DOI: 10.61189/627405ptxbio

·专家述评·

液态生命与数字围栏：元宇宙健康数据的治理困境与范式重构

高承实[1*]，程元骏[2]

1. 安徽栈谷科技有限公司，池州 247100

2. 池州市人民医院胸心外科，池州 247000

［摘要］ 元宇宙与数字医疗的深度融合正在改变健康数据的基本形态。传统电子健康记录作为离散化、事件驱动的“固态记录”，正演变为持续生成、跨平台流动、由算法不断重构的“数字生命流”。这一本体论变革对既有数据治理框架构成根本性挑战：一方面，数据的高度流动性使得传统基于明确边界的隐私保护机制失效；另一方面，大型平台通过技术标准、协议与硬件垄断对流动数据进行“再疆域化”，形成了从软件层到硬件层的新型权力结构。本文以“液态化”与“再疆域化”为核心分析框架，系统考察元宇宙健康数据治理的结构性困境。研究提出3个核心问题：(1)数字生命流如何改变数据治理的基本前提？(2)液态化与再疆域化的辩证关系如何塑造数据权力结构？(3)面对这一双重运动，新的治理范式应如何构建？ 通过从权力分配、经济公平、价值抉择、责任归属、数字主权5个维度批判性分析技术解决方案（联邦学习、零知识证明、可信执行环境）、法律监管模式（GDPR、HIPAA）与市场自我调节机制的局限性，本文揭示单一治理模式难以应对高度动态的数据生态。在此基础上，本文提出一种关系型数据治理范式，并构建由微观技术架构（默认隐私保护、互操作标准、可解释算法）、中观制度创新（数据信托、数字公地、参与式审计）与宏观法律重塑（数字人格权、数字守门人监管、全球最低标准）构成的多层次治理框架。该框架以“数据关系权”取代“数据所有权”，以“集体数字福祉”补充“个人隐私保护”，在核心理念层面完成双重升维，并在制度设计中嵌入数据信托的“四要素”机制（受托人构成、决策机制、收益分配、监督机制）和数字公地的Ostrom八项原则等具体操作化安排。研究引入Apple Health生态、VR心理治疗平台、欧盟健康数据空间等案例作为经验参照，为元宇宙健康数据治理提供理论整合与政策参考。

［关键词］ 元宇宙；健康数据治理；数字生命流；液态化；再疆域化；数据信托；数字人格权

［中图分类号］ R-03 ［文献标志码］ A

Liquid life and digital fence: governance dilemma and paradigm reconstruction of metaverse health data

Gao Chengshi[1*], Cheng Yuanjun[2]

1. Anhui Zhangu Technology Co., Ltd., Chizhou 247100, Anhui, China

2. Department of Thoracic and Cardiac Surgery, Chizhou People's Hospital, Chizhou 247000, Anhui, China

［**Abstract**］ The deep integration of the metaverse and digital healthcare is fundamentally reshaping the nature of health data. Traditional electronic health records (EHRs), characterized as discrete, event-driven "solid records," are evolving into "digital life streams"—continuously generated, cross-platform flowing, and algorithmically reconfigured data processes. This ontological shift poses profound challenges to existing data governance frameworks. On one hand, the heightened fluidity of data renders traditional privacy mechanisms, which rely on clear data boundaries, increasingly ineffective. On the other hand, dominant platforms are "reterritorializing" this fluid data through technical standards, protocols, and hardware monopolies, thereby constructing novel power structures that extend from the software layer to the hardware layer. Employing "liquefaction" and "reterritorialization" as core analytical lenses, this paper systematically investigates the structural dilemmas of health data governance in the metaverse. It poses three central research questions: (1) How does the emergence of "digital life streams" alter the foundational premises of data governance; (2) How does the dialectic between liquefaction and reterritorialization shape the power dynamics of health data; (3) In the face of this dual movement, what form should a new governance paradigm take through a critical analysis of technological solutions (federated learning, zero-knowledge proofs, trusted execution environments), legal-regulatory models (GDPR, HIPAA), and market-based mechanisms—examined across five dimensions: power distribution, economic equity, value choices, accountability, and digital sovereignty—this paper reveals the inherent limitations of single-pronged governance approaches in addressing a highly dynamic data

［收稿日期］ 2026-01-30 ［接受日期］ 2026-02-29

［作者简介］ 高承实，博士，副教授、董事长.

*通信作者（Corresponding author）. Tel: 056-62028361, E-mail: 13838001036@163.com

ecosystem. Building on this critique, the paper proposes a relational data governance paradigm and constructs a multi-level framework integrating micro-level technological architecture (privacy by default, interoperability standards, explainable algorithms), meso-level institutional innovations (data trusts, digital commons, participatory auditing), and macro-level legal reforms (digital personality rights, digital gatekeeper regulation, global minimum standards). This framework moves from "data ownership" to "data relational rights" and supplements "individual privacy protection" with "collective digital well-being," achieving a dual conceptual elevation. It further embeds operational mechanisms such as the "four elements" of data trusts (trustee composition, decision-making, benefit distribution, supervision) and Ostrom's eight principles for governing digital commons. Drawing on case studies including the Apple Health ecosystem, VR psychotherapy platforms, and the European Health Data Space (EHDS), the paper offers both theoretical integration and policy references for the governance of health data in the metaverse.

［**Key Words**］ metaverse; health data governance; digital life stream; liquefaction; reterritorialization; data trusts; digital personality rights

随着元宇宙与医疗健康的深度融合，一个根本性的问题正浮出水面：当患者的生命体征、行为轨迹乃至情绪反应被实时、持续地捕获并汇入虚拟空间，传统意义上边界清晰、用途明确的“医疗记录”，正在演变为一种性质全新的数据实体。这一演变所引发的，远不止于技术应用层面的创新，更是一场关于生命数据控制权的深层治理危机。

1　数字生命流

1.1　*问题提出*　医疗健康数据的形态，正经历着从静态档案到动态流变的根本性跃迁。传统电子健康记录（EHR）或病历，本质上是结构化、离散化的历史快照，其生成与记录依赖于明确的临床交互节点（如就诊、检验）。然而，元宇宙与医疗的深度融合，正在催生一种连续、多模态、高维的情景化数据实体。

在元宇宙医疗场景中，数据采集将突破传统医疗机构的物理与时间边界。通过VR/AR设备、可穿戴传感器及环境感知技术，患者的生理指标、行为数据、情绪反应、乃至与虚拟环境的交互日志，都将被实时、持续地捕获与融合。这些数据不仅体量巨大，更关键的是其高度情景化，数据的医疗意义与生成时的虚拟场景深度绑定，使得脱离情境的数据解读将丧失其临床价值。数据的价值，日益依赖于其在流动与聚合中涌现的新知识。

这种从“离散记录”到“连续生命流”的本质变革，对建立在工业时代与早期信息化基础上的传统健康数据治理范式构成了严峻挑战。旧有范式依赖于清晰的边界、明确的权属关系、基于特定目的的有限收集，以及以“知情同意”为核心的事前授权模型。然而，元宇宙中持续生成的数据流，使得这些前提假设纷纷失效。数据如同“液态”般无孔不入地流动、聚合与重组，其最终用途可能远超收集时的预设，传统的隐私边界在此过程中被迅速侵蚀。

与此同时，掌控数据聚合平台的科技巨头，正试图对这些流动的数据实施“再疆域化”。它们通过技术标准、服务协议和算力优势建立新的数字支配领地，不仅从软件层抽取“数字地租”，更将控制触角延伸至硬件层，通过垄断可信执行环境等核心芯片技术，形成更深层的依附关系。平台资本对健康数据的控制正在向多维度的权力集中演变，风险在健康这一最敏感的领域日益隐现。

因此，核心问题在于，面对性质已经发生根本性变革的元宇宙健康数据，基于旧有数据形态构建的治理框架是否已然滞后乃至失效？我们亟需何种跨学科的新范式，来应对这场由数据“液态化”流动与“再疆域化”垄断所共同引发的治理范式危机？要回答这一问题，首先必须深入理解这种新型数据实体，即“数字生命流”的本体论特征。

1.2　*理解“数字生命流”*　传统电子健康记录本质上是“临床事件的快照”，它记录的是患者在特定时间点、特定医疗场景下产生的离散化、结构化信息。这种数据形态具有明确的边界、预设的采集目的，以及相对静态的存储方式。与之相对，元宇宙医疗场景中涌现的“数字生命流”，是一种性质截然不同的数据实体，其核心特征可归纳为以下4个维度。

一是连续性。数据生成从“点状采集”转变为“无中断流淌”。通过可穿戴设备及VR/AR交互，患者的生理指标、行为轨迹、情绪反应被实时、持续地捕获，形成持续更新的数据序列，而非孤立的数据点。

二是情境依赖性。数据的医疗意义高度内嵌于生成时的虚拟场景之中。一段关于疼痛的行为数据，必须与其所处的虚拟任务（如康复训练中的特定动作）、社交互动（如与虚拟医护的对话）、乃至环境参数（如虚拟空间的沉浸强度）关联解读，才能生成完整的临床意义。脱离情境的数据，其价值将

大幅衰减甚至失真。

三是生成性。数据在流动中不断增值与创生新意。单一维度的数据流与其他数据流聚合后，能够通过算法挖掘出超越原始采集意图的新洞察。这意味着数据的价值不是预存的，而是在动态重组中涌现的。

四是多模态融合性。数据来源突破了单一文本或数值的局限，呈现出生物信号、行为日志、感官反馈、语音情感、环境上下文等多种模态的深度融合。这种融合使得元宇宙中的“患者”形象从抽象的医疗记录编号，还原为一个完整的、具身化的数字人。

以Oxford VR开发的VR心理治疗平台为例，该平台通过虚拟场景暴露疗法治疗社交焦虑症。患者在虚拟环境中与虚拟角色互动时，系统实时记录其眼球运动、头部转向、语音反应、心率变异性等多模态数据。这些数据并非静态记录，而是随着治疗进程持续生成，并在不同治疗阶段被重新分析。例如，早期暴露阶段的行为数据可能与后期康复阶段的数据对比，用于评估疗效。这一案例生动体现了“数字生命流”的4个特征，并将成为后文分析技术治理困境（3.2节）和制度创新（5.2节）的重要经验参照。

与既有概念相比，“数字生命流”具有独特的理论内涵。如果说“量化自我”强调个体主动记录自身行为[1]，而“数据化身体”聚焦于身体的数据表征[2]，那么“数字生命流”则更侧重于技术系统对个体生命过程的持续捕捉与算法重构，强调数据本身的流动性、生成性与情境嵌入性。

简言之，如果说传统EHR是医疗体系为患者绘制的“静态地图”，那么数字生命流则是患者在数字世界中真实经历、持续生成的“动态航行日志”。这一本体论层面的跃迁，构成了现有治理范式失效的根本原因，也为我们理解后续的“液态化”与“再疆域化”双重运动提供了关键的认知前提。

然而，现有研究是否充分把握了这一新型数据形态所带来的治理挑战？下文将系统梳理相关文献，揭示其局限与缺口。

1.3 *文献综述与批评* 当前，学术界与政策界对元宇宙健康数据治理的关注日益增加，现有研究主要围绕三个层面展开，但均存在显著的视角局限或整合缺口。

技术解决方案与框架设计层面的研究，聚焦于应用隐私增强计算（如联邦学习、安全多方计算、可信执行环境）、区块链、去中心化架构等技术，旨在从工程层面解决数据安全、隐私保护与可信共享问题。部分研究已提出针对医疗元宇宙空间数据治理的初步框架，如Das等[3]强调患者控制与安全协议；部分研究探讨区块链、NFT用于健康信息交换的潜力。但这个层面的讨论常陷入技术决定论的乐观想象，默认技术方案能自动解决社会与伦理问题，而忽视了技术的复杂性。零知识证明的可信初始化由少数精英掌控，可信执行环境导致硬件层垄断，可能加剧而非缓解权力集中。

法律与伦理原则的探讨主要是识别并警示元宇宙医疗带来的新型伦理风险与法律挑战，如沉浸式环境中的知情同意、数字模拟体的道德地位、跨境医疗的法律管辖权等，强调在AI时代沿用与更新隐私保护原则（如目的限定、数据最小化、透明度）的重要性。如Kostick-Quenet和Rahimzadeh系统阐述了元宇宙健康数据治理的伦理风险[4]；何之行分析了GDPR原则在AI医疗与防疫中的应用与张力[5]。但这类讨论多为原则性倡导或风险描述，缺乏将这些原则转化为可操作治理机制的深入分析，尤其未能回应“合规成本高企反而巩固大平台垄断”的悖论。

数据政治经济学批判则借鉴相关理论，批判性地分析全球数据经济中的不平等结构。Zuboff提出的“监控资本主义”理论揭示了行为数据如何成为资本主义积累的新资源，强调企业通过持续收集行为数据建立新的市场控制机制[6]。Srnicek的“平台资本主义”理论指出，平台企业通过控制数据接口、算法系统与云计算资源，在数据生产与利用过程中占据核心位置[7]。Cohen进一步分析了法律制度如何被动员起来服务于信息资本主义的扩张，揭示了法律与技术平台的共构关系[8]。另有研究借鉴“数据殖民主义”框架[9]，指出全球南方国家的健康数据被跨国科技公司大量收割并输往全球北方，用于创造价值，而数据来源国与个体却未能公平受益，如Sekalala等[10]的研究。该视角提供了重要的批判性宏观视野，但较少与元宇宙医疗的具体技术情境（如空间计算、数字孪生、硬件层垄断）深度结合，也未能充分提出超越批判的、建设性的替代治理方案。

上述3条研究路径基本处于平行发展状态，存在显著的“分野”现象。技术研究者缺乏足够的社会理论与伦理考量；伦理与法律学者对技术实现逻辑的理解可能流于表面；而政治经济学批判则常与具体治理设计脱节。特别地，现有研究未能系统性地提出一个能够同时把握元宇宙健康数据“双重运

动”，即无界液态化流动与平台主导的再疆域化的分析框架，也未能在此基础上整合技术可能性、法律伦理原则与社会经济正义，构想出切实可行的下一代治理范式。本研究旨在弥补这一核心缺口。

1.4　研究思路与方法　为回应上述研究缺口，本文拟采用“科学、技术与社会”（STS）研究与政治经济学批判相交叉的分析框架。这一框架拒绝将技术视为中立工具，也反对将社会因素视为单纯的外部背景，而是将元宇宙健康数据治理视为一个技术系统、社会制度、经济权力与法律规范共同建构、相互博弈的动态场域。

本研究将以“液态化”与“再疆域化”作为核心分析透镜。“液态化”概念汲取自齐格蒙特·鲍曼的现代性理论[11]，用以描述数据脱离固定容器、持续流动、不可预测且易于重组的状态，它解构了传统的空间、隐私与控制边界。“再疆域化”则源于德勒兹与瓜塔里的政治地理学概念[12]，后被批判数据研究借用[9]，用以分析权力实体（如平台企业、国家）如何通过基础设施、算法、协议与法律手段，试图对流动的数据施加控制、划定归属并从中提取价值，从而形成新的数字领土。这两者并非先后关系，而是同一进程的一体两面。数据的液态化是资本与权力进行更高阶积累（再疆域化）的前提，而再疆域化的努力又不断塑造着数据流动的方向与规则。

在方法上，本文将进行批判性的理论整合与框架构建。首先，系统梳理并对话来自计算机科学、法学、伦理学、社会学与政治经济学的相关文献；其次，运用“双重运动”透镜，对现有的技术方案（如联邦学习、区块链、零知识证明、可信执行环境）与治理模式（如GDPR式监管、市场自我调节）进行深入的内在批判，从软件层的密码学协议到硬件层的芯片垄断，揭示其在应对元宇宙健康数据特质时的内在矛盾与局限；最后，在批判的基础上，尝试构建一个多层级的治理新范式。为增强论证的经验厚度，本文将在技术批判和治理建构部分穿插引入Apple Health生态、VR心理治疗平台、欧盟健康数据空间等案例。

基于上述分析，本文提出以下三个核心研究问题。（1）本体论问题：在元宇宙医疗环境中，健康数据如何从传统的结构化记录转变为持续生成的“数字生命流”？这一转变对数据的基本属性（边界、用途、控制方式）带来了哪些根本性改变？（2）政治经济学问题：数据的“液态化”与平台的“再疆域化”如何构成一对辩证运动？二者的张力如何塑造元宇宙健康数据的权力结构与治理困境？（3）规范性问题：面对这一双重运动，现有的技术治理、法律监管与市场调节模式为何失效？一种能够在技术架构、制度设计、法律保障3个层面协同回应液态化与再疆域化张力的治理新范式应如何构建？

2　液态化与再疆域化的双重奏

元宇宙中健康数据的治理困境，其根源在于数据本身的性质与运动逻辑发生了根本性变革。传统基于静态、离散数据的治理范式，在面对一种持续生成、无界流动且被强力聚合的新型“数字生命流”时已然失效。本章旨在构建一个整合性的理论分析框架，以揭示这一困境的本质。引入“液态化”与“再疆域化”这一对辩证概念作为核心透镜，前者描绘了数据挣脱物理与制度束缚后呈现的流体状态，后者则揭示了资本与权力对这种流动性进行捕获、固化和剥削的新型统治形式。二者共同构成了元宇宙健康数据政治经济学的双重奏。

2.1　理论谱系：从数据化社会到平台权力批判　在展开“液态化”与“再疆域化”这一对核心分析透镜之前，有必要将本文的理论框架置于更广泛的学术脉络之中。近年来，社会科学领域围绕数字技术与数据治理的讨论，逐渐形成了3条相互关联的研究传统：数据化社会研究、平台治理研究以及数据政治经济学批判[13-15]。本文的理论框架正是在这3条路径的交汇处发展而来。

（1）数据化社会研究为理解健康数据的持续生成提供了基础。“数据化”（datafication）概念强调，越来越多的人类活动正在被系统性地转化为可计算的数据形式。Van Dijck等学者指出，在数字平台环境中，社会行为被持续记录并转化为可分析的数据资源，从而形成新的社会组织方式[16]。在健康领域，这一趋势表现为“量化自我”运动、可穿戴设备的普及以及远程医疗系统的发展[1]。个体的身体状态、行为模式与生活环境逐渐被持续记录并整合为数字健康数据。这一过程不仅改变了医学研究与医疗服务的方式，也使健康数据从传统的临床记录转变为一种持续生成的数据资源。

（2）平台治理研究揭示了数字基础设施在组织数据流动中的关键作用。Srnicek提出的“平台资本主义”理论指出，平台企业通过控制数据接口、算法系统与云计算资源，在数据生产与利用过程中占据核心位置[7]。平台不仅提供技术服务，也通过规则制定和数据控制塑造数字经济的运行方式。在健康数据领域，这种平台化趋势同样日益明显。从数字健康应用到虚拟医疗系统，越来越多的医疗服务

依赖平台基础设施运行，这使得平台企业在健康数据流动中拥有重要影响力。

（3）数据政治经济学批判进一步揭示了数据流动背后的权力结构。Zuboff提出的“监控资本主义”理论揭示了行为数据如何成为资本主义积累的新资源，强调企业通过持续收集行为数据建立新的市场控制机制[6]。而“数据殖民主义”理论则指出，当代数字经济正在形成一种新的资源提取模式，即通过技术系统大规模收集并分析用户数据，从而创造经济价值，而数据来源的个体与社群则难以参与价值分配[9]。

这3条研究传统共同表明，数字数据不仅是技术资源，也是重要的社会资源，其生产、流动与利用都深刻嵌入到社会结构之中。然而，现有研究在解释数据流动性与数据控制的关系时仍存在一定局限，数据化研究强调数据生成的持续性，平台治理研究关注平台基础设施的控制能力，而数据政治经济学则聚焦权力与价值分配问题，三者的理论整合仍然有限。

正是在这一背景下，本文提出“数据液态化—再疆域化”分析框架。其中，“液态化”概念汲取自鲍曼的“液态现代性”理论[11]，用以描述数据在数字环境中呈现出的高度流动性与可重组性；“再疆域化”则借用德勒兹与瓜塔里的概念[12]，用以分析平台系统如何通过技术基础设施重新建立数据控制边界。通过整合这两个概念，本文试图在数据技术形态与数据权力结构之间建立更加系统的理论联系，为理解元宇宙健康数据治理问题提供新的分析工具。

2.2 从鲍曼“液态现代性”的视角看数据的液态化

波兰社会学家齐格蒙特·鲍曼提出的“液态现代性”理论，为理解元宇宙健康数据的根本特性提供了深邃的哲学社会学基础。鲍曼指出，现代性正经历从“固态”向“液态”的过渡[11]。固态现代性的特征是坚固、持久的结构与关系（如稳定的职业、地域社群、终身制度），而液态现代性则意味着一切社会形态、关系、制度都在以空前的速度流动、蒸发与重塑。流动性、短暂性和不确定性成为新的生存法则。数字技术的崛起，正是推动并加速这一液态化进程的核心引擎。

在元宇宙医学的语境下，健康数据的“液态化”表现为三个相互关联的维度。

首先，数据的无界复制与聚合重组。传统医疗数据（如病历、化验单）如同被锁在档案柜中的“固体”文件，其复制、流动受严格管控。而元宇宙中的健康数据，包括实时生理信号、行为轨迹、情感交互、虚拟环境反馈，自生成起便是持续的数据流。它们可以近乎零成本地被无限复制，并在不同平台、算法与数据库间瞬间聚合、交叉比对，生成远超单一数据源的“数字孪生”或用户画像。这种流动性是数据价值倍增的源泉，但也意味着其一旦脱离采集瞬间的原始情境，便如同汇入海洋的水滴，流向与用途均难以追踪与控制。

其次，数据目的漂移与语境抽离。液态数据的价值在于其可塑性。一段为康复训练而采集的关节运动数据，可能被用于评估患者的保险风险；一组为心理健康监测而记录的情绪波动数据，可能被用于个性化广告推荐。鲍曼所警示的液态现代性下关系的短暂与工具的即弃性，在数据领域演变为使用目的的随意转换与承诺的脆弱性。数据的原始医疗语境被抽离，沦为一种可供任意解读和利用的原始素材，这使得传统的“基于特定目的”的知情同意原则在数据流的持续重组面前彻底崩塌。这一现象与Nissenbaum所论述的“语境完整性”被破坏[17]形成呼应，当数据脱离其原始生成语境时，原本的规范与预期便被瓦解。

最终，对个体权利基石的侵蚀。液态化最深刻的冲击在于瓦解了个人自主与知情同意，这是现代数据治理的伦理与法律基石。当数据如液体般持续渗出、四处流淌时，那种在特定时间点、针对特定数据集、给予明确授权的“固态”同意模型变得毫无意义。个体陷入一种“同意的悖论”，要么拒绝一切数据化从而被排除在元宇宙医疗服务之外，要么在完全无法预见未来用途的情况下，交出自身生命信息的永久流动权。这导致个体从数据权利的主体，异化为数据流的源头，也就是被监控和提取价值的对象[6]。正如研究所指，数字时代的监控通过数据收集与核对，在习惯于中介化生活的人群中构建了一种新的、稳固的权力形式。个体的生物特征与行为，在液态流动中悄无声息地巩固了外部的控制权力。

2.3 从“数据殖民主义”与平台权力的视角看数据的再疆域化

数据的液态化并非指向一个自由散漫的无政府状态，恰恰相反，流动是为了更好地被捕获与统治。在液态数据的汪洋之上，数字平台资本正凭借其技术优势与市场权力，开展一场轰轰烈烈的“数字圈地运动”，此即数据的“再疆域化”过程。这一过程可借助“数据殖民主义”与“技术封建主义”等批判理论进行透视，二者分别揭示了再疆域化的不同面向：“数据殖民主义”侧重于全球南北之间的

资源提取不平等[9]，而“技术封建主义”则聚焦于平台与用户之间形成的新型依附关系[18]。

“数据殖民主义”指出，当代科技巨头正重复着历史上殖民帝国的逻辑，只不过掠夺的对象从土地和自然资源，变成了人类的生命数据与社交关系[9]。在健康领域，来自全球用户（尤其是发展中地区）的珍贵生物数据被源源不断地“提取”，传输至位于科技核心企业的“宗主国”数据中心进行“精炼”，最终转化为预测模型、算法专利和商业利润，而数据来源的个体与社群往往难以分享其价值。这构成了一种数字时代的健康资源不平等交换。

平台实现再疆域化的核心机制，是构建“数字围栏”。它们通过控制应用程序接口、制定互操作性标准、垄断计算基础设施，将流动的数据捕获进自身的生态闭环。例如，一家提供虚拟现实心理治疗服务的平台，通过其专属的头显设备、传感器和软件，独占用户在治疗过程中产生的全部交互与生理数据。这些数据被封锁在平台的私有数据库内，形成一个个互不连通的“数据孤岛”或“数字领地”。算法则充当了这片领地上精准丈量与收割的“智能围栏”，它不仅能圈占数据，更能实时评估和抽取数据所蕴含的价值。

这种再疆域化直接导致了3种新型不平等。一是算法偏见与健康歧视。在封闭系统中训练的算法，若基于不具代表性或有偏的历史数据，其诊断建议或风险评估会将社会偏见“代码化”，对特定种族、性别或地域群体造成系统性健康歧视。二是服务差异化定价与排斥。基于对用户健康风险的精细化预测，保险或健康服务提供商可在元宇宙中实现极致的“价格歧视”，高风险个体可能被收取天价保费或被变相排斥，侵蚀医疗保障的普惠性。三是数字人身依附关系。用户为了获得持续的医疗服务，不得不依附于特定平台，接受其不断更新的条款，让渡更多数据权利。平台则如同“数字领主”，通过收取“数字地租”（如数据使用费、高额服务分成）坐享其成，而用户则处于依附地位，其健康与数据自主权受到严重束缚。这种关系，被学者批判为是一种数字时代的“从契约到身份”的退步[18]。

这种新型依附关系的内核，在于平台凭借对基础设施和核心数据的垄断，得以持续抽取“数字地租”。在元宇宙健康领域，地租的表现形式多样且隐蔽：制药公司为获取特定患者群体的数字孪生数据以优化药物研发，需向平台支付高额“数据访问费”；保险公司为基于实时行为数据动态调整保费，须与平台签订利润分成协议；甚至广告商为触达具有特定健康偏好的用户群体，也需通过平台的“数据交易市场”完成竞价。这些费用的本质，并非对数据生产者的劳动（患者的生命体验）的合理回报，而是平台凭借其对“数字领地”的排他性控制权，向数据使用者征收的“过路费”。用户作为数据的源头，不仅未能分享这些收益，反而因自身数据被商品化而面临隐私泄露、算法歧视等风险。

这一洞察为理解新范式的制度创新提供了批判性的参照。如果说平台的再疆域化是在数字世界重建封建领地，那么第五部分将要探讨的“数据信托”与“数字公地”，则可视为对抗这种私有化垄断的集体性制度实验。数据信托将分散的个体数据权聚合为集体的谈判力量，由专业的受托人代表社群与平台协商数据使用条款，确保收益回流和数据用途符合成员福祉。而“数字公地”则对于那些具有基础性公共价值（如匿名化的全民健康统计库、开源的数字器官模型）的数据资源，通过多元共治的规则设计，防止其被任何单一平台圈占，保障其向符合公共利益的研发活动平等开放。这两种制度创新，正是试图在被平台“再疆域化”的数字荒野上，重新开辟出属于数据生产者的“共有地”。

2.4　双重困境的辩证关系　在2.2节和2.3节分别阐述了数据的液态化与再疆域化之后，本节将进一步揭示二者的辩证关系。这一关系构成了理解元宇宙健康数据治理困境的核心。

数据的“液态化”与“再疆域化”并非两个独立或先后发生的阶段，而是构成同一进程不可分割的一体两面，它们存在着深刻的辩证关系，具体如表1所示。

液态化是再疆域化的前提与动力。没有数据从传统制度框架（如医院信息系统、隐私法规）中的“融化”与释放，没有其跨场景、连续性的流动，平台资本就无从获得进行大规模捕获、聚合与分析的对象。液态化创造了巨大的、待开采的“数据石油”矿藏。平台追求垄断利润的天然倾向，则驱使其必须对这种流动性加以控制。因此，数据的自由流动幻想，实质上是为更高阶、更隐蔽的资本集中与控制铺平道路。

再疆域化是为液态化赋予私有秩序的努力。无边无际的液态数据本身会造成混乱与不确定性，不利于资本的稳定增值。因此，平台巨头通过技术架构、法律协议和经济手段，致力于将流动的数据“再凝固”起来，将其导入私有的、可管理的“河道”与“水库”中，并贴上所有权的标签。它们试图建立一种基于私人权力的数据封建秩序，以替代传统基

于公共法律与伦理的治理秩序。从这个意义上说，元宇宙中所谓的“去中心化”愿景，在实践中极易被扭曲为“从国家中心化转向平台中心化”的权力转移。

表1 健康数据液态化与再疆域化的辩证关系

维度	数据的液态化	数据的再疆域化	二者的辩证关系
核心表现	连续生成、无界复制、跨场景聚合、目的漂移、语境抽离	平台通过API、标准、算力建立“数字围栏”，形成私有化“数据孤岛”，攫取“数字地租”	液态化创造可被开采的资源；再疆域化实施对资源的私有化控制与剥削
权力机制	解构传统时空与制度边界，削弱个体知情同意与控制能力，权力弥散于流动过程	权力高度集中于平台巨头，通过技术架构与市场地位建立新型依附关系	液态化瓦解了旧权力（如医疗机构垄断），却为更集中、更隐蔽的新数字权力（平台垄断）铺路
个体处境	从权利主体沦为被动数据源，在“全有或全无”的同意困境中丧失自主性	依附于特定平台生态，面临算法偏见、服务歧视与数据依附	在液态化中失去控制权，在再疆域化中遭受系统性剥削，自主权经历双重剥夺

相较于“平台资本主义”聚焦于平台作为新的商业模式[7]，“监控资本主义”关注行为数据的剩余价值剥削[6]，本文提出的“液态化—再疆域化”框架试图解释一个更根本的结构性转变：数据的存在方式本身正在从“固态”变为“液态”，而平台的权力运作也从“占有”转向“组织流动”。这一视角将数据本体论与政治经济学相结合，为理解数字时代的权力重组提供了新的分析工具。

最终，二者共同塑造了元宇宙健康数据治理的核心矛盾。一方面，数据的液态化特征要求治理模式必须具备前所未有的弹性、适应性与全球协调性；另一方面，数据的再疆域化现实却呈现出权力高度集中、规则私有化、生态封闭化的顽固“固态”格局。治理的挑战，正在于如何破解这种“流动的盛宴被固化的高墙所分割”的悖论。

3 技术解决方案的贡献与社科批判

面对元宇宙健康数据“液态化”与“再疆域化”带来的治理危机，技术社区率先给出了一系列充满雄心的解决方案。这些方案以密码学、分布式系统与人工智能的最新进展为基础，承诺在保障隐私与安全的前提下释放数据价值。本章旨在系统审视这些技术回应的核心逻辑与潜在贡献，并引入社会科学视角对其进行深度批判。我们将揭示，技术方案虽在工具层面提供了精巧的破题思路，但若脱离对权力、公平与价值等根本性社会问题的考量，其“去中心化”与“自主权”的承诺可能沦为一种幻象，甚至无意中巩固其试图挑战的不平等结构。

3.1 技术乐观主义的回应 技术乐观主义的叙事建立在这样一个信念之上：元宇宙健康数据治理的难题，本质上可以通过更高级的算法、更安全的协议和更巧妙的系统设计来解决。其核心路径聚焦于两大方向，一是通过“隐私增强技术”确保数据“可用不可见”，二是在缺乏传统信任中介的虚拟环境中，通过“权属与追溯技术”重建可信的数据生产关系。

3.1.1 隐私增强技术（PETs）在流动中构筑“加密围栏” 为解决数据液态化带来的隐私失控问题，一系列PETs被寄予厚望，其目标是在不暴露原始数据的前提下完成计算与分析。

（1）联邦学习。联邦学习是应对数据再疆域化形成的“孤岛”的典型方案。在元宇宙医疗中，多家医院、研究机构或健康平台可在不交换本地原始数据（如患者VR康复轨迹、生理数据）的情况下，协同训练一个共享的AI模型（如疾病预测模型）。各参与方仅交换加密的模型参数更新。这在理论上实现了“数据不动模型动”，既打破了平台的数据垄断，又保护了数据隐私。例如，针对罕见病的诊断模型，可以通过联邦学习聚合全球多个医疗元宇宙的数据进行训练，而无需患者数据离开本地服务器。

（2）同态加密与安全多方计算。这类技术旨在实现“数据可用不可见”的终极形态。同态加密允许对加密状态下的数据进行直接计算，得到的结果解密后与对明文数据计算的结果一致[19]。在元宇宙中，患者可将加密的健康数据上传至云端分析服务，服务商在不解密的情况下完成数据分析，并将加密结果返回，只有患者自己能解密查看。这为将敏感健康数据分析任务外包给第三方算力平台提供了可能，同时确保了数据的绝对机密。

与同态加密不同，安全多方计算（secure multi-party computation，SMPC）将数据分散成若干“秘密碎片”（secret shares），分别交由多个互不信任的计算方持有。各方在本地对碎片进行计算，并通过特

定协议交换中间结果，最终协同完成分析任务，而任何单一计算方都无法获取完整的原始数据。在元宇宙医疗场景中，多家医疗机构可将其患者的敏感数据（如基因组信息、VR诊疗记录）碎片化后分发给多个计算节点，共同完成跨机构的流行病学统计或多中心临床研究，而无需任何一方的数据离开本地或被其他参与方还原。研究表明，采用三方计算框架的隐私保护记录链接方法，其运行速度可比传统两方方案提升14倍，且能有效规避布隆过滤器等传统方法面临的频率攻击风险。

同态加密与安全多方计算形成了互补的技术路径。前者以密文计算为核心，适合单方数据所有者将计算任务外包；后者以多方协同为核心，适合多个数据持有者共同完成联合分析而不泄露各自隐私。

（3）差分隐私。差分隐私通过向数据集中添加精心设计的随机噪声，使得任何单一数据记录的存在与否不会显著影响分析结果。在元宇宙健康研究中，当需要发布包含大量用户行为数据的聚合统计报告（如“某种虚拟疗法对特定人群的平均效果”）时，差分隐私能在保证统计效用可信的同时，从根本上防止对任何特定个体的推断与识别，从而抵御“目的漂移”带来的再识别风险。

（4）零知识证明（zero-knowledge proof，ZKP）。零知识证明允许证明者向验证者证实某一陈述为真，而无需披露陈述背后的具体信息[20-21]。其核心价值在于打破“验证必先知情”的传统逻辑，验证者可以确信某结论成立，但对得出结论所依据的数据一无所知。自Goldwasser等[20]提出零知识证明的原始概念以来，经过Blum等[22]的非交互式改进，以及近年来的效率优化，zk-SNARK等高效实现已具备实际应用可能[23]。

在元宇宙医疗场景中，ZKP适用于三类典型应用。其一，身份属性的选择性披露，比如患者可向远程医疗平台证明自己“年龄超过18岁”或“已完成疫苗接种”，而无需透露具体的出生日期或疫苗接种记录。其二，数据合规性的可验证证明，比如医疗机构可向监管机构证明其数据处理流程符合隐私合规要求（如数据仅用于约定目的），而无需公开数据处理的完整细节。其三，计算结果的正确性验证，比如当使用同态加密或安全多方计算完成数据分析后，ZKP可用于证明计算过程的正确性，确保输出结果未被篡改。ZKP的局限性在于计算开销较大，且许多高效实现（如zk-SNARK）依赖可信初始化设置[24]。然而，随着zk-STARK等无需可信设置的新方案发展，ZKP在医疗数据治理中的应用前景正在扩展。

（5）可信执行环境（trusted execution environment，TEE）。与前文所述密码学方法不同，TEE依托CPU硬件层面的安全能力，在计算平台内部创建一个隔离的“安全飞地”（secure enclave）。在该飞地中，数据及其处理过程对操作系统、云服务商乃至硬件管理员均不可见，仅能通过预定接口输入数据并获取结果。TEE的核心优势在于兼具安全性与高性能，它能够在保证数据机密性的同时，支持复杂计算任务（如AI模型推理）以接近明文的速度运行，但这种安全建立在信任硬件厂商的前提之上[25-26]。

在元宇宙医疗场景中，TEE尤其适用于对实时性要求苛刻的数据处理任务。例如，VR/AR康复训练中需要毫秒级响应的生理数据分析（如跌倒检测、动作矫正），若采用同态加密可能因计算延迟导致体验中断，而TEE则可在确保数据不出安全飞地的前提下实现实时反馈。研究表明，采用Intel SGX或AMD SEV等TEE技术的联邦学习系统，其计算开销远低于基于HE的方案。然而，TEE的局限性在于其安全性依赖于硬件制造商的可信性（需信任芯片厂商），且面临侧信道攻击等新型威胁[27]。

3.1.2　权属与追溯技术为液态数据锚定“数字产权”　为解决数据权属模糊、流向不可控的问题，区块链及相关技术被视为构建可信数据经济的基础设施。

（1）区块链与数据溯源。区块链的不可篡改、可追溯特性，使其成为记录数据生命周期的理想账本。每一次元宇宙健康数据的创建、访问、授权交易都可以作为一条哈希上链存证，形成不可抵赖的审计线索。这为监管机构提供了穿透式监管的工具，也为个体主张自身数据权利提供了技术证据。

数据溯源（data provenance）在此扮演着关键角色。它不仅记录“谁在何时何地访问了数据”这类表层操作日志，更重要的是追踪数据从生成到衍生的完整谱系，包括原始数据来源于哪次VR康复训练、经过何种算法处理生成了新的衍生数据、被哪些第三方模型调用用于训练、以及这些调用是否符合原始授权约定。在元宇宙医疗场景中，患者的数字孪生数据可能被多次聚合、转换和衍生，比如一段步态数据可能被用于训练康复算法，其衍生特征又被用于保险风险评估。若缺乏精细化的溯源机制，个体将无从知晓自身数据的“后代”流向何方、被谁利用。区块链的链式结构和时间戳机制，使得

这种复杂的谱系关系得以被忠实记录和验证，为后续的问责与收益分配提供了可信基础。

（2）智能合约与动态授权管理。基于区块链的智能合约可以编码复杂的、细粒度的数据使用规则，实现从静态同意向动态授权的范式跃迁。

传统知情同意是一次性的、模糊的授权，用户在数据采集时签署一份宽泛的同意书，此后便对数据的实际使用失去控制。动态授权管理则通过智能合约将这种静态权利转化为可编程的、持续更新的控制能力。其核心机制体现在3个层面。

其一，细粒度的条件控制。患者可以设定高度定制化的授权条款，比如其睡眠数据仅能以加密形式提供给A研究机构用于为期一个月的帕金森病研究，且每日调用次数不得超过限定阈值；若机构欲将数据用于商业开发，则需通过合约触发自动支付流程，向患者补偿约定数额的代币。

其二，时间维度的权限管理。授权不再是永久的，而是可设定精确的有效期。一旦研究期满，智能合约自动撤销访问权限，无需患者主动操作。这尤其适用于元宇宙中的持续性数据流场景，用户可授权平台实时访问其康复训练数据，但限定仅在该次训练会话期间有效，训练结束后权限即刻终止。

其三，事后的收益分配与撤销机制。当第三方基于用户数据开发出商业产品并获得收益时，智能合约可根据预设的分配规则，自动向数据源用户支付版税分成。同时，若用户发现数据被滥用，可触发合约中的“紧急撤销”条款，切断后续的数据访问，并将违规行为上链存证，为司法救济提供证据。

这种动态授权管理使得元宇宙中的“知情同意”从一个静态的法律文书，转变为一种实时的、可验证的技术流程，在保障用户控制权的同时，也为合规的数据利用提供了自动化基础设施。

（3）去中心化数字身份。以自主主权身份为代表，用户可拥有一个不依赖于任何中心化平台（如科技公司或政府）的、可移植的数字身份。该身份是用户控制其元宇宙健康数据的枢纽，所有数据授权、访问日志都与此身份关联，用户可以自主选择向不同服务方披露身份的不同维度属性，从而在虚拟世界中重建一种“携带式”的个人数据主权。

值得注意的是，零知识证明虽然主要用于隐私增强计算（3.1.1节），但其“可验证性”特性也可与本节所述的权属追溯技术结合使用。例如，在去中心化身份系统中，ZKP可用于实现属性的选择性披露；在智能合约授权中，ZKP可用于证明用户符合某项授权条件（如已完成知情同意）而不泄露具体身份信息。

技术乐观主义者勾勒的图景极具吸引力：一个数据自由流动但隐私无忧、价值共创但权属清晰、全球协作但个人自主的元宇宙医疗未来。然而，这幅蓝图主要是在工程与逻辑的层面自洽，当其置于复杂的社会现实与权力关系中时，将面临深刻的质疑。

3.2 社科视角的深度批判 社会科学视角的批判并不否认上述技术的工具价值，而是尖锐地指出，将治理难题过度简化为技术问题，可能忽视乃至掩盖了更为根本的政治经济与社会伦理矛盾。本节从权力分配、经济公平、价值抉择、责任归属、数字主权五个维度，系统揭示技术治理方案在元宇宙健康数据领域的内在悖论。这五个维度正是对第二章所揭示的“液态化—再疆域化”双重运动的系统性回应，即技术方案如何在试图应对数据液态化的过程中，反而强化了平台的再疆域化权力。

3.2.1 权力再分配的幻象：从软件去中心化到硬件再中心化 区块链、分布式账本等技术常被赋予“去中心化”和“民主化”的光环，但社科批判指出，这往往是一种“技术中心化”替代“组织中心化”的幻象[14]。技术系统的权力结构并未消失，而是以新的形式重新集中。这种从软件到硬件的权力再集中，正是第二章所论述的“再疆域化”在技术层面的具体体现。

（1）软件层的去中心化神话。技术的开发、标准的制定、核心协议的维护，依然高度集中在少数科技巨头、精英开发团队或学术机构手中。普通用户与医疗机构在技术黑箱面前处于绝对的知识劣势。这导致权力并未消失，而是从传统的机构管理者转移到了更不透明、更难问责的技术专家与平台运营者手中。所谓的“去中心化”，可能只是治理责任的分散化与模糊化，而非权力的民主化[28]。运行节点、理解智能合约、管理私钥等操作具有较高的技术与认知门槛，这使得在传统医疗体系中处于弱势的群体（如老年人、低收入群体、数字素养不足者）在新技术体系中进一步被边缘化，形成“数字治理鸿沟”。他们的数据可能因无法有效行使“自主权”而事实上被默认的协议所处置。

（2）密码学协议的精英掌控。零知识证明技术的引入进一步强化了这一权力转移。高效的ZKP实现（如zk-SNARK）普遍依赖“可信初始化”设置，在系统启动阶段，需由一组参与者共同生成公共参考字符串，若该过程被操纵或秘密参数泄露，整个系统的安全性将土崩瓦解[24]。这一初始化过程往往由少数开发团队或机构掌控，普通用户既无力参

与也无从监督。理解ZKP的数学原理、验证证明的有效性，需要远高于普通数字素养的专业知识，这进一步拉大了技术精英与普通用户的认知鸿沟。所谓的“无需信任”，实际上是将信任从传统机构转移到了掌握初始化密钥或能够编写ZKP电路的技术专家手中。

（3）硬件层的再中心化。当隐私保护的根基从密码学转向硬件时，权力集中以更隐蔽的形式出现。当前主流的可信执行环境（TEE）技术（如Intel SGX、AMD SEV、ARM TrustZone）均由少数几家芯片巨头掌控[25-26]，这意味着元宇宙健康数据的最终安全性，高度依赖于这些商业公司的硬件设计、密钥管理体系和安全更新政策。一旦某厂商的TEE实现被曝出硬件级漏洞（如近年多次出现的SGX侧信道攻击），所有依赖该技术的医疗应用将同时暴露于风险之下，且修复完全依赖于厂商的响应速度与诚意。2023年曝光的“Downfall”漏洞影响多代Intel处理器，修复需等待厂商发布微码更新，这种“硬件层锁定”使得医疗数据安全受制于芯片巨头的商业决策，形成了比软件层更难制衡的权力集中。这种“硬件层的再中心化”，比软件层的权力集中更为隐蔽，也更难通过开源社区或市场竞争来制衡。

（4）技术演进的路径依赖。值得警惕的是，技术系统的权力集中并非静态，而是在演进中不断自我强化[29]。早期选择某种ZKP方案（如zk-SNARK）意味着后续系统将深度依赖其可信初始化流程；早期适配某家TEE芯片意味着未来迁移成本呈指数级上升。这种“路径依赖”使得最初看似中性的技术选择，随着时间的推移固化为难以撼动的权力结构。当我们在元宇宙医疗的黎明期选择技术路线时，实际上也是在为未来几十年的治理格局投下关键一票，而这一投票权，恰恰掌握在少数技术精英和芯片巨头手中。

3.2.2　*效率与公平的悖论：隐私技术的成本排斥*　隐私与安全并非无代价的福音，其成本可能以意想不到的方式加剧不平等。当隐私保护本身成为一种稀缺资源时，技术非但未能促进普惠，反而可能加深既有的社会分化。

（1）算力成本的结构性不平等。联邦学习需要频繁的加密通信和分布式优化，同态加密的计算开销比明文操作高出数个数量级[19,30]。这些成本最终会转化为更高的云服务费用和更昂贵的医疗数据分析产品。资源丰富的顶尖研究机构或商业平台能够承担，而资金拮据的社区医院或公共卫生部门则可能被排除在外，导致健康数据研究与应用向资本密集型方向倾斜，违背医疗普惠的初衷。

（2）密码学隐私的“合规奢侈品”化。零知识证明带来了显著的成本问题，进一步加剧了技术应用的不平等。生成一个zk-SNARK证明虽已优化至毫秒级，但其可信初始化过程需要“信任设置仪式”，参与方若合谋可伪造证明[24]。zk-STARK虽无需可信设置，但其证明规模可达数百KB（通常为200-300KB），远大于zk-SNARK的几百字节，验证成本较高[31]。在元宇宙医疗场景中，若要求每一次数据交互、每一笔授权记录都附带ZKP验证，其累积计算成本将使小型医疗机构难以承受，这种“隐私税”可能进一步加剧医疗资源不平等。这可能导致ZKP沦为大型平台的“合规奢侈品”，它们有能力投资专用硬件和优化算法来满足隐私合规要求，而资源匮乏的机构则被迫在“成本高昂的完美隐私”与“成本低廉的隐私裸奔”之间二选一。

（3）硬件门槛与数字鸿沟。可信执行环境不仅带来权力集中问题，也制造了新的经济门槛。适配特定TEE方案（如为Intel SGX优化算法）需要专门的技术积累和开发投入，更换硬件平台面临高昂的重构成本[26]。对于资源有限的公共卫生机构而言，这种硬件锁定效应可能使其长期被排除在隐私计算的主流生态之外。

（4）性能妥协的伦理权衡。差分隐私添加的噪声可能降低数据分析的精度；联邦学习中非独立同分布的数据可能导致模型性能下降[32]。在诊断、预后等对精确性要求极高的医疗场景中，这种为隐私付出的性能代价是否可接受？这构成了一个严峻的伦理权衡：我们是否愿意为群体的隐私保护，承受对个体患者诊疗准确性的潜在微小风险？技术方案本身无法回答这个价值抉择问题。

3.2.3　*治理与价值的不可通约：“代码即法律”的限度*　最深刻的批判指向技术治理的哲学基础。“代码即法律”的信奉者认为，可自动执行的智能合约能超越低效、模糊的人类法律，实现绝对的规则公正[33]。然而，这一理念将治理问题化约为技术问题，忽视了社会价值的复杂性与不可通约性。

（1）规则的刚性与社会情境的复杂性。智能合约的规则是预先编写、僵化执行的，但医疗实践充满伦理灰色地带和需要人道主义例外的情境。例如，一项严格限制数据共享的合约，在突发公共卫生事件（如元宇宙内追踪传染病接触者）时，可能阻碍必要的公共利益实现。代码无法理解“情有可原”，而人类社会的治理恰恰依赖于这种情境化的判断与协商。

(2)价值抉择的技术固化。数据治理的核心问题,隐私与公益的边界、个人权利与集体利益的权衡、商业价值与社会价值的分配,本质上是政治问题和伦理问题。技术可以提供实现某种既定价值的工具,但无法替代民主社会就价值排序进行公开辩论、协商并达成共识的过程。将价值抉择编码进看似中立的算法,实则是将特定的、通常是开发者的价值偏好进行"技术固化",这是一种更具隐蔽性的专制[34]。

(3)健康认知的技术化重构。更深层的问题是,当健康数据被持续量化、算法化为可计算的指标时,我们对"健康"本身的理解也在悄然改变。元宇宙中的数字孪生体、持续追踪的行为数据、AI生成的健康评分,正在塑造一种新的"数据化健康观"[2],那些难以量化但同样重要的维度(如患者的心理体验、疼痛的主观感受、治疗的尊严价值)可能被边缘化[1]。这种认识论层面的重塑,使得患者逐渐从"体验的主体"异化为"数据的集合",而技术系统则成为定义"何为健康""何为有效治疗"的隐蔽权威。

(4)算法黑箱与民主监督的缺失。当健康决策越来越多地由算法辅助甚至主导时,算法的内部逻辑却往往处于不透明状态。即便技术方案提供可解释性模块,其解释也往往面向技术专家而非普通患者。这种"解释鸿沟"使得受算法决策影响的个体难以理解、质疑或申诉,技术系统因此绕过了民主监督的基本程序。

3.2.4 责任与信任的消解:自动化系统中的问责黑洞 当错误发生时,谁应当负责?在高度去中心化、自动化的技术系统中,这一问题的答案变得极其模糊。责任主体的消解,使得传统的法律追责与救济机制难以运作,最终损害的是个体的权利保障。

(1)责任主体的模糊化。当因加密算法漏洞导致数据泄露,或因智能合约漏洞导致授权错误时,责任在开发者、矿工、节点运营商、用户之间飘移不定。这种"责任漂浮"状态,使得受害者难以找到明确的追责对象,法律救济途径因此被堵塞。

(2)密码学证明的责任困境。零知识证明的引入非但未能化解责任困境,反而可能使其更加复杂。当ZKP验证通过但事后发现证明内容虚假(如证明者利用数学漏洞构造了欺骗性证明),或当ZKP系统的可信初始化参数被泄露导致大规模伪造证明时,受害者应向谁追责?是设计ZKP电路的开发者、执行初始化的参与者、运行验证节点的矿工,还是部署该系统的平台?ZKP的数学保证是"无条件"的,但其工程实现和初始化的安全性却是"有条件"的[23],而这"条件"的责任归属,在去中心化、自动化系统中恰恰最难以界定。

(3)硬件后门的追责难题。可信执行环境将信任基础从密码学转移到硬件厂商,但硬件层的责任问题同样悬而未决。若TEE芯片被曝存在设计后门,或因微码更新导致数据泄露,受害者应向芯片厂商追责,还是向部署该硬件的平台追责?芯片厂商往往通过终端用户许可协议限制自身责任,而平台则可能将责任推给硬件供应商,形成责任链条的无限回溯。

(4)技术麻醉效应。当技术系统以"数学保证""硬件级安全"等名义声称解决了隐私问题时,可能诱导社会降低对制度监管的重视。然而,技术方案的安全性是概率性的,而非绝对性的。例如,联邦学习虽声称"数据不动模型动",但研究表明,通过模型参数反推原始数据的"梯度泄露攻击"已被证实可行[35-36]。这种"技术麻醉"效应使得社会放松警惕,一旦技术防线被突破,将造成更大规模的损害。

3.2.5 主权与依附:硬件层的数字殖民主义 当数据治理的根基从软件层延伸至硬件层时,一个更根本的问题浮出水面:谁掌控着数据赖以运行的基础设施?这不仅是技术问题,更是主权问题。这一发现与第二章关于"数据殖民主义"的论述形成呼应,表明再疆域化不仅发生在软件层的数据流动中,更延伸至硬件层的基础设施控制[9]。

(1)供应链信任的单向强加。TEE要求用户"信任"芯片厂商的硬件设计和密钥管理基础设施,但这种信任是单向强加的,用户既无法验证芯片内部是否留有后门,也无从监督厂商的密钥使用是否合规[25]。在元宇宙医疗的跨国场景中,若某国的医疗平台采用他国厂商的TEE芯片,其患者的敏感健康数据的安全性,实际上建立在两国政治关系与厂商商业道德的双重"黑箱"之上。

(2)硬件锁定的数字依附。一旦医疗应用深度适配特定TEE方案,更换硬件平台将面临高昂的重构成本[26]。这种"硬件锁定"效应,使医疗机构和患者被绑定在特定芯片厂商的生态内,形成一种新的依附关系:数据虽"自主",运行数据的土地却属于他人。这与前文讨论的数字地租形成呼应,平台抽取的是软件层的地租,而芯片厂商抽取的是更深层的硬件层地租。

(3)从软件殖民到硬件殖民。如果说数据殖民主义是平台资本对全球南方健康数据的"软件层掠夺"[25],那么TEE的硬件垄断则构成了"硬件层控

制”。全球南方的医疗系统不仅可能失去对数据的控制权，甚至连数据赖以运行的计算基础设施也掌握在他国芯片巨头手中。这种双重依附，使得数字时代的南北不平等从经济领域延伸到技术主权层面。当医疗数据安全依赖于他国芯片厂商的商业决策和所在国的政治环境时，数字主权便面临实质性挑战。

3.2.6　小结：技术治理的结构性局限　综观本节所述，从软件层的密码学协议到硬件层的可信执行环境，技术方案在回应隐私挑战的同时，也以其独特的方式复制乃至深化了权力集中的悖论。表2汇总了技术乐观主义承诺与社会科学批判现实之间的多重张力，这些张力共同揭示了一个根本困境：当治理问题被化约为技术问题时，被排除出议程的恰恰是最关键的社会政治追问。

表2　技术承诺与社科现实之间的张力

维度	技术乐观主义的承诺	社会科学视角的批判现实	核心张力
权力分配	去中心化网络将权力归还用户	权力向技术精英和芯片巨头集中，形成软件—硬件双重垄断	去中心化理想 vs. 再中心化现实
经济公平	隐私技术普惠所有用户	高昂成本制造“隐私税”，弱势群体被排除	技术普惠愿景 vs. 成本排斥
价值抉择	代码规则确保治理确定性	刚性规则无法处理伦理复杂性与情境例外	代码理性 vs. 社会协商
责任归属	透明算法实现自动问责	责任主体模糊化，受害者难以追责	自动化信任 vs. 问责真空
数字主权	硬件级安全提供终极保护	硬件垄断导致供应链依附和主权侵蚀	技术安全 vs. 主权自主

这一批判性审视并非要否定技术的工具价值，而是旨在划清其能力的边界。技术可以构筑精密的锁具与管道，却无法决定数据之河应流向何方、灌溉何处、又由谁受益。治理元宇宙健康数据，不能止步于工程思维的“怎么办”，而必须首先回答社会政治的“为谁治理”和“为何治理”。尤其值得警惕的是，当隐私保护的根基从软件密码学延伸至硬件层时，我们非但未能摆脱权力集中，反而可能陷入更隐蔽、更难制衡的“硬件封建主义”。

正是带着这一认识，我们将目光转向更广阔的社会制度层面。下一章将深入剖析法律监管与市场自我调节模式在面对元宇宙健康数据双重运动时的结构性困境，考察现有的制度框架是否能为这些技术嵌入更坚实的规则底座。

4　现有治理模式的困境与转型需求

前文剖析了元宇宙健康数据“液态化”与“再疆域化”的双重运动，并检视了纯技术解决方案的局限。本章对法律监管与市场调节模式的批判，正是对第二章所揭示的双重运动的制度层面回应，既有制度如何因无法适应数据液态化而失效，又如何在不经意间强化了平台的再疆域化权力。我们将论证，面对这一根本性变革，奠基于工业时代与早期互联网数据的传统治理模式，无论是依赖成文法的“法律监管模式”，还是信奉市场理性的“自我调节模式”，均已陷入系统性失效。它们的困境并非源于执行不力，而是其内在逻辑与元宇宙数据的本质属性发生了深刻错配。因此，治理范式必须进行根本性转型，从单一主体的管控，迈向“国家—市场—社会”协同的多元共治，即所谓“第三代治理”。

4.1　法律监管模式（以GDPR、HIPAA等为例）的滞后性　第3章的批判表明，技术方案虽能构筑隐私保护的“锁具与管道”，却无法替代制度层面的规则底座。当我们将目光转向既有的制度框架时，首先映入眼帘的便是以GDPR和HIPAA为代表的法律监管模式。

以欧盟《通用数据保护条例》（GDPR）和美国《健康保险携带和责任法案》（HIPAA）为代表的现代数据保护法，是应对数字时代隐私风险的里程碑。它们确立的“知情同意”、“目的限定”、“数据最小化”及“主体权利”等原则，构成了当下数据治理的基石。然而，这些原则在应对元宇宙中实时、连续、多模态的“数字生命流”时，显露出结构性的滞后与无力。

首先，“数据最小化”与“目的限定”原则在元宇宙海量情景化数据前近乎失效。GDPR要求数据收集应限于“与处理目的相关的、适当的、最小化的”范围，但元宇宙的沉浸式体验依赖于对用户生物特征（如眼球追踪、脑电波、手势）、空间位置、行为轨迹及情感反应的全景式、持续性收集。在此场景下，何为“最小必要”变得极其模糊。例如，为提供流畅的VR康复训练而收集的精细运动数据，是否“必要”包含了可以推断用户精神专注度的微表情数据？这些数据在收集瞬间可能仅为优化体验，但

其作为连续流的一部分，蕴含着未来不可预见的医疗或商业价值，这使得“目的限定”在数据生成之初便可能被突破。这种数据用途的不可预见性，正是第二章所论述的“数据液态化”中“目的漂移”特征在制度层面的体现。

其次，“知情同意”模型在实践中的崩塌。法律设想用户是在特定时点、基于清晰信息做出理性授权的“数据主体”。但在元宇宙中，用户通常只能通过点击冗长、晦涩的“服务条款”来接入整个虚拟世界。这种“捆绑式”、“一揽子”同意，与GDPR所要求的具体、知情、自由给予的同意相去甚远。用户为了获得基本的医疗服务或社交功能，不得不让渡自身最敏感的生物识别信息，导致同意在实践中沦为一种被迫的形式，而非真正的自主控制。更重要的是，元宇宙的持续数据流使得知情同意面临“认知超载”困境，用户即便有机会阅读条款，也难以理解数据被持续采集、聚合、衍生的复杂后果。这种认知不对称使得同意从“理性授权”异化为“被迫点击”[37]。

再者，数据主体权利的行使面临巨大障碍。即便法律赋予用户访问、更正、删除（被遗忘权）和可携带其数据的权利，在元宇宙复杂的数据生态中也难以落地。数据在用户、设备商、平台运营商、第三方应用开发者之间瞬时流动、聚合与衍生，其存储位置与控制权高度分散。当用户想行使其“被遗忘权”时，可能面临无从知晓数据副本存在于何处、由谁掌控的困境，更遑论彻底删除。这种“去中心化追责风险”使得法律赋予个体的权利武器，在技术上变得钝化。

最后，法律体系的内在矛盾与高昂合规成本削弱了其效能。不同领域、不同司法辖区的法律（如数据法、消费者法、竞争法）在适用于元宇宙时可能产生重叠甚至冲突，造成“法律不一致性”。同时，将“隐私嵌入设计”等原则付诸实践需要巨大的资源投入，这实际上将合规能力塑造为一种新的市场壁垒，只有大型科技公司才能承担，从而意外地巩固了其市场地位，与小企业的发展形成矛盾。法律本意为制衡权力，却在执行中可能加剧了权力的集中[38]。

此外，元宇宙的全球穿透性使得法律的地域管辖陷入困境。一场跨国VR远程手术中，患者位于A国、医生位于B国、数据服务器位于C国、平台总部位于D国，应适用哪国法律？GDPR的长臂管辖虽试图应对此问题，但其执行高度依赖国际司法协作，而元宇宙的实时数据流使得传统的事后司法救济模式难以跟上技术节奏。这种“法律的时空错配”，使得监管往往在数据已造成损害后才姗姗来迟[39]。

4.2 *市场自我调节模式的失效* 如果说法律监管试图以国家权力为数据流动划定边界，那么市场自我调节模式则信奉另一种逻辑：将数据视为商品，相信供求关系能自发形成最优秩序。然而，这一逻辑在元宇宙健康数据面前同样遭遇滑铁卢。

数据的商品化逻辑必然导向垄断与“平台资本主义”的强化。健康数据，尤其是元宇宙中高维、连续的生物行为数据，具有显著的规模效应和网络效应：数据越多，算法越精准，吸引的用户越多，进而产生更多数据。这一正反馈循环天然排斥竞争，促使主导平台（“看门人”）建立封闭的“数字围栏”，将用户和数据锁定在自有生态内。大数据市场的研究表明，数据一定程度的排他性、质量和价值的差异性、高昂的收集成本、锁定效应和转换成本以及网络效应等实然属性均会提高市场的进入壁垒，强化主导经营者的市场地位[38]。其结果不是开放、竞争的数据市场，而是少数“技术利维坦”对数字健康疆域的私有化统治。市场调节在这里失灵了，因为它无法阻止赢家通吃后的市场支配地位滥用。

Apple Health生态是平台再疆域化的典型样本，也是第二章“再疆域化”概念的具象体现。通过HealthKit API和ResearchKit框架，Apple将iPhone、Apple Watch和第三方应用的健康数据整合至其封闭生态中。用户虽可通过“健康”App查看数据，但数据向其他平台（如Android设备或非苹果认证的医疗机构）的迁移受到严格限制。2024年发布的Apple Vision Pro进一步将眼球追踪、手势识别等空间计算数据纳入健康监测体系，形成更完整的数据闭环。这一生态展示了“数字围栏”的典型特征：技术标准（如HealthKit）成为数据流动的“关卡”，平台通过硬件（Apple Watch传感器）和软件（iOS系统）的双重锁定实现对健康数据的排他性控制。

更为深刻的是，健康数据商品化会引发严重的“外部性”问题，即交易双方未承担的全部成本或产生的收益，由社会承担。其负外部性至少有以下三点。

第一，公共利益受损。当健康数据被私有平台垄断，用于公共卫生研究、流行病预警或普惠性医疗创新的数据访问就可能受阻，损害社会整体福利。健康数据的公共物品属性意味着，其过度商品化将导致“公地悲剧”的反向，数据资源被私人占有时，社会整体的公共健康利益反而受损。这与

Elinor Ostrom所警示的公共资源治理困境形成呼应[40]。

第二，加剧健康不平等。基于精细化健康数据的“差异化定价”可能使高风险或低收入群体无法负担保险或优质服务，算法偏见则可能在数字世界系统性地复制和放大现实社会中的歧视。研究表明，广泛使用的医疗算法在预测黑人患者的健康风险中显示了严重的种族偏见，该算法将医疗费用作为医疗需求的代理，但由于缺乏准入条件及存在系统性种族主义，黑人所招致的医疗成本比白人低，因此算法低估了黑人患者的健康需求[41]。

第三，侵蚀人的主体性。将生命体验数据化并明码标价，实质上是在推动一种“数字异化”，人的生物性、情感和社交互动被降格为可供提取和交易的生产要素，这与医疗“以人为本”的伦理根本相悖。市场机制无法为这些深刻的社会伦理问题定价，因此其调节是失灵的。

更深层的问题是，健康数据的商品化是否应有伦理边界？当个体的基因组数据、脑电波数据、情绪反应被明码标价，我们是否在默许一种“生命本身的商品化”？这种追问触及市场逻辑的根本限度，有些东西一旦被标价，其内在价值便已受损。医疗领域尤其如此，健康不是消费品，患者不是消费者，将医患关系重构为“数据卖家”与“数据买家”的交易关系，本身便是对医疗伦理的背离。

4.3　迈向多元协同共治：国家、市场与社会的角色重构　既有的“国家中心”的法律管控与“市场中心”的自我调节双双陷入困境，表明元宇宙健康数据的治理需要超越这种二元对立，建构一个更具适应性、包容性和回应性的新范式。这就是强调多元主体协同、多种工具并用的“第三代治理”（亦称“多元协同共治”）。这一转型的核心在于承认治理权力的分散化与治理责任的共享性。它不再将国家视为唯一的规则制定者和执行者，也不盲目崇拜市场的自发秩序，而是寻求一种动态平衡。

（1）国家的角色转型：从直接控制者到“元治理者”与底线守卫者。国家的作用并非减弱，而是变得更加关键和精巧。鲍勃·杰索普提出的“元治理”概念，正是强调国家对治理机制的统筹协调，以防止治理失败[42]。具体而言，国家需要从事后惩罚转向事前介入与合法性引导，负责制定顶层设计、设定核心伦理与法律红线（如禁止某些类型的健康歧视）、并确保不同法规间的协调一致。同时，国家需扮演“仲裁者”和“赋能者”角色，一方面对科技巨头进行反垄断监管，防范“数字利维坦”；另一方面通过监管沙盒、标准制定等柔性工具，为负责任的创新预留空间。

（2）市场的角色修正：从无序扩张到负责任的创新主体。企业，尤其是平台企业，需要在追求商业利益的同时，内化其行为的社会成本。这要求其超越合规，践行“通过设计保护隐私”和“通过设计保障伦理”。市场机制应被引导至建设开放、互操作的数据基础设施和可信计算环境，而非构筑封闭花园。例如，采用标准化API促进数据在保障安全下的有限、可控流通。

（3）社会的角色崛起：从被动客体到积极参与的治理主体。这是第三代治理最具革命性的维度。它意味着患者社群、专业协会、伦理委员会、公民社会组织等社会力量应被制度性地纳入治理架构。其参与形式包括：对算法进行独立的审计与影响评估；通过数据信托等新型法律机构，代表集体管理成员的健康数据，在保护隐私的前提下促成数据用于公共利益[43]；以及提升公众数字素养与健康数据主权意识，使个体能从“数据主体”转变为真正的“治理主体”。

欧盟《健康数据空间条例》（EHDS）是应对平台再疆域化的制度性回应。该条例要求所有电子健康记录系统采用欧洲电子健康记录交换格式（EEHRxF），确保数据在不同成员国之间的互操作性。同时，EHDS建立了“健康数据访问机构”（Health Data Access Bodies）作为各国数据治理的协调机制，研究人员可通过这些机构申请访问匿名化的健康数据。这一案例展示了“国家作为元治理者”的角色：不是直接控制数据，而是通过标准制定和机构设置，为数据流动建立规则框架，防止平台私有化垄断。

需要清醒认识的是，多元协同共治并非一剂立竿见影的万能药。多元主体协同意味着决策过程的复杂化与时间成本的增加，当需要就某一数据使用规则达成共识时，国家、市场、社会三方的话语体系、利益诉求与行动逻辑可能存在深刻分歧。历史经验表明，多元治理结构本身并不能自动防止权力集中，强势主体可能通过资源控制、议程设置、话语霸权等方式，将多元形式转化为实质上的单方主导。因此，第三代治理的制度设计必须包含对“元权力”的制衡机制，如为弱势群体提供参与补贴、设立独立监督机构、建立议程公平规则等，防止“协商”沦为“扯皮”，避免强势主体在“多元共治”的外衣下继续主导议程。此外，多元治理对参与主体的能力要求较高，可能形成新的“参与鸿沟”。第三代

治理与其说是一种既成模式，不如说是一个需要持续探索的“治理实验场”。

综上所述，我们整理了元宇宙健康数据治理模式的演变与对比，具体见表3。由表3我们可以看到，现有治理模式的困境揭示了单向度思维的局限。元宇宙健康数据的治理，必须走向一个承认复杂性、拥抱多样性、并强调协同韧性的新范式。这不仅是技术和管理上的挑战，更是一场深刻的社会实验，关乎我们如何在数字时代重新定义健康、隐私、公平与人的尊严。

表3 元宇宙健康数据治理模式的演变与对比

治理模式	核心理念	主要工具	在元宇宙健康数据治理中的困境	转型方向
第一代：法律监管模式	国家中心主义，通过统一、刚性的成文法进行外部控制	立法、行政监管、司法诉讼、处罚	原则滞后于技术现实；合规成本高企；权利行使困难；跨国执法复杂	国家向“元治理”与底线规制转型，提升法律的一致性与前瞻性
第二代：市场自我调节模式	市场中心主义，相信竞争与契约能自发产生最优秩序	产权界定、市场竞争、企业自律、服务条款	必然导致数据垄断与平台霸权；无法解决负外部性（公益损害、不平等）；侵蚀人的主体性	市场需在伦理与合规框架内创新，承担社会责任，推动互操作与开放生态
第三代：多元协同共治模式	网络化治理，强调国家、市场、社会等多主体基于共识的协同与合作	“回应型”法律框架、行业标准、技术伦理、社群公约、数据信托、参与式审计等	主体间协调成本高、权责划分难、共识形成慢；存在“协商被俘获”风险；对参与主体能力要求较高，可能形成“参与鸿沟”	构建包含法律、代码、市场、规范的混合治理体系，培育各主体的治理能力，形成动态平衡的治理共同体；在实验迭代中探索本土化路径

本章提出的多元协同共治转型方向，正是试图回应第二章所揭示的核心矛盾：如何在承认数据液态化现实的同时，有效制衡平台的再疆域化权力。下一章将在此基础上，进一步构建微观技术层（如默认隐私保护、互操作标准）、中观制度层（如数据信托、数字公地、参与式审计）、宏观法律层（如数字人格权、数字守门人监管）的三层治理框架，使本章提出的“国家—市场—社会”协同理念落地为可操作的制度设计，为从“批判”走向“建设”提供更具操作性的路线图。

5 构建跨学科的元宇宙健康数据治理新范式

前文揭示了现有治理模式与技术方案在应对元宇宙健康数据双重运动时的深层困境。第二章提出的“液态化—再疆域化”双重运动框架揭示，元宇宙健康数据治理的核心矛盾在于：数据的高度流动性要求治理模式具备弹性与适应性，而平台的再疆域化权力却呈现出权力集中、规则私有化的“固态”格局。回应这一矛盾，需要从理念层面完成根本性转向。历史经验表明，当技术变革引发根本性的社会关系重组时，修补旧范式往往徒劳无功，必须进行理念与架构的重塑。本章旨在提出一个积极的、跨学科的治理新范式，这一范式不以禁锢数据流动或回归中心化控制为目标，而是致力于在流动性中建立秩序，在开放中保障权益，其核心在于从对抗性管控转向关系性治理，从孤立思维转向系统生态思维。

5.1 从原子化权利到关系性生态的核心理念转变

构建新范式，首要的是完成两项根本性的理念转向，它们构成了所有后续制度与技术创新之魂。

第一，从“数据所有权”到“数据关系权/数据管理权”。传统法律框架执着于界定数据“归谁所有”，这实质上是将数据类比为土地、房屋等排他性动产。然而，元宇宙中的健康数据作为持续生成、多方贡献（个人生成、平台处理、算法解读）、价值在关联中涌现的“生命流”，其“所有权”在法理与实践上皆难以清晰切割，强行界定反而会引发无尽纠纷或导致数据僵化。

新范式应超越所有权思维，转向“数据关系权”框架。这一理念由学者如萨尔坎·巴哈莫特所倡导，其核心是关注数据实践中的动态关系、相互义务与影响力，而非静态的归属。它意味着治理的重点不在于回答“数据是谁的财产”，而在于规范“谁在何种情境下能对数据做什么，并需承担何种责任”。与之配套的是强化“数据管理权”，即赋予数据主体（个人或集体）一系列针对其数据生命周期的实质性控制权力，包括知情权、访问权、反对权、可携带权，以及至关重要的“持续管理权”。即便数

据已被共享，主体仍有权知晓其流向、用途变更，并能在特定条件下撤回授权或要求收益分享。这实质是将权利从“产权”的控制逻辑，转向“治理”的参与与问责逻辑。关于隐私、信息与数据三者的区分，申卫星指出应在严格区分权利客体与权利本身的基础上，构建数字时代个人权利的差序格局——隐私、信息与数据分别处于事实层、描述/内容层和符号层，三者之上分别成立隐私权、个人信息权与数据所有权[44]。

第二，从“个人隐私保护”到“集体数字福祉与生态系统健康”。个人隐私保护仍是基石，但仅此不足以应对系统性风险。当平台算法基于有偏数据导致对特定族群的健康歧视，当数据垄断阻碍公共卫生研究时，损害的是集体利益和整个数字生态的健康。

因此，新范式必须将“集体数字福祉”与“生态系统健康”提升为核心目标。这要求我们不仅保护个体不受侵害，更要主动塑造一个公平、可信、可持续的数据生态。这意味着承认健康数据具有公共物品属性，其治理需考虑正负外部性。例如，一个开放、高质量的数字人体模型库能加速全球医学研究（正外部性），而一个封闭、有偏的诊断算法则可能损害特定社群健康并加剧社会不公（负外部性）。治理的任务，就是通过制度设计，最大化正外部性，内化负外部性，确保元宇宙健康这一“数字公地”不被过度掠夺或污染，最终服务于人类整体的健康福祉。

需要强调的是，集体数字福祉的构建并非以牺牲个体自主为代价，而是要求个体在数字生态中扮演更积极的“公民”角色。集体福祉的实现，离不开每一个体对自身数据权利的理性行使和对公共数据治理的参与。这意味着，在保护个体隐私的同时，还需培育个体的“数字健康素养”，使其理解数据的价值与风险，知晓如何授权、撤回、审计自身数据的使用，并有能力参与数据信托等集体治理机构的决策。国际研究表明，提升数字健康素养对于改善健康结果、弥合数字鸿沟、减少健康不平等具有显著潜力[45]。个体不再是孤立的“数据所有者”，而是数字共同体中负有责任与权利的成员。只有当个体的能动性与集体制度形成良性互动，新范式才能避免滑向精英治理或技术寡头统治。

上述两大核心理念为治理框架提供了价值指引，它们需要落地为微观、中观、宏观3个层面的具体制度安排。图1展示了新范式的核心逻辑：两大核心理念（数据关系权/数据管理权、集体数字福祉与生态系统健康）作为价值指引，贯穿并指导微观（技术）、中观（制度）、宏观（法律）3个层次的治理框架设计。每个层次对应具体的治理工具，形成理念引领、多层联动、工具协同的治理生态系统。微观技术层通过默认隐私保护、互操作标准和可解释算法，将伦理嵌入系统架构，回应数据液态化的“无界复制”风险；中观制度层通过数据信托、数字公地和参与式审计，创建新型治理主体和制衡机制，直接制衡平台的再疆域化权力；宏观法律层通过数字人格权确权、数字守门人监管和全球标准协作，提供制度保障和底线约束，为数据流动划定制度边界。

5.2　构建韧性协同治理生态系统的多层次治理框架要素

基于上述理念，新范式的实践需要构建一个微观、中观、宏观3层联动，技术、制度、法律与文化多要素协同的治理生态系统。本节提出的三层治理框架，正是对第四章“国家—市场—社会”三元转型方向的具体化：宏观法律层对应国家作为“元治理者”的角色，微观技术层对应市场作为“负责任创新主体”的要求，中观制度层则为社会力量的积极参与提供了制度化渠道。

5.2.1　微观（技术层）嵌入伦理的架构与开放的标准

技术架构是治理的“地基”。必须在元宇宙健康系统的设计源头，贯彻“通过设计保障伦理”的原则。

（1）默认隐私保护与数据最小化架构。系统应默认以最高隐私规格运行，例如，在设备端或边缘计算节点完成初步数据处理，仅上传必要的、脱敏的聚合信息；采用联邦学习、同态加密等隐私增强计算作为默认选项，而非事后附加。

（2）强制性互操作性与开放标准。为打破“数字围栏”，必须通过法规或产业共识，强制核心健康数据接口和虚拟环境组件遵循开放标准。这类似于互联网的TCP/IP协议，允许用户在符合安全规范的前提下，将其健康数据与数字身份在不同平台间迁移，促进竞争与创新。

互操作性标准已在健康数据交换领域取得实质性进展。国际组织HL7开发的FHIR（Fast Healthcare Interoperability Resources）标准已成为全球健康数据互操作的事实基准，支持临床数据、公共卫生报告、保险理赔等多场景的数据交换。欧盟2025年启动的“i2X项目”致力于在12个成员国推广欧洲电子健康记录交换格式（EEHRxF），通过35个试点项目覆盖电子处方、实验室结果、患者摘要、医学影像等五大领域，首次实现欧洲范围内电子健康记录系统的互联互通。

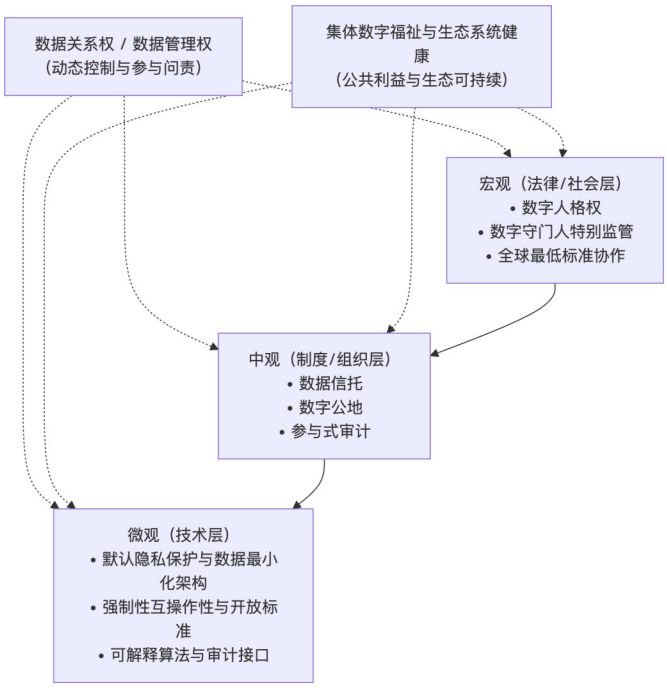

图1 元宇宙健康数据治理新范式：从核心理念到多层次治理框架

与此同时，德国“健康数据实验室”（Health Data Lab）已向研究人员提供覆盖该国90%参保人口（约7500万人）的假名化健康数据，依托联邦学习架构在保障隐私的前提下促进医学研究。这些标准化和数据空间的实践，为元宇宙场景下打破“数字围栏”提供了技术可行性和政策示范。

（3）可解释算法与审计接口。所有用于健康诊断、风险评估的算法，必须内置可解释性模块，并能提供标准化的审计接口，供独立的第三方机构进行黑箱或白箱测试。

5.2.2 中观（制度/组织层）创新治理主体与参与式制衡 这是新范式最具创新性的层面，旨在创建介于国家与个人之间的新型治理主体。辛苑、田新民的研究指出，第三方数据信托通过构建法定信义义务框架规范数据共享行为，依托信托财产独立性原则与权能分割机制重塑数据利益格局，在规范层面构建差异性授权与动态监管的弹性规制体系，在经济层面通过资产隔离与收益结构化设计降低数据交易成本[46]。

（1）数据信托。这是管理集体健康数据的理想制度工具，由一个独立、专业的受托人机构（如由法律、医学、伦理专家及社群代表组成的董事会）代表特定社群（如某疾病患者群体）的利益，统一管理其成员自愿托管的健康数据。信托根据预设的章程（如仅用于非营利的医学研究）与数据使用者谈判、签订合约、监督执行并分配收益。它解决了个人谈判力量薄弱、无力管理复杂数据授权的问题，将分散的数据主权聚合为有效的治理权力。

数据信托并非纯粹的学术构想，已出现值得关注的早期探索。英国开放数据研究所（Open Data Institute，ODI）与政府人工智能办公室于2019年联合发起数据信托试点项目，探索其在减少食物浪费、打击野生动物非法贸易、改善公共服务等领域的应用。研究结论表明，数据信托能够赋予个体和小型组织比传统数据关系中更大的“话语权”，尤其是在数据涉及自身或数据使用影响自身利益时。尽管这些早期试点尚未深入医疗领域，但其验证的治理原则，独立受托、章程约束、多方参与，为医疗健康数据信托的构建提供了宝贵经验。目前，欧盟《健康数据空间条例》（EHDS）的推进，正催生更多成员国探索患者数据集体管理的制度创新。

数据信托的成功运作离不开个体成员的积极参与。首先，信托的章程和重大决策（如接纳新类型的数据使用者、修改收益分配规则）应设置成员民主表决机制，确保个体意愿得以表达。其次，信托需建立透明的信息披露平台，使成员能实时查看自身数据的被访问记录、用途及产生的收益，强化“持续管理权”。最后，信托应承担“数字健康素养”培育功能，通过培训、指南等方式帮助成员理解数据信托的运作逻辑，提升其参与决策的能力，避免

因专业知识不足而使信托沦为少数精英的“代理机构”。

在制度设计细节上，数据信托的运作需明确以下关键问题。一是受托人构成，应由法律专家、医学伦理专家、技术专家和社群代表共同组成董事会，其中社群代表比例不低于1/3，这一比例借鉴了公司治理中独立董事的制度经验，旨在确保数据主体在决策层拥有实质性话语权，避免信托被专家精英主导。二是决策机制，重大事项（如接纳新类型的数据使用者）需经董事会2/3多数通过，并需向全体成员公示。三是收益分配，数据使用产生的经济收益，扣除信托运营成本后，应按照“贡献度”原则分配，贡献度可由数据被调用的频次、数据质量等指标综合计算[47]。李智、王苗苗的研究进一步指出，个人数据信托可在数据收集和流转阶段对数据资源与数据产品作出区分，厘清各阶段数据增值的劳动贡献，对个人数据的收益作出“事先协商+法定补充”的复合型分配设计，并以证券化的方式助力数据要素从资源到资产的实现[48]。关于贡献度的具体计算，可借鉴合作博弈中的Shapley值方法，或基于数据稀缺性、准确性、完整性等维度的综合评价体系，这需要后续研究进一步细化[49]。四是监督机制，信托运作应接受独立第三方审计，审计报告向成员公开。

（2）数字公地。对于具有重大公共价值的基础性健康数据资源，如经过匿名化处理的全民健康数据统计库、开源的数字孪生器官模型等，应确立其“数字公地”地位。由一个多元利益相关者委员会（包括政府、学界、产业界、公众代表）共同制定使用规则，确保其在严格保护隐私的前提下，向符合公共利益的研发活动平等、低成本开放，防止其被私有化垄断。

在制度设计细节上，数字公地的治理可借鉴Ostrom的八项原则：①清晰界定边界（哪些数据属于公地）；②使用规则与当地条件相适应（如不同疾病的匿名数据可有不同访问权限）；③集体选择安排（使用者参与规则制定）；④监督机制（对数据滥用行为的监督）；⑤分级制裁（根据违规程度设置不同处罚）；⑥冲突解决机制（设立申诉渠道）；⑦对组织权的认可（公地治理机构的合法性）；⑧嵌套式企业（多层治理机构之间的协调）。

（3）参与式审计与算法影响评估。建立制度化的公众参与渠道。在算法部署前，强制进行有社群代表参与的“算法影响评估”，预测其对不同群体可能造成的公平性、隐私性影响。在运行中，定期由公民陪审团、倡导组织或专业审计机构对关键算法进行“参与式审计”，审查其输入数据、逻辑与输出结果是否存在偏见。这使技术问责从封闭的专家评议走向开放的社会监督。

算法影响评估已在部分国家获得制度化实践。加拿大政府于2019年生效的《自动化决策指令》要求所有联邦机构在部署自动化决策系统前，必须完成“算法影响评估工具”（Algorithmic Impact Assessment，AIA）的问卷测评，以识别风险等级并采取相应缓解措施。该工具涵盖系统影响范围、数据来源、决策可逆性、公平性考量等多个维度，成为全球首个将算法影响评估纳入法定程序的先例。在欧盟层面，2024年生效的《人工智能法案》将情感识别、生物特征分类等系统列为高风险，要求部署前进行符合性评估，并正在制定关于AI透明度义务的实施指南与实践准则。这些制度实践为元宇宙医疗中的算法审计提供了可借鉴的方法论框架。

5.2.3　宏观（社会/法律层）重塑法律根基与全球协作　微观与中观的创新需要宏观法律与社会共识的支撑与引领。

（1）确立“数字人格权”的法律地位。应在民法典或专门数字法典中，承认自然人在数字环境中享有与其生物人格不可分割的“数字人格权”。

这一权利与传统隐私权、个人信息权存在根本区别。隐私权侧重防范私生活被侵扰，个人信息权聚焦于信息处理过程中的控制与透明，而数字人格权则直接指向数字空间中“人”的完整性、自主性与尊严[1]。其内涵至少包括三个维度：其一，对生物识别数据（如脑电波、步态、心率变异性）的自主控制，防止其被用于身份伪造或行为操纵；其二，对“数字化身”（Avatar）完整性与尊严的保护，禁止对他人的数字孪生体进行扭曲、侮辱或未经授权的商业化利用（例如将患者的虚拟形象用于广告）；其三，对AI生成或篡改健康数据的防御权，当深度伪造技术可能生成虚假的医疗记录或诊疗影像时，数字人格权赋予个体要求验证数据来源、更正错误信息、删除伪造内容的权利。这为应对元宇宙中“身份混淆”“数据污染”“算法操纵”等新型风险提供了法律根基。

在权利具体化方面，数字人格权在立法层面需明确以下权能：①访问权，有权了解自身哪些数据被采集、存储于何处、用于何种目的；②更正权，有权要求更正错误的数字身份信息；③删除权，有权要求删除非必要的数字痕迹；④可携带权，有权将自身数字人格数据在不同平台间转移；⑤反对权，

有权反对将其数字人格用于商业目的(如广告投放);⑥继承权,数字人格在主体去世后的处理方式。关于继承问题,可借鉴《民法典》对死者人格利益保护的规定,探索“近亲属同意+死者生前意愿优先”的处理模式,在尊重死者生前意愿与保护近亲属情感利益之间寻求平衡。

(2)对垄断平台实施“数字守门人”特别监管与公共效用监管。借鉴欧盟《数字市场法》思路,将掌控元宇宙核心基础设施与数据的超大型平台认定为“数字守门人”,对其施加特别义务:包括强制数据互操作、禁止自我优待、开放核心服务接口等。同时,鉴于健康数据的极端敏感性,可考虑对其实施类似公用事业的“公共效用监管”,要求其以合理、无歧视的条件提供基础性健康数据服务,并接受在价格、数据访问权等方面的更严格监管。

(3)推动全球治理的最低标准协作。健康无国界,数据流动亦无国界。应通过世界卫生组织、经济合作与发展组织等平台,推动形成全球性的“元宇宙健康数据治理最低标准”,在个人同意、数据安全、算法公平、跨境传输等核心议题上达成基本共识。这并非追求统一法,而是建立一种基于“共同但有区别责任”的协作框架,防止“监管洼地”的出现导致全球健康风险。

5.3 *新范式下从分野到共生的学科角色重构* 这一跨学科范式的成功,最终依赖于计算机科学与社会科学的角色从分离走向深度共生。跨学科研究强调,应对数字技术的复杂社会挑战需要超越单一学科视角,通过整合不同科学视角的见解来培养新一代公共部门专业人员[50]。

计算机科学家需要从纯工具构建者转向具备社会视野的系统架构师。他们不能仅满足于实现功能与提升效率,而必须将公平、问责、透明、隐私等社会价值作为核心设计约束。这意味着需要学习基本的伦理与法律框架,在系统设计之初就与社会科学者合作,思考技术选择可能引发的社会后果,并主动将治理逻辑(如可审计性、可解释性)编码到系统架构之中。

社会科学家需要从外部批判者转向共同设计者与效果评估者。他们需要超越事后的理论批判,更早、更深入地介入技术生命周期。作为“共同设计者”,他们应参与制定技术需求、设计用户研究、共同草拟治理章程;作为“效果评估者”,他们应主导算法影响评估和社会接受度研究,运用定性与定量方法,持续监测和评估技术部署后的真实社会影响,为迭代优化提供证据。

这种角色重构的目标,是培育一批真正的“跨学科桥梁人才”,他们能够理解技术的逻辑与社会的复杂,从而在元宇宙这片新疆域上,共同设计出既能释放巨大技术潜力,又能坚守人类尊严与公正的治理体系。这不仅是应对健康数据挑战的必需,更是为一个日益深度数字化的社会培育跨学科治理能力的重要基础。

6 结 论

元宇宙的兴起,标志着人类交互与认知正经历一场从物理原子世界向数字比特世界的深刻迁徙。在这一迁徙中,医疗健康,这一最关乎人类本体安全与尊严的领域,也无可避免地迈入虚拟与现实交织的新边疆。然而,本研究的核心论点是:这一技术跃迁所带来的,远不止于诊疗效率的提升或服务形式的创新,它更引发了一场关于生命数据控制权的根本性治理危机。本文通过层层剖析,旨在揭示这场危机的本质,批判应对方案的局限,并最终指向一个更具韧性、公平与智慧的治理未来。

6.1 *研究总结* 本研究始于一个核心观察:元宇宙中的健康数据,其性质已从传统的结构化、离散化记录,嬗变为连续、多模态、高维的情景化“数字生命流”。这一本体论层面的根本性变革,使得奠基于工业时代与早期互联网思维的治理范式陷入系统性失效。

本文识别并论证了构成这场危机内核的“双重运动”:一方面是数据的液态化,即数据以前所未有的速度和规模挣脱传统的制度与物理边界,无界复制、聚合重组、目的漂移,导致个体知情同意与隐私边界趋于崩塌;另一方面则是资本的再疆域化,即大型平台凭借技术架构、协议标准与市场权力,对流动的数据流进行捕获、圈占与定价,构建起封闭的“数字围栏”,形成了健康数据生态的私有化与新型“技术封建”关系,平台与用户形成的依附性权力结构[18]。这两股力量并非对立,而是辩证统一:液态化为再疆域化提供了掠夺的原料,而再疆域化则试图为无序的流动赋予私有化的秩序,其结果是个体自主权遭受双重侵蚀,集体福祉面临系统性风险。

面对这一困境,当前的应对方案呈现出显著的局限性。以联邦学习、区块链、零知识证明、可信执行环境为代表的技术乐观主义回应,虽在工具层面提供了隐私保护和权属追溯的精致方案,但其“去中心化”承诺在权力维度沦为技术专家垄断或硬件巨头掌控的幻象(ZKP的可信初始化由少数精英主

导，TEE的硬件层被芯片寡头垄断）；在公平维度因高昂算力成本与认知门槛制造新的“隐私税”，将弱势群体排斥在外；在价值维度以“代码即法律”的逻辑替代必要的社会价值商谈，导致规则刚性无法应对伦理复杂性；在责任维度引发责任主体模糊化的“问责黑洞”，使受害者难以寻求救济；在主权维度则因硬件层垄断引发供应链依附风险，形成从软件到硬件的“双重殖民”[9]。同时，以GDPR为代表的法律监管模式在应对海量情景化数据时显露出原则滞后、权利行使困难、合规成本高企反而巩固大平台垄断的“合规悖论”；而依赖市场自我调节的逻辑，则必然走向数据垄断与商品化，其负外部性（公共利益受损、健康不平等、人的主体性侵蚀）无法通过市场机制内部化。

6.2　主要贡献　本研究的主要贡献在于，超越了对元宇宙健康数据风险的现象描述或单一学科的技术性回应，提供了一个融合技术批判与政治经济分析的综合性理论框架。

（1）理论框架的建构。本文将齐格蒙特·鲍曼的“液态现代性”理论与“数据殖民主义”“平台资本主义”“技术封建主义”等批判政治经济学视角相结合，创造性地提出了“液态化”与“再疆域化”这一对核心分析透镜。相较于“平台资本主义”聚焦于平台作为新的商业模式、“监控资本主义”关注行为数据的剩余价值剥削，这一框架揭示了更根本的结构性转变：数据的存在方式本身正在从“固态”变为“液态”，而平台的权力运作也从“占有”转向“组织流动”。这一框架不仅深刻揭示了元宇宙健康数据动态的本质矛盾，流动与控制的辩证共生，也为理解更广泛的数字时代资源与权力重组提供了有力的分析工具。

（2）跨学科的深度批判。研究对主流技术方案进行了超越工程学视角的社会科学批判，揭示了技术治理在权力、公平、价值、责任、主权五个维度的内在限度，从软件层的密码学协议（ZKP的可信初始化）到硬件层的可信执行环境（芯片寡头垄断、供应链主权侵蚀），技术方案以其独特的方式复制乃至深化了权力集中的悖论。同时，对法律与市场治理模式的困境分析，指出了单纯依靠国家管控或市场自发秩序在应对新型数字社会形态时的结构性缺陷，尤其是法律合规成本意外巩固大平台垄断的“合规悖论”，以及数据商品化对医疗伦理的根本背离。这种多维批判为寻找新路径扫清了认识障碍。

（3）范式转型方向的系统性勾勒。本文最大的建设性贡献在于，明确提出了从旧有范式向“国家—市场—社会”多元协同共治的第三代治理范式转型的必然性，并系统性地构建了一个覆盖理念、技术、制度、法律多层次的治理新蓝图。在理念层面，完成了从“数据所有权”到“数据关系权/数据管理权”、从“个人隐私保护”到“集体数字福祉与生态系统健康”的双重升维；在制度层面，创新性地设计了数据信托、数字公地、参与式审计等中观治理机制，使第四章提出的“国家—市场—社会”三元转型方向得以具体化，并引入英国ODI试点、加拿大算法影响评估工具、FHIR互操作标准等实践案例作为可行性参照；在宏观层面，提出了“数字人格权”的法律确权、数字守门人特别监管、全球最低标准协作等制度构想。这一蓝图为政策制定者、产业实践者与学术界提供了清晰且可行的行动路线图。

（4）学科角色的重构倡议。本文首次在元宇宙健康数据治理语境下，明确提出计算机科学家需从工具构建者转向具备社会视野的系统架构师，社会科学家需从外部批判者转向共同设计者与效果评估者，并倡导培育“跨学科桥梁人才”[50]。这一倡议为治理范式的落地提供了主体性基础。

6.3　研究局限与未来展望　作为一项前瞻性的理论探索，本研究亦存在其局限，这些局限恰恰指明了未来研究富有潜力的方向。本节将从理论、方法与制度3个层面反思研究不足，并在此基础上提出对应的深化路径。

（1）理论层面框架开放性与动态性的局限。元宇宙技术本身仍在快速迭代，人工智能生成内容、脑机接口、空间计算等新技术的融合将不断提出新的伦理与治理挑战。本文提出的“液态化—再疆域化”框架虽力求涵盖从软件层到硬件层的权力结构，但其解释力仍需在技术演进中持续检验与更新。如何在保持框架稳定性的同时赋予其足够的开放性，以容纳未来可能出现的新型数据形态与治理问题，是本研究未能完全解决的难题。

（2）方法层面实证检验缺失的局限。本研究采用理论整合与框架构建的方法，未进行系统的实证检验。这一选择有助于在概念层面构建完整的治理图景，但也使部分论断缺乏经验支撑。例如，5.2.2节提出的数据信托制度设计，其“四要素”机制（受托人构成、决策机制、收益分配、监督机制）的可行性尚需通过试点项目验证；3.2节对技术成本的批判，其具体数值（如ZKP计算开销、TEE硬件适配成本）需结合真实部署环境测算；5.1节提出的“数字健康素养”培育路径，其实际效果有待通过干预研究评估。理论推演固然能够揭示结构性矛盾，但无法

替代经验证据对制度设计的校准作用。

(3)制度层面文化适应性与落地可行性悬置的局限。本文提出的治理范式具有普适性抱负,但具体制度的实践必然受到不同国家和地区文化传统、法律体系、医疗体制与社会结构的深刻影响。例如,“数据信托”的法律主体地位、受托人的权责界定、运作模式等,需要在英美法系与大陆法系的不同语境下进行细致的设计与比较研究;“数字人格权”的确立方式,在大陆法系国家可通过民法典修订,在普通法系国家则可能依赖判例积累;“参与式审计”机制的有效运作,高度依赖公民社会的成熟程度与制度信任基础。本文对这些“地方性知识”的讨论仍停留在原则层面,未能深入不同法域的制度细节。

综上所述,本文的理论建构只是一个起点。真正有效的治理范式,需要在与经验世界的持续对话中接受检验、修正与丰富。唯有理论、方法与制度实践的协同演进,才能在数据的“液态”河流与权力的“固态”围栏之间,开辟出真正可行的第三条道路。

6.4 结语 元宇宙中的健康数据治理,绝非一个单纯的技术管理或法律合规问题。它是一场发生在数字新大陆上的、关于权力、正义与人类尊严的前沿谈判。本文揭示了旧地图无法指引新航路的困境,批判了仅靠修补船帆而非重新设计航向的努力,并尝试绘制一幅需要多元舵手共同协作的新航海图。这幅图景以“数据关系权”与“集体数字福祉”为罗盘,以微观技术嵌入、中观制度创新、宏观法律重塑为三层甲板,以计算机科学家与社会科学家的深度共生为共同划桨者。这幅图景或许尚不完美,但其核心指向是明确的:我们必须在数据的“液态”河流与资本的“固态”围栏之间,开辟第三条道路,一条以数据关系权为基石、以集体数字福祉为指引、以三层治理框架为支撑、以跨学科作为动力的数字健康治理新路。这条道路的开拓,将是技术专家、社会科学家、政策制定者与每一位公民共同承担的、至关重要的时代使命。

伦理声明 无。

利益冲突 所有作者声明不存在利益冲突。

作者贡献 高承实,选题,撰写、修改论文;程元骏:选题,修改论文。

参考文献

[1] Lupton D. The quantified self: a sociology of self-tracking[M]. Cambridge: Polity Press, 2016.

[2] Ruckenstein M, Schüll N D. The datafication of health[J]. Annu Rev Anthropol, 2017, 46: 261-278.

[3] Das B C, Ahmad M, et al. Spatial data governance for healthcare metaverse[M]. Advances in Healthcare Information Systems. Hershey: IGI Global, 2025.

[4] Kostick-Quenet K, Rahimzadeh V. Ethical considerations for health data governance in the metaverse[J]. Journal of Medical Ethics, 2023, 49(2): 87-92.

[5] 何之行, 廖 貞. AI個資爭議在英國與歐盟之經驗:以Google DeepMind一案為例[J]. 月旦法學雜誌, 2020, 302: 127-156.

[6] Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power[M]. New York: PublicAffairs, 2019.

[7] Srnicek N. Platform capitalism[M]. Cambridge: Polity Press, 2017.

[8] Cohen J E. Between truth and power: the legal constructions of informational capitalism[M]. Oxford: Oxford University Press, 2019.

[9] Couldry N, Mejias U A. The costs of connection: how data is colonizing human life and appropriating it for capitalism[M]. Stanford: Stanford University Press, 2019.

[10] Shaw J, Sekalala S. Health data justice: building new norms for health data governance[J]. npj Digital Medicine, 2023, 6(1): 1-4.

[11] Hormazábal C. Bauman Z. (2000). liquid modernity. Cambridge: polity press[J]. Athenea Digit Rev De Pensamiento E Investig Soc, 2001, 1.

[12] Deleuze G, Guattari F. A thousand plateaus: capitalism and schizophrenia[M]. Minneapolis: University of Minnesota Press, 1987.

[13] Van Dijck J, Poell T, De Waal M. The platform society: Public values in a connective world[M]. Oxford: Oxford University Press, 2018.

[14] Gillespie T. The politics of 'platforms'[J]. New Media & Society, 2010, 12(3): 347-364.
Gillespie T. The politics of 'platforms'[J]. New Medium Soc, 2010, 12(3): 347-364.

[15] Couldry N, Hepp A. The mediated construction of reality[M]. Cambridge: Polity Press, 2016.

[16] Van Dijck J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology[J]. Surveillance & Society, 2014, 12(2): 197-208.

[17] Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life[M]. Stanford: Stanford University Press, 2010.

[18] Rikap C. Capitalism as Usual Implications of Digital Intellectual Monopolies[J]. New Left Review, 2023, 139: 145-160.

[19] Gentry C. Fully homomorphic encryption using ideal lattices[C]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 169-178.

[20] Goldwasser S，Micali S，Rackoff C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing，1989，18(1)：186-208.
[21] 李　耕，刘建伟，张宗洋. 大规模监视下安全性定义再分析[J]. 密码学报，2020，7(3)：326-341.
[22] Blum M，Feldman P，Micali S. Non-interactive zero-knowledge and its applications[C]. Proceedings of the 20th Annual ACM Symposium on Theory of Computing. New York：ACM，1988：103-112.
[23] Ben-Sasson E，Chiesa A，Tromer E，et al. Succinct non-interactive zero knowledge for a von Neumann architecture[C]. Proceedings of the 23rd USENIX Security Symposium. Berkeley：USENIX Association，2014：781-796.
[24] Swanson T. Consensus-as-a-service：a brief report on the emergence of permissioned distributed ledger systems[R/OL]. (2015-04-06). https://www. ofnumbers. com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers. pdf.
[25] Costan V，Devadas S. Intel SGX explained[J]. IACR Cryptology ePrint Archive，2016，2016(86)：1-118.
[26] Luevano L S，Frey D. Analyzing trusted execution environments：comparing commercial implementations and diverse applications[R/OL]. HAL Preprint，2024. https://inria. hal. science/hal-04393667.
[27] 冯登国，刘敬彬，秦　宇，等. 创新发展中的可信计算理论与技术[J]. 中国科学：信息科学，2020，50(8)：1127-1147.
[28] 胡　凌. “分享经济”的法律规制[J]. 文化纵横，2015(4)：42-49.
[29] David P A. Clio and the economics of QWERTY[J]. The American Economic Review，1985，75(2)：332-337.
[30] Gao Y，Quan G，Homsi S，et al. Secure and efficient general matrix multiplication on cloud using homomorphic encryption[J]. J Supercomput，2024，80(18)：26394-26434.
[31] Ben-Sasson E，Bentov I，Horesh Y，et al. Scalable，transparent，and post-quantum secure computational integrity[J]. IACR Cryptology ePrint Archive，2018，2018(46)：1-28.
[32] 刘　睿，陈晓峰. 联邦学习安全与隐私保护研究综述[J]. 软件学报，2022，33(3)：924-945.
[33] Lessig L. Code and other laws of cyberspace[M]. New York：Basic Books，1999.
[34] 郑　戈. 算法的法律与法律的算法[J]. 中国法律评论，2018(2)：66-85.
[35] Zhu L，Liu Z，Han S. Deep leakage from gradients[C]. Advances in Neural Information Processing Systems 32. Red Hook：Curran Associates，2019：14774-14784.
[36] Fan M，Wang F，Chen C，Zhou J. Boosting gradient leakage attacks：data reconstruction in realistic FL settings[C]. Proceedings of the 34th USENIX Security Symposium. Berkeley：USENIX Association，2025.（Accepted）arXiv preprint arXiv：2506. 08435，2025.
[37] Solove D J. Introduction：privacy self-management and the consent dilemma[J]. Harvard Law Review，2013，126(7)：1880-1903.
[38] 殷继国. 大数据市场反垄断规制的理论逻辑与基本路径[J]. 政治与法律，2019(10)：134-148.
[39] 袁　康，赵宛如. 跨境数据流动中的管辖权冲突及其协调[J]. 重庆邮电大学学报(社会科学版)，2024(2).
[40] Ostrom E. Governing the commons：the evolution of institutions for collective action[M]. Cambridge：Cambridge University Press，1990.
[41] Obermeyer Z，Powers B，Vogeli C，et al. Dissecting racial bias in an algorithm used to manage the health of populations[J]. Science，2019，366(6464)：447-453.
[42] Jessop B. The rise of governance and the risks of failure：the case of economic development[J]. Int Social Sci J，1998，50(155)：29-45.
[43] 陈　磊，郑　森. 数据信托中"信任"的实现——以自决性个人信息权利的实现与表达为核心[J]. 学术交流，2025(7)：82-95.
[44] 申卫星. 数字权利体系再造：迈向隐私、信息与数据的差序格局[J]. 政法论坛，2022(3)：89-102.
[45] Powell D，Asad L，Zavaglia E，et al. Promoting digital health data literacy：the datum project[J]. JMIR Form Res，2025，9：e60832.
[46] 辛　苑，田新民. 第三方数据信托模式在数据共享中的作用机理与实现路径[J]. 江西社会科学，2025(2).
[47] 邢亚楠，李跃文. 数字经济视域下数据信托参与主体利益分配的合作博弈分析[J]. 时代经贸，2025(11)：177-181.
[48] 李　智，王苗苗. 数据信托：个人数据交易与收益分配实现机制[J]. 学术交流，2025(7)：66-81.
[49] 李　智，张津瑶. 数据信托本土化的现实困境与路径构建[J]. 学术交流，2023(7).
[50] Jabbouri R，Issa H，Dakroub R，et al. Unlocking immersive education：the emergence of the meta-governance framework[J]. Information Technology & People，2025，38(4)：2069-2093.

引用本文

高承实，程元骏. 液态生命与数字围栏：元宇宙健康数据的治理困境与范式重构[J]. 元宇宙医学，2026，3(1)：16-37.

Gao C S，Cheng Y J. Liquid life and digital fence：governance dilemma and paradigm reconstruction of metaverse health data[J]. Metaverse Med，2026，3(1)：16-37.