元宇宙中的用户数据隐私问题

陈　辉　闫佳琦　陈瑞清　沈　阳

（清华大学 新闻与传播学院，北京 100084）

摘　要：元宇宙作为虚实融生的新一代互联网形态，显著改变了用户数据的生产与控制机制，并带来新的用户数据隐私问题。一是如何克服中心化控制机制导致的用户数据所有权被架空与收益权旁落，以及元架构公司侵犯用户智识隐私可能引发的情感与决策操纵。二是去中心化控制机制下，如何化解区块链的透明性与用户隐私数据保护之间的矛盾。文本提出从用户个体与元宇宙经济生产关系变革两个层面回应上述挑战，用户个体层面：一方面，从以结果为导向的监管转向程序性监管，通过用户隐私协议格式、内容与更新的监管备案，增强元宇宙企业事前隐私合规动力；另一方面，引入基于智能合约的用户数据隐私安全参数保险，完善面向用户的隐私风险事后补偿机制。元宇宙经济生产关系层面：经由“数据作为劳动”的认知与生产关系变革，分析元宇宙企业为用户数据工作付酬的伦理、经济与技术价值，并为从操作层面探索用户数据定价机制提供可能方向。在此基础上，提出元宇宙用户智识隐私保护的可行路径。

关键词：元宇宙；数据隐私；智识隐私；用户

中图分类号：G20　　**文献标识码：**A　　**文章编号：**1005-9245（2022）05-0112-09

DOI:10.14100/j.cnki.65-1039/g4.20220412.001

一、引　言

美国科幻小说家戴夫·艾格斯（Dave Eggers）认为，信息传播技术的发展会压缩人们的隐私空间、重塑人们的隐私观念，并在小说《圆圈》一书中构建了一个零隐私的世界，将这一认知推向极致。在该小说中，互联网公司Circle（圆圈）开发了一套一体化的“真你”（TruYou）操作系统，用一个账号将用户的个人邮件、社交媒体、银行业务和购物信息连接起来，进而形成一个完全透明的新世界。Circle创始人主张消除秘密和隐私，提倡毫无保留的分享，并将这一理念转化为该公司的口号：“秘密即谎言，分享即关怀，隐私即偷窃。”[①] 其背后的思考路径是：当所有的用户都可以查阅彼此的全部数据时，用户之间会形成新的权利平衡。

《圆圈》一书以极致化的想象力引发人们思考人与技术、用户与平台之间日渐失衡的关系。元宇宙的到来是否会使小说中描绘的零隐私世界变成现实？毕竟元宇宙作为虚实融生的新一代互联网形态，需要对用户的指纹、声纹、面部轮廓以及肌电信号、脑波模式等生物特征数据，工作、教育、社交、娱乐等场景行为数据，以及电子支付、生产要素等财产数据进行细颗粒度挖掘和实时同步，以支撑自身持续运作。这为各类商业力量持续收集和挖掘用户数据提供了新的场景和契机，同时，也为社会治理者追踪和识别用户以加强对新一代互联网的管理提出挑战。这里的挑战不同于赛博空间初期的用户高度匿名，而是当赛博空间用户数据极大

收稿日期：2022-02-28

基金项目：本文系国家社会科学基金青年项目“中国互联网信息服务的分类与多元协同治理模式研究”（18CZZ035）的阶段性成果。

作者简介：陈辉，清华大学新闻与传播学院博士后；闫佳琦，清华大学新闻与传播学院博士研究生；陈瑞清，清华大学新闻与传播学院硕士研究生；通讯作者：沈阳，清华大学新闻与传播学院教授、博士生导师。

① D.Eggers.The Circle，New York：Knopf，2013.

丰富之后，政治力量如何在网络治理、产业发展与用户权益保护等多重目标约束之下重新确立规则、维护秩序。

目前，国内尚无系统讨论元宇宙数据隐私话题的研究文献。与此话题间接相关的研究呈现两条脉络：一是聚焦个体层面或区块链等特定技术场景的数据隐私挑战分析及应对。例如，有研究者提出应对个人隐私数据按价值和敏感程度分类，在数据生命周期的不同阶段，采取差异化的保护策略[①]。还有研究者从区块链结构和隐私内容出发，对链上数据隐私威胁展开分析，并提出相应的技术解决方案[②③]；二是在数字经济或公共治理等广阔语境下理解与回应数据隐私挑战。戴昕认为，讨论数据隐私问题，应更加注重从实践层面回应数字经济和技术发展带来的数据隐私挑战[④]。季卫东认为,隐私保护与人工智能技术发展不可偏废，应将集权式人工智能算法与分权式区块链协议相结合，进行合理的社会治理机制设计[⑤]。

国外与元宇宙数据隐私相关的研究，主要集中在两个领域：一是社交元宇宙对用户数据隐私的挑战。利恩斯（Ronald Leenes）以聚合游戏与社交服务的“第二人生”为例，讨论了元宇宙中的隐私规制问题[⑥]。还有研究者将社交元宇宙中的用户数据隐私分为个人信息隐私、行为隐私和交流隐私，认为社会元宇宙中的隐私风险主要来自游戏及社交中的骚扰、社会工程学攻击和恶意社交机器人[⑦]。用户可以通过创建多个化身、创建独家使用的公共空间副本，以及对其他用户隐身等方式进行隐私风险管理；二是增强现实 / 混合现实（AR/MR）等元宇宙前端设备在用户数据采集、使用等环节的隐私风险分析。AR 等前端设备的隐私风险可分为用户隐私风险[⑧]和旁观者隐私风险[⑨]。前者主要涉及 AR/MR 系统采集和存储用户的动作数据、生物特征数据以及空间环境数据引发的隐私风险；后者涉及环境中的旁观者在不知情的情况下被 AR/MR 设备采集并存储相关信息。因此，有研究者提出，AR/MR 系统中保护用户隐私的关键是要确保数据的保密性、匿名性、隐蔽性和无关联性[⑩]。

总体而言，既有研究一方面为讨论元宇宙用户数据隐私问题提供了丰富的路径启发，例如，法律经济学视角的独特价值、隐私保护与产业发展之间的平衡、数据隐私保护领域新的技术实现机制，等等；另一方面，提供了丰富的微观研究案例和基于特定技术情境的数据隐私风险分析启示。但既有研究仍存在一定不足：一是缺乏对元宇宙经济背后的数据生产与控制的系统性思考，以及对元宇宙中用户数据隐私挑战的整体观照；二是忽视了元宇宙中用户数据隐私话题的重要面向——智识隐私问题[⑪]，即元宇宙语境下元架构企业利用自身平台和数据优势，监控用户的阅读、思考和创作等智识活动的数字踪迹而引发隐私侵权问题。

本文中的用户数据指能关联到已识别或可识别的自然人的电子信息，与之相对应的用户数据隐私问题指由公共或商业服务提供者“利用信息技术收集、存储、传输、分析用户个人信息的实践而引发的政治、经济、法律乃至伦理问题”[⑫]。因此，本文旨在探讨与移动互联网相比，元宇宙中个体数据的生产与控制机制会发生何种变化？这些变化如何影响用户数据隐私保护？如何看待用户数据隐私保护与元宇宙新技术新业态发展之间的关系？

① 祝阳、李欣恬:《大数据时代个人数据隐私安全保护的一个分析框架》,《情报杂志》, 2021 年第 1 期。

② 祝烈煌、高峰、沈蒙等:《区块链隐私保护研究综述》,《计算机研究与发展》, 2017 年第 10 期。

③ 王晨旭、程加成、桑新欣等:《区块链数据隐私保护：研究现状与展望》,《计算机研究与发展》, 2021 年第 10 期。

④⑫ 戴昕:《数据隐私问题的维度扩展与议题转换：法律经济学视角》,《交大法学》, 2019 年第 1 期。

⑤ 季卫东:《数据、隐私以及人工智能时代的宪法创新》,《南大法学》, 2020 年第 1 期。

⑥ R.Leenes.Privacy regulation in the metaverse,In Handbook of research on socio-technical design and social networking systems,IGI Global, 2009：123-136.

⑦ B.Falchuk,S.Loeb,R.Neff.The social metaverse：Battle for privacy,Technology and Society Magazine, 2018（2）.

⑧ K.Lebeck,K.Ruth,T.Kohno,et al.Towards security and privacy for multi-user augmented reality：Foundations with end users,Symposium on Security and Privacy（SP）, 2018：392-408.

⑨ F.Roesner,T.Kohno,D.Molnar.Security and privacy for augmented reality systems,Communications of the ACM, 2014（4）.

⑩ J.A.De Guzman,K.Thilakarathna,et al.Security and privacy approaches in mixed reality：A literature survey,ACM Computing Surveys（CSUR）, 2019（6）.

⑪ N.Richard.Intellectual privacy：Rethinking civil liberties in the digital age,Oxford University Press, 2015：95.

二、元宇宙中用户数据的生产与控制

赛博空间中的用户数据不仅是一种个体化的数字踪迹，还是一种生产资源。对商业机构而言，吸引用户在自己的平台进行数据生产，并建立一套常态化的控制机制确保这一过程持续稳定运行，是实现自身商业利益的前提。这一机制在移动互联网中已趋于成熟，并由此诞生诸多互联网科技巨头，几乎垄断了人们线上线下日常生活的所有入口，成为社会生活中不可或缺的数字基础设施。

移动互联网中用户数据的生产与控制机制，包括账号、数据和声誉评价[①]三个关键要素。账号是用户从现实世界进入虚拟世界的入口，也是用户数据历时性积累的载体。数据主要包含四个层次：一是用户的身份认证数据；二是用户在各平台前台生产的内容数据；三是平台自动记录的用户后台行为数据；四是根据前台内容数据和后台行为数据进行深度挖掘后产生的衍生数据，例如，平台基于各类算法生成的用户分类和标签数据。声誉评价是虚拟空间中的重要约束机制，用以规范和引导虚拟空间用户行为，激励合规用户，淘汰违规用户。

与移动互联网相比，元宇宙中用户个体数据化的方式及其控制机制发生了若干变化。一是以账号为核心的身份控制机制，由原来单一的中心化平台控制转向中心化与去中心化控制机制并存。移动互联网中，用户以账号为核心的数字身份，是在互联网科技巨头控制的中心化技术架构上创建的。因此，互联网科技巨头对基于平台架构产生的用户数据，拥有高度控制权，用户在由此产生的收益分配中被边缘化。元宇宙的到来，催生了一批元架构公司，同时推动传统科技巨头向元架构公司转型，他们如同元宇宙中的元房间。在元架构公司中，中心化的身份控制机制虽然得以延续，但用户可以获得更大的内容生产与收益分配权限。以游戏公司罗布乐思（Roblox）为例，其与传统游戏公司的不同之处在于，其只是一家元游戏公司，本身不面向用户提供游戏产品，仅提供开发架构。用户可以在其提供的架构基础上开发各类游戏及周边产品，并吸引其他用户成为玩家。用户作为游戏开发者，在自身内容数据和收益分配方面享有更大的话语权。随着元宇宙中互操作技术的进一步成熟，用户可以在不同的元架构公司之间实现数据及其价值的自由转移。

与此同时，区块链技术的引入为元宇宙带来新的去中心化身份（DID）控制机制。作为元宇宙实现形态之一的 Web3.0，描绘了用户摆脱科技巨头对自身账号数据掌控的技术实现机制，用户将真正获得自身数据的所有权和收益权。以区块链游戏公司加密猫（CryptoKitties）为例，游戏中的每一只宠物猫都须经过区块链验证，用户购买即享有独占权，在不经用户允许的情况下，即使是游戏开发商也无法变更其所有权。一旦不同区块链之间以及链上链下互操作技术发展成熟，经由一个账号连接社交、购物、娱乐的多场景线上生活的愿景将变为现实。

二是用户数据维度更加多元。相较于移动互联网，元宇宙中用户数据的维度在三个方面发生变化。首先，用户数据的时间维度与空间维度得到拓展。元宇宙中用户数据具有时间性，一方面，用户数据的历时性累积，构成其声誉评价和后续行为预测的重要面向；另一方面，通过引入时间戳，对用户数据产生的时间进行验证，为数据打上时间标签，在此过程中，数据的时间序列得到强调，成为标定数据安全性的判断标准之一。元宇宙中用户数据的空间性增强，三维化生产和存储日益成为主流。用户身份数据和用户面向前台生产的内容数据，都将借助数字孪生和虚拟仿真技术实现三维化。这在提升元宇宙用户沉浸感的同时，也引发了新的空间隐私问题。其次，用户数据的人机融合性得到提升。元宇宙用户数据的生产，离不开扩展现实（XR）等元宇宙前端设备的支持。借助一系列运动追踪和感知交互技术，用户的声音、动作、眼动、肌电等生物特征数据和环境数据被前端设备捕捉和留存[②]，并由此生成与元宇宙中用户身份形象、前台场景的沉浸交互。最后，用户数据的资产属性更加凸显、交易机制更加完善。元宇宙为各种场景的用户内容生产提供技术实现工具、搭建开放协作机制，以及基于区块链的数据所有权认证体系与交易机制，推动元宇宙中用户数据资产化。

三是中心化与去中心化的声誉评价机制并存。一系列元架构公司的存在，将使中心化元宇宙与去中心化元宇宙在较长一段时间内并存，进而决定了移动互联网语境下的中心化声誉评价机制将在元宇宙中得以延续。在中心化声誉评价机制下，元宇宙

① X.Dai.Toward a reputation state：The social credit system project of China，Available at SSRN 3193577，2018.

② Supplemental Oculus Data Policy，https://www.oculus.com/legal/privacy-policy/.

中的用户行为仍将受到来自平台的中心化规范，相应地用户数据的控制权与收益权也将受到平台的制约。与此同时，在 Web3.0 中，依托区块链技术正在孕育和形成新的去中心化声誉评价机制。这里的去中心化是指传统互联网科技巨头不再强势主导用户个人数据采集、存储、传输、分析等过程，去中心化自治组织（DAOs）或专门的用户数据服务公司将接替其角色。二者的区别在于，用户不再仅是名义上拥有自身数据，而是通过相应的技术实现机制和治理机制真正获得自身数据的所有权和处置权。用户个人数据资产化的天平进一步从平台向个人倾斜。具体而言，在去中心化声誉评价机制下，用户的自我量化趋势将进一步深化，其在区块链上积累的生物特征数据、交易记录和行为数据等将被充分挖掘，进而生成用户声誉凭证。元宇宙中的用户声誉评价体系类似于生命日志（Lifelogging），不仅记录用户在元宇宙中的所有行为，还包括一个人的成就、贡献、兴趣和活动等生活记录[①]。

三、元宇宙与用户数据隐私面临的挑战

信息技术的不断发展，使数据与隐私这对充满张力的概念组合在一起。一般而言，数据化是隐私的天敌，隐私信息一旦数据化，其出现在公共领域可能只是时间早晚的问题。任何一条信息，一旦进入互联网，就应默认其会永远存在，因为目前尚未出现可以彻底撤回或销毁信息的方法。这一认知，应该成为人类面对当下和未来数字生活的默认心理设置。信息技术发展已成不可逆转之势，人们只有调整自身的隐私观念，以适应新的“技术—社会”情境。在互联网早期阶段，在网络上发布某人的照片，会被认为侵犯其隐私。但是，当网络相册（Flickr）和照片墙（Instagram）等图片类社交网络兴起之后，人们在照片中被标记，也不会认为自己的隐私被侵犯。这背后的实质原因是 Web2.0 架构提供的用户数据生产方式，悄然改变了人们的隐私观念，即从空间范式的隐私观转向控制范式的隐私观。

移动互联网兴起后，大量生活方式类公司嵌入并重塑人们的日常生活。这类公司的运作需要海量用户隐私数据作为支撑，由此，人们的身份信息、家庭住址、联系方式、实时位置等个人隐私信息变得数据化。更为关键的是，用户衣食住行等日常生活的数字化，导致其在各大生活方式类平台存留大量数字踪迹。这些行为记录与特定身份信息相结合，在大数据计算的加持下，不仅可以识别出特定的自然人，还能精确勾画特定人群或个人的生活轨迹乃至生活习惯。换言之，用户在互联网科技巨头面前，几乎毫无隐私可言。一个人如果想保有个体生活的隐私而完全不接触、不使用这些生活方式类平台，他将成为当代数字生活的“边缘人”或“流放者”。

控制范式的隐私观成为数字生活语境下的默认设置，即商业机构在收集和使用个人数据时，须获得用户许可，即知情同意。用户在参与数据流动的过程中，需要动态地维护自身的数据隐私权益。为加强用户对自身数据的控制权，欧盟颁布施行的《通用数据保护条例》赋予用户知情权、访问权、更正权、删除权、限制处理权、可携带权、反对权、反自动化决策权等八项权利[②]。即便如此，仍无法改变用户在面对互联网科技巨头时的弱势地位。作为平台方的企业认为，经过收集、加工等形成的用户数据集，体现的是用户与企业双方的共同劳动。此外，经过平台算法挖掘和分析后形成的数据集，可以提高经济运作效率，提升社会整体福利。因此，企业主张对用户数据集的排他性权属[③]。企业通过的一系列专业复杂的数据授权协议，形式上是对用户数据所有权的承认，实质上却获得了用户数据及其衍生数据的永久使用权和收益权。如此，用户对自身数据的所有权在事实上被架空，所谓的尊重用户数据隐私，更多沦为一种话术包装。

相较于移动互联网，元宇宙的运作对用户个人数据的需求，在数据种类、维度和深度等方面都更进一步。元宇宙承诺的是一个虚拟与现实深度交融映射又随时切换的三维世界。面向用户的元宇宙场景，在传统二维数据的基础上，还需要全身型虚拟化身、全身实时动作捕捉、周围空间环境实时重建等三维数据采集和加工。如果说移动互联网让用户

① J.Smart，J.Cascio，J.Paffendorf.Metaverse roadmap overview，Pathways to the 3d web，https://www.metaverseroadmap.org/overview/.

② General Data Protection Regulation（GDPR），Chapter 3，Rights of the data subject，https://gdpr-info.eu/chapter-3/.

③ 许可:《数据保护的三重进路——评新浪微博诉脉脉不正当竞争案》,《上海大学学报（社会科学版）》, 2017年第6期。

交出自身的发型、服饰、口味等生活方式类数据和指纹、声纹、面部轮廓等生物特征数据，那么，元宇宙则在此基础上，将数据边界进一步向用户身体内部推进，诱使用户交出眼球运动、肌电信号、脑电波、基因构成等深度生物隐私数据，试图将人机交互机制一步到位地建立在解剖学基础之上。在众多元宇宙游戏、音乐、电影等内容消费场景中，扩展现实技术和脑机接口技术将以提升用户体验的名义，大量采集用户脑电波与其他神经元活动数据。上述种种，都对元宇宙中的用户数据隐私保护提出挑战。

从用户数据控制机制看，挑战表现在两个方面。一是老问题：由传统互联网科技巨头转型而来的中心化元架构公司，他们依然是元宇宙中的关键玩家和重要服务提供商。面对这些元架构公司，用户在自身数据掌控方面依然处于弱势地位。二是新问题：区块链的透明性与隐私保护之间的矛盾。即如何确保在网络架构去中心化的同时，保护用户隐私数据。从数据形态看，基于AR和MR等前端设备生成的三维用户数据，是在现实空间之上叠加新的信息层，较容易引发隐私风险。现实环境中与交互无关的用户敏感数据和旁观者的敏感数据，也存在被不当采集并曝光的风险[①]。在数据存储方面，用户三维数据存储过程一旦发生数据泄露或应用程序访问不当，将会带来深度空间隐私损害。基于AR设备的多用户交互场景，还可能引发用户隐私数据访问失控以及虚拟物品和个人物理空间所有权被侵害等问题[②]。

元宇宙带来的挑战还包括智识隐私风险加剧。用户隐私数据不仅关系用户的财产权益，还影响用户人格与心智结构的养成，即智识隐私的范畴。在原初语境中，这一概念指向防止公权机构经由数字踪迹监视公民的阅读、思考与私密交流活动，进而阻断社会批评与质疑。笔者借用这一概念，讨论元宇宙中的科技巨头即元架构公司，利用数字踪迹干涉用户智识活动甚至操纵用户心智的风险。在元宇宙中，大量的用户创新创造活动是在元架构公司提供的平台上展开的，他们更直接地掌握海量用户智识活动的数字踪迹。换言之，用户在平台上的阅读、思考和创新创造等智识活动都处于元宇宙科技巨头的监视之下。而保持人的智识活动的隐私性质，确保私人领域不被监视和干扰，是现代社会个体形成独立自主人格和维系创新创造活力的重要前提。

提出这个问题并非杞人忧天。有研究者在Facebook（脸书）上做了一场大规模情绪感染实验（N=689003），表明用户情感状态可以在毫无察觉的情况下被人为操纵，而且这种情绪感染不需要人们直接参与互动，甚至不需要任何非语言暗示，只需要控制Facebook上用户能够接触到的朋友情绪表达帖文，就足以使其感染某种情绪[③]。还有研究者通过实验证实，出于特定目的干预搜索排名会导致搜索引擎操纵效应。该效应可影响选民对候选人的评价，进而改变其投票意向[④]。这两项研究的关键之处在于揭示了社交和搜索领域的科技巨头能够以极为隐秘的方式操纵群体情绪乃至行为决策，这是智识隐私侵害需要严肃审视之处。社交和搜索依然是元宇宙中不可或缺的基础需求，而且元宇宙中的科技企业对用户数据的采集在数量和深度方面都更甚于移动互联网时期。因此，应更加关注元宇宙中的智识隐私问题。

四、元宇宙中用户数据隐私保护的可能路径

元宇宙的快速发展受商业利益的驱动，这是思考元宇宙中用户数据隐私保护问题的重要语境。这一背景要求在关注用户数据隐私问题时，应注意平衡个体利益与社会福利之间的关系，在推动元宇宙经济发展中保护用户数据隐私权益。具体而言，可以从用户个体层面和面向未来的元宇宙生产关系调整层面两个视角切入，讨论用户隐私数据财产权益的可能实现机制；同时，从智识隐私视角出发，

① J.A.De Guzman，Thilakara，A.Seneviratne.Security and privacy approaches in mixed reality：A literature survey，ACM Computing Surveys（CSUR），2019（6）.

② K.Lebeck，K.Ruth，T.Kohno，et al. Towards security and privacy for multi-user augmented reality：Foundations with end users，In 2018 IEEE Symposium on Security and Privacy（SP），2018：392-408.

③ A.D.Kramer，J.E.Guillory，J.T.Hancock.Experimental evidence of massive-scale emotional contagion through social networks，Proceedings of the National Academy of Sciences，2014（24）.

④ R.Epstein，R.E.Robertson.The search engine manipulation effect（SEME）and its possible impact on the outcomes of elections，Proceedings of the National Academy of Sciences，2015（33）.

探讨用户隐私数据的表达权及人格权面向的实现路径。

(一)个体层面数据隐私保护的法律与技术实现路径

数据所有权因牵涉用户、企业和社会等诸多层面的利益,历来争讼不断。但毋庸置疑的是,用户是数据的主体,是数据的价值起源。这是因为隐私数据具有附身性[①],只有忠实反映被记录主体的数据才有价值[②]。商业机构对用户碎片化的隐私数据的采集、存储、分发和展示之所以能够带来次生价值,也是因为经过整理、加工的隐私数据集,最终仍然指向数据主体即用户自身。换言之,在法理上,商业机构不能因其在用户隐私数据采集及使用等方面的技术及人力要素投入,而主张数据所有权。这为以数据为关键要素的数字经济发展带来较大的不确定性。知情同意原则的引入将互联网企业面临的数据所有权难题转换为用户在特定平台或应用场景下隐私数据的选择性自主披露问题。在确认用户数据所有权和处置权的同时,从法律层面承认商业机构采集和处置用户隐私数据的正当性。

在移动互联网语境下,基于知情同意模式的用户选择性自主披露,并未在实质上改善用户与各类商业机构在隐私数据博弈中的弱势地位。在某些情况下,知情同意甚至成为企业独占用户数据的博弈话术。即便如此,对用户数据所有权以及知情同意和最小必要原则的法律确认仍是十分必要的。这在《中华人民共和国民法典》、《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》中均有所体现,也为用户与企业间的数据博弈提供了重要法律基点。出于公共治理或产业发展的需要,上述三部法律均规定,经过去标识化或匿名化处理的个人信息,不受知情同意原则限制。三部法律中的但书条款,通过标定个人信息与非个人信息的边界,为公权机构“依数治理”和数据业者开展用户隐私数据交易提供了法律依据,但对个体隐私数据匿名化之后的相关风险,缺乏系统和前瞻因应。这对元宇宙中用户数据隐私风险管理较为不利。因为元宇宙对用户隐私数据在种类、维度及深度等方面的需求大大超过移动互联网,即使经过匿名化处理,用户仍然可能面临较大的剩余风险。

为降低元宇宙中用户的数据隐私风险,立法部门及网络主管部门应转变规制理念,从以结果为导向的现行监管思路转向针对用户隐私数据采集、存储、分发和展示等过程的程序性规制。在当下及未来一段时期,用户隐私协议仍然是多数元宇宙科技企业寻求用户许可和授权的主要方式。因此,网络管理部门可以从用户数据隐私协议的监管入手,展开程序性规制探索。元宇宙中对用户隐私数据进行中心化控制的企业,其在用户数据隐私协议格式、内容、更新等方面,可以经由特定接口在网络主管部门备案,并向社会公开。这项操作不会增加企业在用户数据隐私合规方面的实质性负担,却可以在一定程度上提高企业用户隐私协议的社会能见度。借助各类媒体和广泛的公众监督,提升企业隐私合规动力。此外,主管部门还要对 XR 等元宇宙前端数据采集设备的用户隐私协议持续保持敏锐的监管。

企业为提升自身服务的安全性和隐私合规竞争优势,还可以借助智能合约机制,设计用户数据隐私安全保险及相应赔偿。这一事后风险补偿设想在技术上是可行的。其关键要素有三点:一是去中心化的计算机网络,即区块链;二是智能合约,企业与用户双方约定,当发生用户隐私数据泄露或滥用等风险事件并达到某一参数,即触发风险补偿;三是预言机,其重要功能是安全可靠地进行链上与链下信息传递,确保当链下违约或风险事件发生时,链上智能合约可以得到有效执行。

如图 1 所示,元宇宙中的服务提供商可以设计一份基于智能合约的用户数据隐私安全参数保险。双方约定当发生用户隐私违约或风险事件时,由多个数据源向预言机输入相应的风险参数,再由预言机根据网络中不同数据源的输入参数,向链上智能合约输出。如果该参数满足双方约定的触发条件,合约自动执行,用户获得相应赔付。这里的预言机网络是一个去中心化网络,可以有效避免预言机服务商操纵智能合约,对企业和用户而言均具有公允性。该智能合约的设立,可以在一定程度上驱动元宇宙企业加大对用户隐私数据安全保护的投入。从技术实现机制上,推动元宇宙经济不但注重形式法治层面的隐私合规,同时,在实质法治层面切实回应用户数据隐私关切。此外,预言机作为链上链下互操作的技术机制,也为解决区块链透明性与用户

① 陈本皓:《大数据与监视型资本主义》,《开放时代》,2020 年第 1 期。

② 利求同:《大数据买的就是隐私》,https://www.thepaper.cn/newsDetail_forward_1353973。

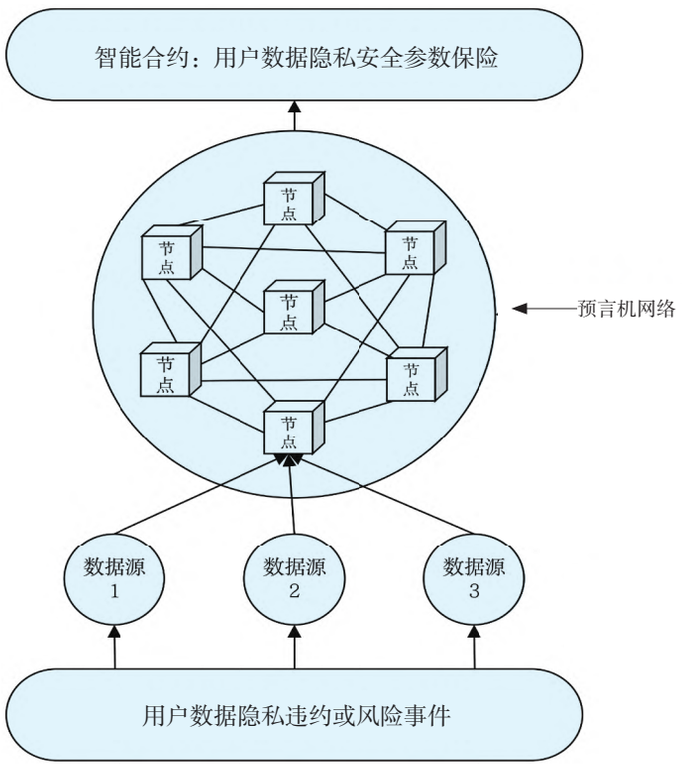

图1　基于智能合约的用户数据隐私安全参数保险示意图

数据隐私保护矛盾提供了可能方案[①②]。

（二）“数据作为劳动”：生产关系变革与用户数据隐私保护

移动互联网语境下，用户以免费的数据生产换取互联网公司的免费服务，已经成为一种心照不宣的共识或默契。在这一认知语境下，用户生产的数据是其在平台消费体验的“自然排放物”，是一种价值稀薄但又不可或缺的资源，只有具备强大算法和算力的科技巨头才有资格入场“开采”。随着移动互联网巨头向生活方式类平台转型的完成，“数据作为资源”[③]的认知似乎在逐渐固化。曾经推动移动互联网经济走向繁荣的生产关系日显疲态，表现为：一是互联网上庞大的用户数据集正在成为“数据公地”，用户在数据生产过程中付出的劳动无法获得公允回报，隐私泄露、心智操纵等丑闻层出不穷；二是科技巨头独占海量用户数据，彼此之间壁垒森严，“赢家通吃”的网络效应和“数据孤岛”后果叠加，阻碍数字经济进一步发展；三是免费数据生产导致数据质量相对较低，无法适应机器学习、人工智能等信息技术发展的数据需求。

元宇宙的到来，促使新认知落地的同时，也为数字生产关系变革提供了重要契机。从“数据作为资源”到“数据作为劳动”[④]认知的转换，不仅为推动元宇宙（数字）经济的进一步发展开辟了道路，也为思考用户数据隐私保护提供了更加宽广的观照语境。“数据作为劳动”的内涵是用户作为平台上的数据生产者，为数字经济运作贡献生产资料，作为一种数据工作，应该得到承认并获得相应劳动报酬。在“数据作为劳动”视野下，作为服务提供商的元宇宙企业，为用户数据工作付酬，一方面，可在一定

① F.Zhang，D.Maram，H.Malvai，et al.DECO：Liberating web data using decentralized oracles for TLS，In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security，2020：1919-1938.

② D.Maram，H.Malvai，F.Zhang，et al.Candid：Can-do decentralized identity with legacy compatibility，sybil resistance，and accountability，In 2021 IEEE Symposium on Security and Privacy（SP），2021：1348-1366.

③ I.Arrieta-Ibarra，L.Goff，D.Jiménez-Hernández，et al.Should we treat data as labor? Moving beyond“free”，In aea Papers and Proceedings，2018：38-42.

④ E.A.Posner，E.G.Weyl.Radical markets，Press.Princeton，NJ：Princeton University Press，2018：205-249.

程度上为其收集和使用用户隐私数据时面临的伦理争议解套;另一方面,为企业对用户数据集的使用和交易提供有力理据。此外,还能提升自身数据集的质量和技术优势,进而提高生产效率。以人工智能技术为例,无论是人工给数据贴标签,还是基于特定算法自动贴标签,在质量上均不如用户自身对数据的理解更准确、更经济。

从操作层面看,“数据作为劳动”的落地,还需要一套行之有效的数据定价机制。在元宇宙中,可依托用户声誉评价机制评定数据质量,以此作为用户数据定价的依据之一。此外,数据工作的行业、供求关系以及劳动复杂程度等,也会影响用户数据定价。就元宇宙经济而言,针对用户数据工作的定价,是一项基础工作。成熟的数据市场,一方面,有利于维护用户隐私数据权益,激励用户积极参与平台内容生产;另一方面,有利于对元宇宙企业用户数据池的估值和交易定价,进而推动数据资源的流动和共享。从长远看,数据资源的加速流动和共享,有利于减少用户重复劳动,降低平台企业的能源消耗。

(三)元宇宙用户智识隐私保护

用户隐私数据本身既牵涉财产权益,还涉及人格权、表达权等权益。笔者主要讨论元宇宙中用户隐私数据的表达权、人格权如何实现,即如何保护用户的智识隐私。元宇宙经济的一个重要特征是创作者经济,但创作者经济生态的搭建,不仅依赖于完善的经济激励机制,还需要作为创作者的用户拥有独立健全的人格和自由宽松、免于被监视的创作环境。后两者的实现,得益于良好的用户智识隐私保护。因此,即使从功利视角出发,元宇宙的持续运作也需要可靠的智识隐私保护机制。

一般而言,元宇宙中用户智识隐私保护,可以从企业、政府和用户三个视角展开思考。就元宇宙企业而言,面对智识隐私问题,不应将思路停留在遵守特定法律规则的策略性隐私合规层面,也不应将视野局限于单纯的用户知情同意层面,而应将其视为一个战略性议题,着手建立企业内部自律机制:一是在企业内部设立有影响力且相对自主的职业隐私官,使其既能接触企业高层,也能参与企业战略议题决策,同时,与政府、用户等外部利益相关者保持密切联系;二是在文化与价值观层面,将隐私部门作为回应社会关切、维护社会价值的重要功能窗口,将用户隐私数据保护纳入企业核心价值;三是在执行机制层面,在隐私部门与业务部门之间建立一套分布式网络,将隐私专家与业务部门经过专门培训的员工纳入其中,以便在产品设计和业务发展早期阶段帮助企业识别和处理隐私问题[①]。元宇宙企业借助这一机制,可以实现用户数据隐私风险的常态化管理,内部自律机制的有效运作也会为企业赢得无形的声誉。

立法及网络主管部门应对元宇宙中平台型企业收集和分析用户智识活动数据保持警惕,并积极探索一系列基于技术架构、市场机制、法律法规和社会规范的多元监管框架,形成有效的他律机制。需要注意的是,外部威慑机制并非越严厉越好,而应做到适用得当、激励相容[②]。适用得当是指元宇宙中的智识隐私问题适用何种监管框架。我国现行法律中存在网络安全框架和个人信息保护框架两种思路。元宇宙中的智识隐私问题更适合在个人言论及信息保护框架下处理,不宜轻易启动网络安全审查程序。用户智识隐私权益具有一定的相对性,牵涉用户与企业、企业与企业之间的博弈与竞争,为个人信息保护框架提供了较大的回旋与妥协空间。相应地,网络安全审查牵涉国家安全,一方面,为国内相关产业发展和企业参与国际市场注入较大不确定性;另一方面,无法真正维护国家安全及用户智识隐私权益,易导致多方共输的局面。

激励相容指国家经由外部立法,推动企业完善内部自律机制,引导企业在开发利用用户隐私数据、追求自身利益的同时,遵守相关法律法规、维护用户智识隐私权益,即激励监管。例如,在元架构企业中,用户主要基于平台架构开展创新创造活动。因此,网络管理部门应对用户与企业之间的服务协议保持监管注意,指导企业设立完善的内部治理机制,规范自身用户隐私数据采集及处置行为,同时,针对企业侵犯用户智识隐私的行为规定明确和直接的惩罚措施,做到激励与约束相平衡。此外,平台封闭和数据垄断是导致移动互联网语境下用户情感与心智受到操纵的重要基础。在元宇宙产业发展进程中,立法及网络主管部门应更加注重依靠市场机制

① K.A.Bamberger,D.K.Mulligan.Privacy on the ground:Driving corporate behavior in the United States and Europe,MIT Press,2015:13-14.

② 周汉华:《探索激励相容的个人数据治理之道》,《法学研究》,2018年第2期。

增强网络服务的开放性和多样性，让用户拥有自主选择权。

对于普通用户而言，亟需提升自身隐私意识及数据素养，体认到在算法和代码定义的当下及未来数字社会，个体生活的量化趋势既深且巨、有增无已，需清醒审慎地看待其对个体权益和心智结构的再塑造。

五、结　语

本文从账户、数据和声誉评价三要素层面，描述了元宇宙中用户数据生产与控制机制相较于移动互联网的变化，以及这种变化引致的元宇宙用户数据隐私风险，从个体层面提出化解用户数据隐私风险的法律与技术路径，初步阐释了元宇宙中数字生产关系变革的必要性及其对用户数据隐私保护的意义，讨论了元宇宙中用户智识隐私风险的应对原则。

元宇宙中的用户数据隐私问题，既涉及用户个体层面的财产、表达与人格权益，还牵动数字经济背后的生产关系调整，反映了社会商业力量、政治力量和个体权益之间的多维博弈。换言之，用户数据隐私问题具有突出的现实意义，后续研究应更加注重元宇宙细分场景中的用户隐私关切，以及政府和企业层面相应的隐私合规与监管设计。例如，AR/MR 设备使用中多用户交互引发的安全与隐私问题以及可能的因应措施，即当下元宇宙经济发展中一个具有现实迫切性的实践课题。

User Data Privacy in the Metaverse

CHEN Hui　YAN Jia-qi　CHEN Rui-qing　SHEN Yang

（School of Journalism and Communication，Tsinghua University，Beijing 100084）

Abstract: The metaverse，as the next generation Internet，significantly changes the production and control mechanism of user data and brings new user data privacy issues. The first is how to overcome the hollowing out of user data ownership caused by centralized control mechanism and the possible manipulation of emotions and decisions triggered by meta-architecture companies that violate user's intellectual privacy. The second is how to resolve the contradiction between the transparency of blockchain and user privacy data protection under the decentralized control mechanism. In this paper，we propose to respond to the above challenges at two levels：individual users and changes in production relations. There are two initiatives at the individual level. First，we shift from result-oriented regulation to procedural regulation，and enhance the incentive of ex-ante privacy compliance of metaverse enterprises through the regulatory filing of user privacy agreement format，content and updates. Second，we introduce smart contract-based insurance of user data privacy security parameters to improve the post-facto privacy risk compensation mechanism for users. Measures at the level of production relations：through the cognitive and production relations change of "data as labor"，we analyze the ethical，economic and technical values of metaverse enterprises to pay for user data work，and provide possible directions to explore the pricing mechanism of user data at the operational level. Finally，we propose a possible path to protect the intellectual privacy of metaverse users.

Key words: Metaverse；Data Privacy；Intellectual Privacy；User

[责任编辑：王文秋]
[责任校对：曹晶晶]