减。因此建议，从国家标准的角度出发，个人信息保存期限应为实现目的所必需的最短时间，即个人信息的保存期限不能超过实现目的所需的最短时间。数据主体在不影响社会评价的基础上理应可通过行使被遗忘权，避免自身相关数据

不必要的泄露，增加不必要的风险。

第四节 推动数据产权的技术发展与应用

4.4.1 现有技术在数据产权的探索

数据产权是数据法律体系中的基础性规则，对激活数据要素市场、促进数字经济发展具有根本性意义。进入信息时代，各类数据在生产经营活动中的作用日益凸显，并成为不可代替的生产要素。在数据使用过程中，应当保障数据不被窃取，数据产权不被恶意侵犯，其中较为重要的技术是隐私计算。

隐私计算是一种提供数据隐私保护并实现数据价值挖掘的技术体系，可以在满足数据隐私安全的基础上对数据进行计算和分析，实现数据安全流动与共享，推动数据产权的发展。一般而言，隐私计算指为保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，实现数据在流通与融合过程中的“可用不可见”。隐私计算是一个技术领域，或者是一系列技术集合，它要实现的目标是保证数据隐私不泄露的情况下实现计算分析。^①

隐私计算的技术路径主要分为三大类：以多方安全计算为代表的密码学路径、以联邦学习为代表的机器学习路径和以可信执行环境为代表的硬件路径。

^① 中国信息通信研究院. 联邦学习场景应用研究报告（2022）[R]. 2022.

4.4.1.1 多方安全计算

多方安全计算 (Secure Multi-party Computation, MPC) 始于姚期智教授 1982 年提出的“百万富翁比财富”问题，即两个百万富翁如何在不借助第三方且不透露自己财富总量的前提下比较谁更富有。多方安全计算用于解决在一组互不信任的参与方之间保护隐私的协同计算问题，确保输入的独立性和计算的准确性，同时不将输入值泄露给其他参与方。

目前多方安全计算中主流的技术包括同态加密、秘密分享、不经意传输及混淆电路等。

一是同态加密 (Homomorphic Encryption, HE)，它是一种加密函数，对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。根据支持密文运算的程度，同态加密可分为全同态加密和部分同态加密。部分同态加密仅支持有限的密文计算深度，仅支持同种加密运算即同乘或同加。全同态加密可同时满足加同态和乘同态性质，是可以进行任意多次加和乘运算的加密函数。

二是秘密分享 (Secret Sharing, SS)，它的思想是将数据以适当的方式拆分成多个无意义的数，拆分后的每一个数由不同的参与者管理，单个参与者或者少数几个参与者无法恢复原始数据，只有若干个参与者一同协作才能恢复原始数据。通过拆分原始数据，将秘密分散到一群参与者中，能

有效地防止系统外敌人的攻击和系统内用户的背叛。基于秘密分享的多方安全计算可支持加减乘除及多项式运算。

三是不经意传输（Oblivious Transfer, OT），它是构建 MPC 的一个常用协议。在 OT 中，参与方 Alice 提供一组数据，另一方 Bob 从中选择一个数据，OT 协议能保障 Alice 不知道 Bob 获得了哪个数据，Bob 有且只能获得一个数据。

四是混淆电路（Garbled Circuit, GC），它又称姚氏电路（Yao's GC），是姚期智教授于 1986 年针对百万富翁问题提出的解决方案，由安全多方计算协议，通过加密门电路完成 MPC。在 GC 中，所有的计算逻辑都被表示成门电路，Alice 将自己的数据、门电路的所有可能执行路径加密后传递给 Bob，其根据自己的输入依次执行各个门电路，并获得密态形式的最终结果。

多方安全计算采用的是密码学的路径，要求敏感的中间计算结果也不可泄漏，在近四十年的发展中其核心技术不断接受学术界和工业界的检验，具有很高的可信性。

4.4.1.2 联邦学习

联邦学习（Federated Learning, FL）本质上是一种分布式的机器学习框架，由 Google 于 2016 年首次提出^①。其核心思想是在多个数据源共同参与训练时，无需各方提供自己的本地数据，仅通过交换中间参数（例如模型参数、梯度

^① McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. PMLR, 2017:1273-1282

等) 来实现模型的联合训练。在这个过程中, 原始数据不出本地, 中心节点无法看到原始数据, 只能得到模型结果, 因此有效地保证了数据的隐私。

典型的联邦学习过程(见图 11): ①是聚合服务器将全局模型下发至各个参与方, 每个参与方得到初始本地模型; ②是各参与方利用本地数据训练初始本地模型; ③是各方将模型更新(例如模型参数、梯度等)上传至聚合服务器; ④是聚合服务器采用一定算法聚合各方上传的更新, 得到新的全局模型, 至此完成一轮迭代过程。重复步骤 1—4, 直至全局模型收敛或达到所需精度要求。

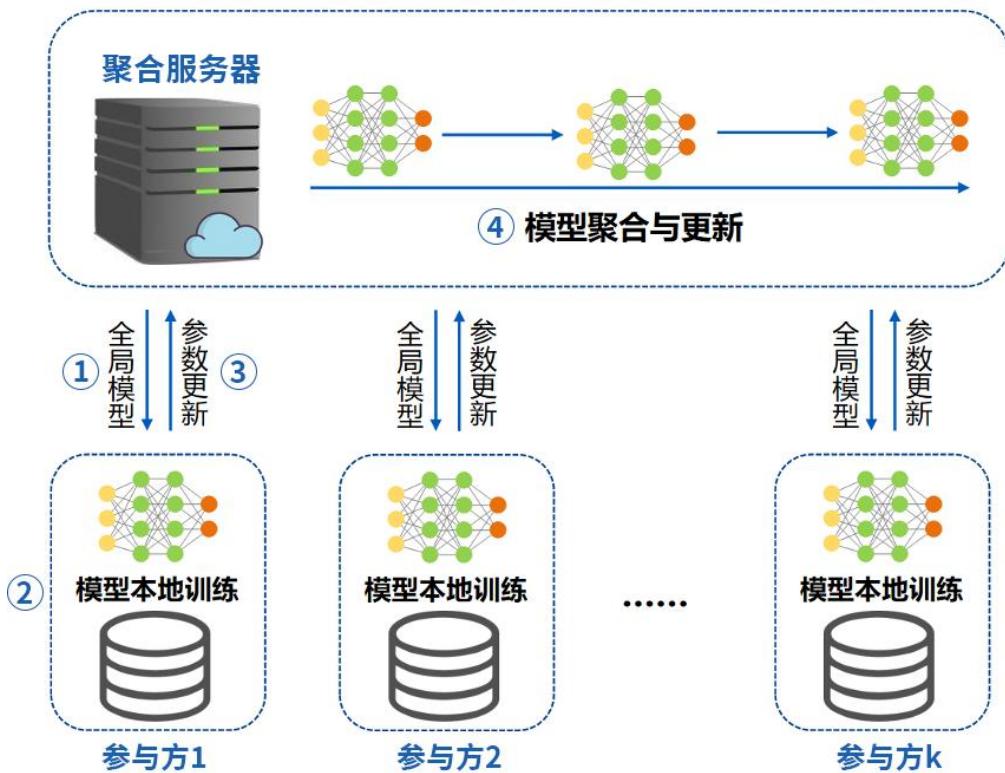


图 11 联邦学习流程图

在联邦学习过程中, 中央聚合服务器得到的只是模型更新而非原始数据, 既保证了各方数据不出本地, 又完成了协

同训练的任务，适用于多种场景需求。例如，由于法律限制而不能共享某些数据库的情况下，联邦学习可以使得需求方避免获取原始数据，而同时得到需求结果。同时联邦学习也可以结合同态加密、差分隐私等技术进一步提高数据协作过程中的安全性。^①

根据联邦学习各参与方拥有数据的情况，可以将联邦学习分为以下三类^②：

一是横向联邦学习：在两个数据集的用户特征重叠较多，而用户重叠较少的情况下，把数据集按照横向（即用户维度）切分，并取出双方用户特征相同而用户不完全相同的那部分数据进行训练，其本质是不同客户之间样本的联合。Google AI 团队提出联邦学习算法框架应用于移动互联网手机终端的单词预测就是典型的横向联邦学习场景。

二是纵向联邦学习：在两个数据集的用户重叠较多而用户特征重叠较少的情况下，把数据集按照纵向（即特征维度）切分，并取出双方用户相同而用户特征不完全相同的那部分数据进行训练。比如同一地区的银行、医院、运营商想要共同训练一个模型，他们的用户集包含该区域的大多数居民，但银行记录的是用户的收支行为的信息，医院记录的是用户的就诊记录，运营商记录的则是用户的通讯信息等，三者的特征空间存在很大的不同。假设我们希望对用户进行信用评

^① 中国信息通信研究院安全研究所, 阿里巴巴集团安全部, 北京数牍科技有限公司. 隐私保护计算技术研究报告 (2020 年). [R]. 2020.

^② 中国信息通信研究院. 联邦学习场景应用研究报告 (2022) [R]. 2022

估，则需要融合三方数据来共同训练一个预测模型，纵向联邦学习即是将这些不同的特征聚合在一起，利用多方数据协作构建一个模型。

三是联邦迁移学习：在两个数据集的用户与用户特征重叠都较少的情况下，不对数据进行切分，而利用迁移学习克服数据或标签不足的情况。比如两个机构，一个是位于北京的电商平台，一个是位于杭州的物流公司。由于地域限制两个机构的用户群交叉点小，由于业务不同，双方的特征空间重叠也少。这种情况下可以利用迁移学习来克服数据与标签的不足，需要从公共样本获取公共表示，用于获取具有单侧特征的样本预测。（见图 12）



图 12 联邦学习分类

由于法规或商业机密等原因，很多行业的数据不能直接聚合用于训练机器学习模型，这些行业涵盖金融、医疗、政务、教育、智慧城市、边缘计算、物联网、区块链等。联邦学习作为能够在满足隐私、安全、合规的前提下，使用分散于多方的数据构建共享和定制化模型的机器学习建模机制，在诸多领域都有广阔的应用前景。

4.4.1.3 可信执行环境

可信执行环境（Trusted Execution Environment, TEE）指的是为保障数据和代码的保密性和完整性，设置的一种独立于系统其他部分的处理执行环境，该环境包含了记忆存储设备和计算能力，可以抵御软件层面的外界攻击和硬件层面系统主存储器的攻击。作为一种基于硬件的技术，可信执行环境强调通过软硬件方法在中央处理器中构建一个安全飞地（Security enclave），并基于该安全飞地进行计算操作，未经授权则无法查看数据或者执行操作，其安全可信性离不开硬件厂商的配合。

目前主流的 TEE 技术以 X86 指令集架构的 Intel SGX 和 ARM 指令集架构的 TrustZone 为主。这里以 TrustZone 为例介绍一下 TEE 在隐私保护中所起的作用。在同一颗 ARM CPU 上存在着两套系统（见图 13），左边蓝色部分 Rich OS Application Environment (REE) 表示用户操作环境，可以运行各种应用，例如电视或手机的用户操作系统，图中右边绿色部分 Trusted Execution Environment (TEE) 表示系统的安全环境，运行 Trusted OS，在此基础上执行可信任应用，包括身份验证、授权管理、DRM 认证等，这部分隐藏在用户界面背后，独立于用户操作环境，为用户操作环境提供安全服务。^①

^① 隐私计算联盟，中国信通院云大所. 隐私计算白皮书（2021 年） [R]. 2021.



图 13 ARM TrustZone 架构

与密码学路径的相关技术不同，可信任执行环境主要由特殊的硬件提供外在的安全环境。在实际运行时，数据以明文形式进行，因此在运算速度上具有优势。

4. 4. 1. 4 隐私计算对数据要素流通具有重要支撑作用

隐私计算给数据产权带来了安全和隐私保证，对数据要素流通具有重要支撑作用，要结合数据保护影响评估的合规工具，进一步推动数据产权的发展。此外，隐私计算中不同的技术路径有着自己的优势和应用场景，需要结合实际合理选择使用：多方安全计算安全性有很高的保证，但所需的算力资源大，计算耗时较长，效率较低，适用于数据规模不大，计算复杂性低的场景。联邦学习计算速度快，易拓展，但因其是分布式的框架，需要众多参与者经多轮迭代才能完成计算，对通信效率要求较高。可执行环境的通用性和效率更

为优秀，但研发成本高，对硬件依赖程度高，需要相关硬件厂商配合，适用于计算复杂性高且对通信效率敏感的场景。总的来说，各项技术互有优劣，仍需提升通用性、安全性和性能以满足更为广泛的数据产权保护需求。^①（见表 8）

表 8 隐私计算各技术路径总结

技术名称	安全多方计算	联邦学习	可信执行环境
通用性	高	中	高
安全性	高	中	中
计算性能	低	中	高
适用场景	简单逻辑运算场景	复杂建模计算场景	复杂逻辑计算场景
优势特点	无需第三方参与、数据 安全性高	原始数据不出本地、算 力成本低	域内无算法限制、数据 信息无损耗
技术局限	计算通信开销大，计算 耗时长	通信成本高、隐私保护 无密码学验证	开发部署难度大、需要 信任硬件厂商

4.4.2 数据产权技术方面的未来发展

目前隐私计算正处于快速发展阶段，可一定程度解决企业、政府、机构和个人面临的数据合规问题，为数据产权提供有力的技术支撑。在政策的持续推动下，隐私计算技术不断更新，体系也逐渐完善，场景更加丰富，发展一切向好。但是隐私计算也存在一些未来需要克服的困难，唯有努力解决这些苦难和挑战，方能持续绽放活力，服务每一个人。

4.4.2.1 完善相关法律法规，加速技术与法律融合

近年来国家针对数据隐私已经出台多部法律法规和相关指导要求，我国的隐私相关法律体系正处于不断建设与完

^① 隐私计算联盟. 隐私计算应用研究报告（2022 年） [R]. 2022.

善的阶段。可以预见在不久的将来，法律与政策层面将持续完善，特别是针对数据交互、数据共享、数据产权等方面政策要求。

隐私计算不应只关注技术的实现，更应该关注相关法律法规的指导，要将技术与法律融合，发展符合法律要求的隐私计算技术。隐私计算技术所带来的数据“可用不可见”的价值更普遍地被理解为能够助力解决数据安全性问题。但数据是否被合法、公平地处理，处理的结果是否对个人或公众造成侵害或影响，数据产权是否受到侵害，更是当今大数据时代所面临的重要问题。我们需要对这一技术保持全面、客观的认识，应当将技术与制度规则进行有机结合，实现保护数据主体、维护社会公众利益与促进规范有序的数据要素市场秩序的目标。

4.4.2.2 推动技术融合发展，实现隐私计算的统一

目前主流的隐私计算技术都存在一些局限，例如多方安全计算速度慢、联邦学习的安全性没有密码学保证、可信执行环境需要硬件厂商配合等，为解决单一技术带来的局限，将隐私计算应用到更为广阔的场景，多技术融合提供了一定的思路，在某些场景下甚至可以产生“ $1+1>2$ ”的效果，有助于推动数据产权技术的未来发展。

联邦学习与多方安全计算融合，利用多方安全技术对联邦学习中用户上传的梯度进行加密，使用户的梯度对服务器

不可见，增强中间计算结果的安全性，可以实现模型的安全聚合，弥补联邦学习缺乏密码学验证的缺点。如通过秘密分享的方式完成模型聚合更新或使用全同态加密的方式在密态环境下完成模型训练。

联邦学习与可信执行环境融合，联邦学习的用户可以在可信执行环境内完成模型的本地训练，本地的隐私数据也可以放在可信执行环境所规定的安全内存中，借助可信执行环境的可靠性和隔绝性，保护相关数据的安全与隐私，从而增强整个联邦学习系统的安全性。

4.4.3 数据交易所等数据产权探索

从国际上来看，在数据确权尚没有成熟完善的技术方案情况下，各国对于数据产权的制度设计各有侧重。如美国并未针对数据要素进行综合立法，而是选择在传统隐私权的框架下，以“信息隐私权”来保护个人的隐私权利，从而回避了所有权问题。欧盟将数据划分为“个人数据”和“非个人数据”来实现自然人人权的保护和数据流动、开发的平衡。

“数据二十条”提出的“三权分置”数据产权制度框架，构建起具有中国特色的数据产权制度体系。一些数据交易所与相关机构已针对数据产权进行了一些尝试和积极探索。

2022年7月29日，北京国际大数据交易所数据资产登记中心揭牌。数据交易是释放数据要素红利的关键环节，但在实践中还面临“确权难、定价难、入场难、互信难、监管

“难”等问题。开展数据资产的权属登记能够进一步激发交易主体积极性，推动更多高价值数据交易流通，进而激活数据要素潜能。数据资产登记中心作为数据进入流通环节的核心机构，是北京市构建数据要素核心基础设施、推进数据要素市场化流通的重大探索。

上海数交所已在数据权属界定方面做了三方面探索：一是紧扣建设国家数据交易所的定位，明确“规范确权、统一登记、灵活交付、集中清算”四大特征，在自行开发的 niDts 新一代智能数据交易系统和全国数据资产登记系统中，将“规范确权”融入登记和交易的主要环节；二是牵头上海市数据交易相关地方标准的制定工作，紧密围绕数据产权制度，将“数据二十条”中三权结构性分置的产权设计转化为可落地的地方标准；三是深度参与数据知识产权保护工程上海试点工作，如合作搭建数据知识产权登记服务平台，打通数据交易平台系统，实现数据知识产权登记、保护、存证、交易、备案“一站式”发展。在分类分级确权授权方面，上海数交所建立了“数据分级”和“分级交付”的基本架构和技术路线，并挂牌了 800 多个数据产品，其中绝大部分是不敏感或低敏感的企业数据，涉及金融、交通、工业、通信等 12 个行业领域。

深圳数据交易所围绕数据资源产权、交易流通、收益分配、安全治理等领域基础制度和技术标准，构建全面、系统

的交易场所制度规则体系。现已制定发布 12 项交易规则和管理制度，正在制定 9 项技术标准和规范，并参与 6 项国家、地方标准制定。2020 年 10 月发布的深圳综合改革试点实施方案就明确“加快培育数据要素市场”，包括率先完善数据产权制度，探索数据产权保护和利用新机制，建立数据隐私保护制度。2022 年 11 月 29 日，由深圳市标准技术研究院开发建设的国内首个专注数据知识产权登记的信息化系统——“数据知识产权登记系统”正式上线。深圳市市场监管局印发《数据知识产权登记试点工作方案》，明确为经过一定规则处理的、具有商业价值的非公开数据提供数据知识产权登记服务。

深圳市标准技术研究院按照《数据知识产权登记试点工作方案》建立了配套制度规范，依托深圳市知识产权保护综合服务平台和数据知识产权登记系统，为数据处理者提供“数据哈希值存证—登记申请—材料审核—信息公示—证书发放”全流程服务。数据知识产权登记系统上线后，深圳市前海数据服务有限公司、广东省坤舆数聚科技有限公司及深圳市众信电子商务交易保障促进中心等多家机构发起申请，数据涉及经济指标、科技创新、自然资源监测、电子商务等领域。2022 年 12 月 9 日，在经过审核与公示后，深圳市前海数据服务有限公司、广东省坤舆数聚科技有限公司获颁“数据知识产权登记证书”。

浙江省市场监督管理局印发了《浙江省数据知识产权制度改革试点方案》。试点方案以数据知识产权登记为核心，在国家知识产权局指导下，根据《浙江省知识产权保护和促进条例》，深入开展市县数据知识产权相关调查研究，立足浙江实际谋划制定，遴选了14个市、县（市、区）作为首批省级试点地区。试点方案包含了工作背景、目标体系、工作体系、政策体系、评价体系和保障措施等6个方面内容22项工作举措，在深化数据知识产权理论研究、开展数据知识产权登记、促进数据知识产权运用、加强数据知识产权保护等方面作出试点工作部署，从组织领导、协同联动、经费保障等方面制定试点工作保障措施。

第五章 建立健全数据要素各参与方合法权益保护制度的思考

“数据二十条”指出，建立健全数据要素各参与方合法权益保护制度。在建立健全权益保护制度时，对数据来源者、数据处理者、数据经营权都有明确的要求：充分保护数据来源者合法权益，合理保护数据处理者对依法依规持有的数据进行自主管控的权益，保护经加工、分析等形成数据或数据衍生产品的经营权。

依法承认和保护数据要素所有参与方的权益，合理界定数据要素市场各参与方的权利和义务。保护数据来源者和数据处理者的各项合法权益，界定数据生产、流通、使用过程中各参与方享有的合法权益，推动基于知情同意或存在法定事由的数据流通使用模式，保障数据来源者享有获取或转移由其促成所产生数据的权利以及数据处理者使用数据和获得收益的权利，才能在多元利益主体间构建激励相容的数据权益分配与保护机制。

建立保障权益与合规使用的数据产权制度，应当在确保各参与方数据产权关系清晰的基础上，依靠数据产权规则使数据资源持有者、数据加工使用者、数据产品经营者承认和尊重数据产权制度，并合理与合规地行使数据资源持有权、数据加工使用权、数据产品经营权（三权），如果违背或侵犯它，就要受到相应的制约或制裁。

蓝皮书从建立健全数据要素各参与方合法权益保护制度的角度提出一些思考和方向，助力行业标准加快建设，推动数据确权授权平台搭建，为行业提供示范作用。

第一节 保护数据来源者合法权益

数据来源者包括数据的收集者和数据的产生者，也包括通过转让的受让方。如果数据来源者的数据来源正当合法、必要且诚信地取得数据，数据来源者的合法权益就须得到承认和保护，确保数据来源者享有获取或转移由其促成所产生的数据的权利。

5.1.1 保障知情同意权、可携带权和收益权

近年来，个人信息安全风险事件频发，个人信息关涉人格尊严与个人生命、财产安全。企业对个人信息的收集、使用等行为应当遵循合法、正当、必要原则，特别是在处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息时，应取得用户“单独同意”。

目前，数据来源者的“同意”存在有效性难题，企业获取个人信息告知形式化，存在“告而不知”现象。此外，还存在数据来源者对同意后果认知不足、缺乏知情主动性及被迫同意等现象。知情同意原则应是个人信息保护中的一项重要原则。在数据处理者与数据来源者的不平等关系中，数据来源者的同意是对数据处理者的最佳限制，要完善知情同意原则的规范结构及适用过程中的立法保护。

5.1.1.1 保障数据来源者的知情同意权

由于数据的“可复制性”特征，造成数据来源者的数据在被使用、处理时出现不知情的情况，因此，保障数据来源者的知情同意权尤为重要。以个人信息为主的数据来源者的数据在利用时必须保障“充分知情”，《个人信息保护法》中就明确指出个人在个人信息处理活动中的权利包括知情同意权。

数据处理者和利用者在采集、产生数据时，必须告知数据来源者数据的内容、用途等，数据来源者需自愿同意授权才能处理和使用。

5.1.1.2 保障数据来源者的可携带权

数据可携带权指当数据控制者基于数据主体的同意或者基于合同的约定，以自动化的方式处理个人数据时，数据主体有权获取其提供给数据控制者的数据副本（副本获取权），同时有权不受原数据控制者阻碍的将个人数据转移至另一个数据控制者（数据转移权）。

数据来源者的数据具有转移的权利。《个人信息保护法》明确规定，个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。保障数据来源者的数据可携带权，有助于健全数据要素权益保护制度，建立合规高效的数据要素流通和交易制度，促进数据产业合作共赢。

5.1.1.3 保障数据来源者的收益权

数据来源者提供数据，尤其是承载个人信息的数据，应按《个人信息保护法》界定其处理和收益行为，并保障数据来源者的收益权。

保障数据来源者的收益权，就要打破超级平台实施数据封锁、构筑封闭生态系统等行为，弥补个人用户和平台企业之间的数据收益分配失衡，保障以个人为主的数据来源者的数据收益权。

5.1.2 法律、平台、标准共同保护合法权益

保护数据来源者的合法权益，需要从法律层面、平台层面、标准体系建设层面等共同发力，共同维护数据来源者知情同意权、可携带权和收益权，为数据要素产权制度的建设打下坚实基础。

5.1.1.1 完善顶层设计，构建完备的数据流通法律体系

目前我国已出台《数据安全法》《个人信息保护法》等一系列法律法规，搭建起数据基础制度框架，在实际操作中，对于数据确权流通、保障数据来源者合法权益等方面，缺少可操作性的法律制度，完善顶层设计势在必行。

政府作为个人信息保护的责任主体，应建立专门的数据管理和隐私保护机构，通过制定相关法律法规，加强数据开放审核力度，强化协同监管，规范数据采集方式，严厉打击非法数据交易，切实保障公民合法享有数据使用的知情同意

权、移转权等。此外，法律还应积极推动企业采用高效、流程化的数据合规管理体系，如建立隐私管理部门、规划数据保护战略等，将保护隐私数据贯穿数字产品全生命周期，并持续进行监督。

5.1.1.2 落实平台责任，实现数据收集者充分告知义务

有学者认为，在我国，目前信息收集者主要采取用户协议或隐私协议这些格式协议的方式来履行告知义务，并且很容易通过文字游戏来规避告知义务责任的承担。所以在今后的立法中，需要对信息收集者的告知义务和形式要求进行确定，明确企业的告知义务并且设置相对应的惩罚措施。此外，还可改变告知的形式或制定统一的“知情同意”模板，如通过第三方机构或行业协会来保护个人信息，将隐私协议中经常出现的条款进行统一文字定义，使其变得简单易懂，实现数据收集者充分告知的义务责任。

信息监管部分还可引入知情同意原则中的白名单和黑名单机制，通过黑名单机制向社会发布风险预警，通过白名单机制激励企业和平台合规。

5.1.1.3 细分同意类型，制定信息分级分类的保护制度

我国对于一般性与敏感性的个人信息采用同等保护模式，导致知情同意原则流于形式化，应细分“同意”类型，将不同级别、不同类别的个人信息分别对应不同的同意层级。未成年人、公众人物等特殊主体的个人信息数据设立特殊的

同意规则，达到强化对敏感个人信息数据的保护和对一般个人信息数据的利用目的，实现二者之间的利益平衡，也避免“同意”的形式化，不让法律上对敏感性数据的保护缺位。

5. 1. 1. 4 建立举证规则，给予数据主体随时同意撤回权

鉴于数据来源者的信息获取能力，有专家学者主张，在涉及个人信息侵权的案件中，应当确立除“谁主张，谁举证”之外的特殊规则，即举证责任倒置规则，也就是说由被控数据侵权方承担其已取得同意的举证责任，从而降低信息主体的维权门槛，实现在诉讼中对于信息主体的二次保护。^①

此外，还应给予数据来源者同意撤回权，即数据来源者有权随时撤回已作出的同意，数据处理者不得利用服务协议及技术等手段，对数据来源者撤回同意进行不合理限制。我国现行法律中没有规定同意的撤回权，部分数据条例出于对数据市场的发展需要有所提及，未来可引入同意撤回规则，使得知情同意原则的结构更加完整，给予数据来源者更进一步的保护。

第二节 保护数据处理者合法权益 确立准入机制

“数据二十条”指出，合理保护数据处理者对依法依规持有的数据进行自主管控的权益。在保护公共利益、数据安全、数据来源者合法权益的前提下，承认和保护依照法律规

^① 《论大数据背景下公民个人信息保护中的知情同意原则》，法律论文，<https://www.svvv.cn/chachong/73416.html>

定或合同约定获取的数据加工使用权，尊重数据采集、加工等数据处理者的劳动和其他要素贡献，充分保障数据处理者使用数据和获得收益的权利。

数据要素权益需明确规定数据处理者可以做什么，然后通过权利交易达到社会数据总产品利用的最大化。

一方面要保护好数据处理者的合法权益，要依法保障数据处理者使用数据和获得收益的权利，依法确认数据采集、加工等数据处理者的劳动付出和收益权，承认和保护依照法律规定或合同约定获取的数据相关权利；另一方面，应确立数据处理者的合法准入机制，制定数据处理者准入的标准，确保数据处理者依法依规采集、持有、托管和使用数据，保障数据安全和各方权益。

5.2.1 数据处理者的身份界定与权益依法保护

根据国家网信办 2021 年 11 月发布的《网络安全数据管理条例》（征求意见稿），数据处理者是指在数据处理活动中自主决定处理目的和方式的个人和组织，其中包括互联网平台经营者、大型互联网平台经营者。欧盟《通用数据保护条例》第四条第八款规定：“‘数据处理者’是指代表控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织”。通常这是指数据处理者按照合同约定，根据数据控制者的指示进行数据处理。

5.2.1.1 依法保障数据处理者的合法权益

承认和保护数据处理者合理收益，是激活数据要素市场关键所在，数据处理者是市场上数据要素的真正创造者，如果忽视数据处理者合法权益，可能导致数据市场萎靡、数据黑市猖獗。承认和保护数据处理者合法权益，是数据产权保护和数据有效利用有机统一这一原则的延伸，也是尊重数据作为特殊生产要素的必然选择。

近年来，国家逐渐加大对数据处理者的权益保护，促进数据流动和交易。

2022年4月，国家知识产权局在2021年中国知识产权发展状况新闻发布会上介绍称，国家知识产权局已成立工作专班，形成了充分尊重数据处理者创造性劳动和资本投入、承认和保护数据处理者的合理收益等原则性思路。有关部门也将充分尊重数据处理者创造性劳动和资本投入，承认和保护数据处理者合理收益，保障市场机制有利于数据流动和交易、促进繁荣数据市场、壮大数字产业、促进产业数字化转型、支撑经济高质量发展。

数据产业的发展离不开数据的收集和处理，每个个体都是数据的创造者，同时也是数据的拥有者，但分散在个体处的数据并不具有价值，不能作为生产要素投入到生产中去。这意味着数据向数据要素的转变要经历一个处理的过程，平台企业往往是这个过程的生产者。通过一些程序将原始数据

转变为生产要素数据，在这个过程中，数据有了隐形的价值升值过程，健全后的市场机制还需尊重这一过程，承认数据处理者的劳动价值。

“数据二十条”指出，在保障安全前提下，推动数据处理者依法依规对原始数据进行开发利用，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。

国家发展和改革委员会发文《加快构建中国特色数据基础制度体系、促进全体人民共享数字经济发展红利》指出，健全数据要素由市场评价贡献、按贡献决定报酬的机制，以促进数据开发利用为出发点，肯定数据处理者的劳动价值创造，着重保护数据要素各参与方的投入产出收益，牢固树立“劳动创造价值”的数据观。

不少专家也对保护数据处理者合法权益持肯定态度，指出在数据时代不仅需要对数据来源者提供保护，还要对数据处理者和数据使用者的利益加以保护。企业在生产经营活动中采集加工的数据，只要不涉及个人信息和公共利益的内容，应当由企业享有数据持有、支配和收益的权利，确保企业投入的劳动等要素资源获得合理回报。

法律不妨承认在信息使用者具有合法利益时，对个人信息进行处理具有正当性，从而使信息使用者的合法利益成为个人信息处理的合法性基础之一。但这并不意味着，信息使

用者具有任何合法利益都可以直接进行个人信息处理，信息使用者仍然需要尊重信息主体的权益，这种尊重主要表现为履行相应的告知义务，让其知情。^①

5.2.1.2 依法保障数据处理者合法权益的合理路径

“数据二十条”提出合理保护数据处理者的权益。对数据处理者应当依法保障其使用数据和获得收益的权利，依法确认数据采集、加工等数据处理者的劳动付出和收益权，承认和保护依照法律规定或合同约定获取的数据相关权利。

数据处理者具有处理、转移数据等的权利，同时具有收益权，但也应遵守相应规则。首先，数据处理者的数据来源必须是合法的，其采集、加工、产生、利用的全过程必须合法，数据处理者，如平台的数据具有公共属性，并非“私人领地”，在使用和处理的过程中要在法律法规规定的范围之内运作。在保障数据处理者的权益前，必须保障数据来源者的权益，保护个人信息，建立负面清单，排除涉及个人敏感信息的数据。

其次，数据处理者在合法获得数据后，对数据进行加工，为此付出了劳动，在这种情况下，数据处理者就享有收益权。

对于数据处理者的收益权，可以通过两种方式进行确权。一方面是通过法律规定的形式，法律明确规定哪些收益权，目前尚没有法律法规明确规定的事项。另一方面，也是当前

^① 高富平：《个人信息使用的合法性基础——数据上利益分析视角》，《比较法研究》2019年第2期，www.lmdna.com/news/124.html

主要的方式，经济上的约定，如以合同的形式约定，在合规合法的情况下，数据处理者可以获得收益权。

5.2.2 制定数据处理者准入的标准

保障数据处理者的合法权益，也意味着数据处理者需要依法依规履行义务，保障数据安全、维护各方的合法权益。

当前，数据处理者在数据处理的过程中，存在一些安全问题，出现违规处理数据的现象。如“滴滴”事件、知网被罚等对于其他的“数据处理者”也是一个警示和威慑，体现了国家对于危害国家网络安全、数据安全以及侵害公民个人信息的违法行为越来越重视。

国家网信办于2021年11月公布的《网络数据安全管理条例（征求意见稿）》，对数据处理者提出包括向第三方提供要满足合规流程、隐私政策内容等“合规”要求。如《网络数据安全管理条例（征求意见稿）》第十二条规定，数据处理向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规定：（一）向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；（二）与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；（三）留存个人

同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

2021年9月，公安部也对数据处理者提出相关安全要求，督促、指导数据处理者采取相应的技术措施和必要的其他措施，保障数据安全；督促数据处理者依法履行安全保护责任和义务，整改网络安全、数据安全风险、隐患、漏洞和突出问题，提高安全保护能力。

首先，数据处理者在处理数据时必须是合法合规的，其采集、加工、产生、利用的全过程须合法。部分数据处理者，如平台具有公共属性，在进行数据处理时必须在法律法规规定的范围内运作。

其次，建立数据处理者的标准规范，建立“负面清单”，一方面设立数据处理者在利用数据的边界，促进整体数据的利用；另一方面确立对数据处理者“违规操作”的界定。

再次，培育“数据经纪人”等具有权威性、公正性的第三方机构。明确权责明晰的第三方机构标准，有助于其他数据处理者明确数据处理活动的方向，如建立有央国企背景的第三方机构等。

第三节 依法保护数据及数据衍生产品的经营权

传统权利制度框架难以破解数据产权困境，“数据二十条”创新数据产权观念，淡化所有权、强调使用权，聚焦数

据使用权流通。^①“数据二十条”提出的“三权分置”数据产权运行机制。通过分类分级分置、场景化确权授权，助力破解数据产权不明确难题，有效保障数据及数据衍生产品的经营权利，进一步释放数据要素价值。

5.3.1 依法规范数据使用者许可他人的权利

数据产品经营权主要指数据竞争性权益，即数据处理者对第三方的限制性权益，以防止同行业竞争者不当利用其数据产品获得利益。由于数据产品能带来可观的商业利益和市场竞争优势，依据洛克劳动财产理论和市场激励理论，数据处理者应当对数据产品享有独立的财产权益。但是，数据处理者将原始数据进行加工、处理后，产生数据产品并提供给他人使用，数据使用者利用该数据产品形成新的数据衍生品，产生新的市场价值。数据处理者对新形成的数据衍生品不具有使用权、经营权等权益，数据使用者对其所形成的数据衍生品享有合法的使用、经营等权益。

数据产品经营权主要是为了保护数据处理者和数据使用者利用数据创造新价值的合法权益，保障在数据加工、数据分析、数据重新排列组合等数据价值挖掘环节的劳动、资源投入能有所回报。

数据处理者将数据产品的使用权转让或授权给数据使用者，数据使用者对该数据进行新的组合和汇总，让其产生

^① 李婕：《“数据二十条”对外发布，构建数据基础制度体系——做强做优做大数字经济》，人民日报海外版，www.gov.cn/xinwen/2022-12/21/content_5732906.htm

新的呈现形态和经济价值，促进数据流通利用，挖掘数据新价值，实现数据社会价值最大化。因此，数据使用应对其形成的数据衍生品享有数据产品经营权。同时，要依法保障数据使用者利用数据和获得收益的权利，承认和保护依照法律规定或合同约定获取的数据相关权利。

5.3.2 保障数据衍生产品的合法权益

“数据二十条”提出要推动数据处理者依法依规对原始数据进行开发利用，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。对应数据产品经营权，要保护经加工、分析等形成数据或数据衍生品的经营权，依法依规规范数据处理者许可他人使用数据或数据衍生品的权利，促进数据要素流通复用。

数据是对原始数据进行去个人标识化、经加密、加工挖掘，具有交换价值和技术可行性的数据。个人信息是企业数据的基础和本源，是企业用户数据项下的原始数据，同样也是衍生数据的来源。有专家学者表示，数据处理者通过提供服务、签订合同等合法方式收集数据，并通过筛选、特定组合、深度开发、系统整理等大量智力和体力劳动赋予了数据更高的价值，生成的数据衍生产品能够应用于市场，并提供经济效益。

在不少数据衍生产品中，由于对原始数据进行不同程度的加工，原始数据中的个人信息无法被识别，做到数据“可

用不可见”，规避数据安全隐私风险。原始数据归属于数据来源者，数据处理者对数据衍生产品享有数据产品经营权，合理平衡数据处理者与数据来源者的利益关系，鼓励数据处理者不断进行技术创新，进一步挖掘数据要素市场价值。

目前，数据衍生产品交易面临诸多困难，如难以精确匹配购买方的需求、不能充分发挥购买方自有数据资源作用、难以实现按需购买、数据得不到及时更新等。^①数据衍生资产评估涉及极为复杂的数据定价等专业问题，由于数据交易的复杂性，无法简单照搬传统实物资产或知识产权资产评估办法。

为加快数据衍生资产流通，更好保障数据衍生产品交易各方权益，国家有关部门包括地方有关部门，应积极筹建数据评估专业机构，组织会计师、审计师、资产评估师、数据分析师、律师等专业人士，为数据衍生资产评估提供权威咨询服务，形成具有一定法律效力的评估文件，确保数据资产的规范高效流通。

第四节 做好数据全生命周期的服务

由于数据自身具有无形性、负外部性、难以追溯等特点，数据在采集、传输、存储、使用、删除、销毁等全生命周期中都存在需要关注的潜在问题风险。传统治理模式和手段难以跟上数据流通应用的实际需要，条块分割的行业和属地治

^① 唐文发：《论数据的国家权属及数据衍生权》，旗帜网，www.qizhiwang.org.cn/n1/2022/1229/c422377-32596147.html

理模式难以适应数据要素跨地区、跨行业、跨层级流通交易的治理需求，线下治理难以满足数据要素市场线上线下一体化发展趋势。

我国海量数据中，不仅包括公共、企业、个人等方面的数据，也有很多三者交叉在一起的数据，具有三者共有的特点。东南大学法学院副研究员徐珉川指出，“个人数据、企业数据、公共数据在范围上既存在交叠又有所差异，个人数据上的权利与个人隐私、个人信息权益既有联系又存在区别，公共数据中政务机关控制的数据与公共性社会服务运营机构控制的数据之间的联系和区别等问题，都存在一定的争议。”^①

为此，整体的数据全生命周期服务有助于解决当前具有交叉性质的数据要素产权难题。

其一，可采取数据经纪人模式。数据经纪人模式助力消弭与破解数据要素流通过程中的障碍，数据经纪人可以做数据流通的中间人，挖掘数据要素价值。

其二，可采取共有产权模式。数据要素产权及收益的配置应该使数据形成过程中的所有贡献者共享数据红利，明确数据“多元主体”共有，兼顾多方主体的分配利益、基于“分级分类”，构建数据要素“多元共治”体系。

建立由政府授权监管的确权平台，开展数据资产登记确

^① 徐珉川：《徐珉川：论公共数据开放的可信治理》，《比较法研究》2021年第6期，fzzfyjy.cupl.edu.cn/info/1035/13844.htm

权法治化，是做好数据全生命周期服务的有效实践探索。探索形成可参照、可操作的确权平台工作协调机制，结合数据确权中的实际问题，开展资产登记确权等工作。同时，理清数据要素各参与方的合法权益，明确国家对不同类型数据的要求，逐步形成归属清晰、权责明确的数据产权登记确权制度，做好全生命周期的各项服务。

场景案例 7

（一）场景背景

受数据要素基础制度不完善的制约，数据产权难以进行有效界定，数据产品的定量、定价、定质等环节均未取得突破，数据资产的确权机制尚未建立，数据要素的充分流转流通存在巨大瓶颈，各个部门机构为确保数据安全所建立的坚不可破的数据壁垒让数据的跨部门、跨域融合计算缺乏畅通的渠道与机制。停滞的大数据极大地阻碍了数据作为生产要素的价值实现，更无法达成以数据激发实体经济活力，推动产业结构转型升级的目的。

建立以数据确权为核心的数据要素流通流转机制，在各地建设建立新一代的大数据基础设施势在必行：受数据要素基础制度不完善的制约，数据产权难以进行有效界定，数据产品的定量、定价、定质等环节均未取得突破，数据资产的确权机制尚未建立，数据要素的充分流转流通存在巨大瓶颈，各个部门机构为确保数据安全所建立的坚不可破的数据壁

垒让数据的跨部门、跨域融合计算缺乏畅通的渠道与机制。停滞的大数据极大的阻碍了数据作为生产要素的价值实现，更无法达成以数据激发实体经济活力，推动产业结构转型升级的目的，因此，构建以数据确权为核心的数据要素流通流转机制，在各地建设新一代的大数据基础设施势在必行。

（二）场景建设

人民数据推出面向新型数据城市建设的新一代大数据基础设施：“人民数据确权流通平台”。依托完善的数据治理技术框架和先进的区块链确权理念，打破部门间、区域间以及各个市场主体间的数据壁垒，构建以隐私计算为核心的可信计算平台，遵循数据“可用不可见”的基本原则，对数据要素进行归集、治理并形成数据资产，在“人民链”的底层技术加持下，跨平台实现数据的合法、合规、高效流转，让数据成为真正的生产要素，激发市场主体的活力，赋能数字经济实现跨越式发展。

2019年，人民数据即精准把握行业发展脉搏，建设了全国首个数据确权平台“人民数据资产服务平台”，率先进入数据资产确权深水区进行探索和实践，建设行业首个集数据合规性审核、数据确权出版、数据流通登记、数据资产服务为一体的国家级综合性数据资产服务平台，通过打破数据行业壁垒，建立数据合法合规流通机制，整合优质数据资源应用，推动数据要素市场规模化、规范化的发展。

2021 年，经过两年的持续研发升级，人民数据“基于数据确权的数据要素流通交易系统”入选“工信部 2021 年大数据产业发展试点示范项目”，将区块链基础设施“人民链”引入数据要素确权系统，充分发挥区块链技术特点和优势，通过对数据要素的资质审核、资产登记、融合计算、交易流通等环节进行链上存证，确保数据流转全过程可管控、可记录、可追溯，形成完整的业务闭环，进一步升级确权生态。

2022 年，人民数据的新一代综合云管平台“人民云”上线，“人民数据确权流通平台”再次升级，依托“人民链”与“人民云”的底层技术支撑，平台拥有了多节点部署、跨平台服务的能力，可以根据不同区域、不同场景的业务需求，灵活部署 SaaS 或私有化业务系统，打通与现有城市大脑、大数据交易所、数据中台之间的数据链接，实现数据要素的互联互通，在确保数据应用安全的基础上，充分发挥数据作为生产要素的本质，赋能实体经济的发展，真正成为新型数据城市建设的大数据基础设施。

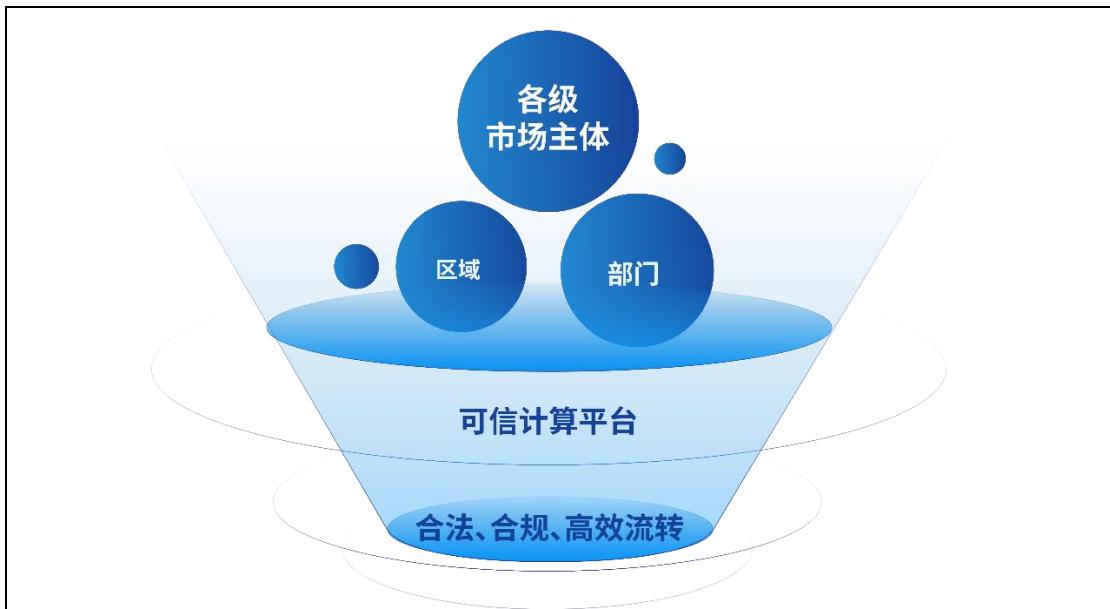


图 14 人民数据确权流通平台示意图

(三) 场景成效

人民数据确权流通平台，作为新型数据城市建设的加速器，可以通过建设数据治理中台，助力落地城市建立城市数据资产目录；可以通过“人民链”的链上登记存证系统，确保数据流转全流程确权链完整可追溯；可以通过搭建可信计算平台，为城市构建安全高效数据融合计算系统；可以通过建设数据资产流转交易中心，推动数据要素以产品化的形式向产业主体高效流转；可以通过搭建城市数据应用生态，为城市核心支柱产业提供数字化解决方案。

人民数据确权流通平台，作为数字经济高速路上的新引擎，具有轻部署、易运营、助产业、保安全的特点。通过整合全域全量数据资源，部署全国节点，实现数据资源互联互通，与丰富的自有数据结合，畅通数据流转渠道，以海量数据资源提升城市数据价值实现；解决现行法律法规要求下的

数据合法合规流转机制课题，以完整授权+链上确权的方式确保每一条数据的全生命周期流转都合规；基于将数据充分应用于产业发展的场景设计原则，结合行业发展特点打造专属解决方案，依托强大算力构建数据原生应用。

截至 2023 年 1 月，人民数据确权流通平台已在全国建立骨干节点五个，业务节点二十多个，实现与十余个国家部委、省级大数据中台或数据要素流通交易平台的打通，累积实现登记存证的数据要素达 200 多亿条，实现精准确权的数据资产一万余宗，成为数据要素行业头部阵营的领航者。

人民数据介绍：

人民数据系人民日报、人民网旗下的数据理论和实践探索平台，主动承担起党媒在数据领域的责任使命，着力推动构建国家数据治理新格局，发挥旗帜引领、枢纽融通、先锋先试的作用，致力于做好党政机关、央国企、民企等大数据的“存、管、用”工作，精准服务于“科学执政、数据执政、智慧执政”的新发展理念，使大数据更加便捷、高效地服务于经济社会发展，为各行各业广泛应用。

作为大数据国家队，人民数据以大数据为核心业务，2019年上线了我国首个数据确权平台，深入挖掘数据资源，开发数据要素资产，以打造人民云、人民链、数据银行、人民党建云等项目为契机，积极推动数字经济与实体经济深度融合，探索出“智数惠民、用数利民、聚数兴民、以数便民”的新路径，形成了数据合法、应用合规、数据可信、数据安全的大数据服务生态。

浙江大学网络空间安全学院介绍：

浙江大学于 2017 年成立网络空间安全研究中心，2019 年成立网络空间安全学院，负责校网络空间安全一级学科建设，由时任校长吴朝晖院士亲自担任建设领导小组组长，由国际知名学者任奎担任院长，是国家首批网安一级学科博士学位授权点之一。

学院坚持以国家网络空间安全重大战略需求为导向，确立了数据安全与隐私、软硬件系统安全、人工智能安全、网络与通信安全四个研究方向。已建立区块链与数据安全全国重点实验室、中央网信办/教育部网络空间国际治理研究基地、浙江省区块链与网络空间治理重点实验室、移动终端安全技术浙江省工程研究中心等多个创新平台，以及浙江大学—华为系统和数据安全联合实验室、浙江大学杭州国际科创中心—浙报数字文化集团—浙江大学网络空间安全学院数字安全联合实验室、浙江大学—阿里巴巴网络空间安全联合实验室、浙江大学—蚂蚁集团—数据安全与隐私保护实验室等多个产学研协同的研究中心和创新基地。

2023 年 3 月 24 日，人民网舆情监测室（北京人民在线网络有限公司）、人民数据管理（北京）有限公司、浙江大学网络空间安全学院共同成立数据安全联合实验室，并在人民日报社新媒体大厦正式揭牌。