元宇宙背景下个人生物信息的法理辨析及保护路径

裴儒雯*

摘要：元宇宙是借助数字技术打造的沉浸式全息虚拟社会，其实现需要依靠增强现实（AR）、虚拟现实（VR）等沉浸式技术设备获得用户的动态，在此过程中需要大量收集用户的身体特征数据、手势动作、眼球位置信息等广义的“个人生物信息”。当前，我国《个人信息保护法》对于广义上的“个人生物信息”并无明确定义，仅将“个人生物识别信息”列举为“特殊个人敏感信息”的七种情形之一。结合个人生物信息在元宇宙中的技术中立、平台管理、跨国利用、去中心化追责风险，应拓宽“个人生物识别信息”的法律概念，将“可识别”纳入其概念范畴内，以回应个人生物信息的广义内涵。此外，还需要建立去中心化身份认证系统，完善“My Data”数据模式，并强化代码与法律的互补，以构建更加全面和有效的个人生物信息保护机制，在技术发展的同时确保个人隐私不受侵害，构建安全、公正、有序的元宇宙环境。

关键词：元宇宙　个人生物信息　敏感个人信息　间接识别　去中心化身份

* 英国曼彻斯特大学

目录

一、问题的提出

从使用简单的静态网站到通过Web2创建全球社区，现代技术的发展已经快要进入Web3时代——基于区块链和加密货币的未来去中心化版本的互联网——也就是元宇宙（Metaverse）时代。元宇宙是指模拟三维数字环境，通过人工智能、虚拟现实（VR）、增强现实（AR）、混合现实（MR）、物联网（IoT）、区块链等技术，为用户提供身临其境的体验并模仿现实世界。[1]

元宇宙是一个纯粹的数字社会，用户可以创建数字化身（Avatar），以数字人或虚拟人身份在元宇宙进行生存、交互，相较于目前的互联网交互，元宇宙用户的数字化身可以在既定环境中形成用户的视觉形象、技能以及社会互动。[2]同时，元宇宙打造虚拟社会需要依靠AR、VR等沉浸式技术设备，在数字孪生和数字原生[3]过程中需要收集比目前互联网当中更多的个人生物信息，如身体特征数据、运动轨迹、手势动作、眼球位置信息等，涵盖面部识别、指纹识别、甚至心率和情绪反应等多个层面。这些信息的应用极大丰富了虚拟环境的互动性和沉浸感，为用户提供了前所未有的体验，也带来了诸多法律和伦理上的挑战。

在元宇宙环境下，根据个人生物信息，元宇宙平台打造者能够结合大数据技术深度挖掘并推断出用户的深层次私人信息。这不仅可能导致基于数据分析的精准推送影响用户的个人决策自由，还可能加剧信息茧房现象和市场垄断问题，从而严重损害用户的合法权益。在元宇宙这一跨界融合的虚拟空间中，若个人生物信息被不当利用，还可能构成国家安全的潜在风险，甚至在极端情况下被用于网络战争等安全威胁。

目前，针对元宇宙的法律研究还只停留在基础领域，如刑事、民事、知识产权等学科的潜在问题，关于元宇宙中个人生物信息保护问题很少提及。因此，本文将在辨析元宇宙中个人生物信息应用与保护的法理基础上，深入分析元宇宙背景下个人生物信息保护所面临的风险类型，结合我国现行立法有关规定，提出重构个人信息概念、建立去中心化身份等建议，以期在保障技术发展的同时最大限度保护个人信息，为构建未来的元宇宙环境提供平衡技术进步与个人权利保护的发展性视角。

二、元宇宙中个人生物信息的法理辨析

（一）个人生物信息的概念厘定

在依托于沉浸式技术的元宇宙语境下，个人生物信息的涵义具有多维性和复杂性。个人

[1] *See* Al-Ghaili, A. M., Kasim, H., Al-Hada, N. M., Hassan, Z., Othman, M., Hussain, T. J., ... & Shayea, I. (2022). A review of metaverse's definitions, architecture, applications, challenges, issues, solutions, and future trends. *IEEE Access*, 125835-125866.

[2] 参见张晨原：《元宇宙发展对个人信息保护的挑战及应对——兼论个人生物识别信息的概念重构》，载《法学论坛》，2023年第2期。

[3] 参见张钦昱：《元宇宙的规则之治》，载《东方法学》，2022年第2期。

生物信息作为元宇宙身份验证和交互的基础，不仅限于传统的指纹、面部识别等生理特征，还包括行为模式、情绪反应等更加细微和动态的信息。具体而言，个人生物信息的范畴可以细分为以下几类：其一，生理信息，如指纹、面部特征、虹膜等静态特征，通常用于身份认证；其二，行为信息，包括但不限于步态、键盘敲击模式、书写习惯等，反映个体的行为习惯；其三，健康信息，诸如血压、血糖数据、基因序列等，通常用于医疗健康领域；其四，心理信息，如情绪反应、压力水平等，可能通过生物反馈设备采集。

元宇宙沉浸式技术收集的实时人体生物信息属于个人信息，但不能直接识别到个人。《个人信息保护法》第四条[4]对个人信息的定义中区分了“已识别”和“可识别”，本质上与欧盟《通用数据保护条例》“识别+关联”的个人信息界定路径相同。识别路径直接定位到个人是根据信息本身的独特性，即“直接识别”；而关联路径可以引申出更多的关于该个人的信息是在已知特定个人的基础上，从而“间接识别”到个人。[5] 在元宇宙沉浸式系统中，需要收集用户个人生物信息的主要是三维显示技术和体感交互技术，[6] 这些技术收集的信息既包括人脸和虹膜等直接识别用户身份的特定生物识别信息，也包括不能直接识别到个人的其他个人生物信息。事实上，“个人生物信息”是一个较为广义的概念，既往立法和学界研究主要集中的“个人生物识别信息”属于其子集。所谓个人生物识别信息，即通过生物识别技术对自然人的物理、生理或行为特征进行特殊技术处理而得到的信息，如指纹、虹膜、脸部特征、声音、步态、笔迹等可以独一无二地关联到个体身份的信息，[7] 该类信息也被《个人信息保护法》列为法定列举的七类“特殊敏感个人信息”之一。

元宇宙背景下的“个人生物信息”与当前立法中的“个人生物识别信息”有着显著的概念区别。一方面，元宇宙沉浸式技术收集的个人生物信息，比如眼球移动信息，皮肤电反应信息等具体的生物信息仅能反映某个人在特定时刻的身体状态，会随时间的变化而变化，如果没有其他的有效信息来辅助确定，这些信息本身不足以准确识别到个人，所以不符合个人生物识别信息的内涵。另一方面，元宇宙沉浸式技术收集的个人生物信息不符合直接识别信息的唯一性。如果仅凭某个个人信息就可以精准识别到个人，那这一信息就必须具有唯一性和稳定性，例如人脸、指纹、虹膜等。[8] 然而，元宇宙沉浸式技术收集的生物信息大多是随时间变化的，而且大概率并不是某个人所特有的，不断变化的信息显然不符合直接识别。因此，在构建元宇宙个人生物信息保护机制时，不应局限于现有的法律框架，而是应追溯元宇宙中个人生物信息收集与应用的法律性质，以满足元宇宙背景下个人生物信息保护的特殊需

[4] 《个人信息保护法》第四条：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。

[5] 参见张新宝主编：《〈中华人民共和国个人信息保护法〉释义》，人民出版社 2021 年版，第 41 页。

[6] 参见杨青、钟书华：《国外“虚拟现实技术发展及演化趋势”研究综述》，载《自然辩证法通讯》，2021 年第 3 期。

[7] 参见杨铜铜：《论个人生物识别信息保护的立法路径》，载《北京理工大学学报(社会科学版)》2021 年第 6 期。

[8] 参见焦艳玲：《个人生物识别信息的界定》，载《重庆大学学报（科学社会版）》。

求。

（二）元宇宙中个人生物信息收集与应用的法律性质

在元宇宙中，个人生物信息的收集通常基于沉浸式技术装置，如头戴式显示器（HMD）、脑机接口（BMI）和追踪设备。[9]例如，头戴显示器能够通过内置的眼球追踪技术，收集用户的视线移动数据；穿戴式设备能够捕捉到心率变化、肢体动作等信息；而肌电图（EMG）和脑电图（EEG）等技术则能够记录神经生理反应。元宇宙收集这些个人生物信息属于间接识别，可以和其他信息结合关联到个人，从而挖掘出更多深层次的信息。用户在元宇宙中会进行各式各样的社会活动，比如购物、游玩，在这些活动中会留下轨迹信息，平台或商家收集这些信息并通过大数据分析出用户的潜在偏好。潜移默化干扰用户的选择判断，结果上为用户造成了很多隐私困扰，很可能侵犯用户的隐私权。[10]单独这些个人生物信息并不能让元宇宙平台识别到用户究竟是谁，但平台却可以通过这类信息了解到用户的行为偏好，进而影响到用户的行为，在更大范围上来看是元宇宙平台利用不特定多数用户的个人信息谋取利益。个人生物信息在元宇宙中的应用场景极为广泛，不仅包括虚拟交互与社交平台上的身份认证、社交互动体验的增强，还包括在教育、训练模拟、医疗健康监测以及广告个性化推送等方面的应用。[11]在法律性质上，尽管个人生物信息的收集为间接识别，但其与用户的紧密联系使得其在法律上具有潜在的敏感性，应被赋予更高的保护层级。

（三）元宇宙平台收集和使用个人生物信息的法律义务

元宇宙平台在收集和使用个人生物信息时，必须遵循《个人信息保护法》等相关法律规定，承担起相应的法律义务，确保个人生物信息的合法性、正当性和必要性。元宇宙平台在收集和使用个人生物信息时，必须明确信息收集的目的、方式和范围，并向用户提供明确的知情同意选择。平台在进行任何形式的个人生物信息处理活动之前，都需要获取用户的明确同意，且这一同意必须是基于充分信息的自由意志表达。

此外，元宇宙平台应当采取相应的技术和管理措施保护个人生物信息的安全，防止数据的非法访问、泄露或滥用。例如，应用加密技术、匿名化处理、访问控制等手段来加强数据安全。同时，平台还应建立数据保护的内部监督机制，对数据处理活动进行持续的审查和评估，以及时发现并纠正可能的风险或违规行为。

在个人生物信息的使用上，元宇宙平台应严格遵守数据最小化原则，仅收集实现特定功能或服务所必需的最少信息，并在使用后及时删除或进行匿名化处理。对于用户的生物信息，还应提供足够的知情权和选择权，包括但不限于数据访问权、更正权、删除权，以及在某些情况下的拒绝处理权。

---

[9] *See* Murala, D. K., & Panda, S. K. (2023). Metaverse: A Study on Immersive Technologies. *Metaverse and Immersive Technologies: An Introduction to Industrial, Business and Social Applications*, 1-41.

[10] 参见张晨原：《元宇宙发展对个人信息保护的挑战及应对——兼论个人生物识别信息的概念重构》，载《法学论坛》，2023 年 3 月第 2 期。

[11] *See* Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, *6*(2), 234-247.

三、元宇宙背景下个人生物信息保护面临的风险

（一）个人生物信息的体系定位反思

我国《个人信息保护法》采用“法定列举”和“具体场景”双标准来判定个人敏感信息，[12]于第二十八条第一款规定：“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。”其中列举的典型情形归类于“特殊敏感个人信息”，其他并未被列举但根据具体情形判断一旦泄露或非法使用对个人生活有重大影响的属于“一般敏感个人信息”。

根据该款定义，元宇宙沉浸式技术收集的个人生物信息与用户本人密切相关，与个人隐私权、人格尊严以及人身和财产安全的密切关联，一旦被泄露或非法利用就会给用户本人造成极大损害，符合敏感个人信息的定义。例如，用户在元宇宙中的行为模式、身体运动、甚至神经生理反应等，都可能被实时记录并用于提供个性化的虚拟体验。这些信息的敏感性在于，它们可以被用来推断出用户的健康状况、心理状态、喜好等私密信息，一旦被滥用，可能导致个人隐私的大规模泄露。但由于个人生物信息并不等于生物识别信息，不属于法律明确列举的几类之一，所以无法归类于特殊敏感信息，只能被界定为一般敏感信息。[13]

然而，与传统的生物信息相比，元宇宙中的信息收集更为广泛和深入，元宇宙的实时性和交互性也意味着个人生物信息的收集和应用几乎是即时的。用户在元宇宙中的每一次动作、每一次交互，甚至每一次视线的停留，从基础的生理反应到复杂的行为模式，都可能成为数据收集的对象。这种高度的信息积累，不仅体量巨大，还具有高度的多样性和复杂性，超越了传统数据收集的规模和范畴。随着技术的发展，尤其是大数据分析技术的进步，从这些庞大数据集中挖掘信息变得更加快速和精准。大数据算法可以识别出用户的行为模式，预测其偏好和行为，甚至可能在用户未明确意识到这些偏好之前就进行预测。这种精准性本身并不是问题，但当这些分析用于超出用户预期和同意的范围时，便构成了个人生物信息的潜在滥用。

再者，用户在元宇宙中往往以匿名或半匿名的身份活动，这种状态下的信息保护尤为复杂。尽管用户在元宇宙中的活动可能不直接显示其真实身份，但通过生物信息，如面部识别、声纹识别、甚至是行为模式等生物特征，有可能间接地揭露用户的真实身份。例如，用户在元宇宙的社交互动中，可能不愿透露自己的真实姓名或地理位置，但用户的运动模式、眼球追踪数据、语音模式等可以成为辨识个体身份的关键线索，这些信息若被第三方收集并与其他数据库中的信息进行匹配，可能会揭露用户的真实身份。一旦这些个性化信息被恶意软件

[12] 参见王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》，载《当代法学》，2022 年第 1 期。

[13] 参见张晨原：《元宇宙发展对个人信息保护的挑战及应对——兼论个人生物识别信息的概念重构》，载《法学论坛》，2023 年 3 月第 2 期。

利用或黑客攻击，就会造成用户隐私的严重泄露，甚至可能威胁到其物理世界中的安全。

因此，现有制度框架将元宇宙情境中收集的个人生物信息简单归类为一般敏感信息难以全面反映其潜在的风险。在法律体系中对个人生物信息的定位需要进一步明确，应考虑到元宇宙中个人生物信息的收集、存储、使用和传输的特殊环境和条件，剖析其可能产生的具体风险，再重新构建具有针对性的保护路径。

（二）元宇宙本身的技术风险

元宇宙作为一个全新的虚拟社会形态，其基础是由先进的科技硬件和复杂的代码所构建。在建设元宇宙的诸多基层代码中有一个至关重要的底层技术——区块链，可以说没有区块链就没有元宇宙。区块链技术自问世以来，因其去中心化的分布式记账特征，被比喻为“信任机器”。有学者认为，法治本质上是一种信任机制，依靠国家主导的各种中介机构来维持社会秩序和可预测的人际关系，[14]被称为“信任机器”的区块链技术因此具有制度技术或者法律技术的属性。[15] 然而，区块链技术本质上是由算法进行决策的，可能产生“算法黑箱”（Algorithmic Black Box）问题。算法黑箱指的是由于技术本身的复杂性，以及技术公司的排他性商业政策，使得用户无法清楚地了解算法的目标和意图，也无法获知算法设计者、实际控制者以及机器生成内容的责任归属等信息，更难以对其进行评判和监督。[16]简而言之，由于算法决策过程的不透明性，用户往往不能理解或预测算法的行为和结果，使得元宇宙中的区块链系统可以在用户不知情的情况下产生自动化歧视，并通过自主学习不断深化发展，使得这种问题日趋普遍、连续、稳定。[17]

此外，元宇宙的基础技术自代码生成和使用以来尚未经过测试和风险评估，因此很可能会因代码错误、泄露、漏洞等自我工程问题而产生用户隐私泄露的风险。用户有权在虚拟和现实世界中保护自己的隐私不被泄露，并应得到平等的法律保护。因此，在元宇宙背景下，用户应该有更大的权利知道和批准使用他们的信息，[18]尤其是个人生物信息这类敏感信息。由于在元宇宙中沉浸且全息的活动方式，用户的所有活动将由代码转换为计算机可读的数据，如果服务提供商即控制元宇宙建造的大型科技公司访问该数据并没有相应的限制措施，[19]用户也没有合理的救济途径，用户的隐私安全将面临极大威胁[20]。

（三）元宇宙平台对个人生物信息的管理风险

---

[14] 参见郑戈：《区块链与未来法治》，载《东方法学》，2018 年第 3 期。
[15] 参见夏庆峰：《区块链智能合同的适用主张》，载《东方法学》，2019 年第 3 期。
[16] *See* Loi, M., Ferrario, A., & Viganò, E. (2021). Transparency as design publicity: explaining and justifying inscrutable algorithms. *Ethics and Information Technology*, *23*(3), 253-263.
[17] 参见熊进光、贾珺：《元宇宙背景下数字侵权法律问题的境遇及应对》，载《上海法学研究》集刊，2023 年第 5 卷。
[18] 参见白牧蓉、张嘉鑫：《元宇宙的法律问题及解决路径的体系化探究》，载《科技与法律》，2022 年第 3 期。
[19] *See* Edvardas Mikalauskas， Privacy in the metaverse: dead on arrival? https://cybernews.com/privacy/privacy-in-the-metaverse-dead-on-arrival/.
[20] 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《科技与法律》，2022 年第 3 期。

元宇宙构建过程中，平台——开发元宇宙的大型科技公司——起着至关重要的作用。由于元宇宙全虚拟的设定，代码可以创造这个世界中的一切，是无所不能的。在元宇宙中，代码几乎是“神”一样的存在，比现实物理世界中的法律和政府更加具有权威性和强制力。因此，大型科技公司在这一全新的虚拟世界中拥有绝对的编码和管理权力，他们的平台政策、技术选择和商业模式将直接影响用户的隐私和个人信息安全。

元宇宙平台通过各种沉浸式技术装置收集用户的生理和行为信息。在元宇宙背景下，用户在虚拟空间中进行各种活动，一举一动都成为透明的数据源和目标进行分析，但是这是完全单向的信息传递，用户完全不知道数据收集者的行为究竟是什么。当用户的行为、喜好甚至情绪状态等个人生物信息都被转换为数据时，用户在注册或使用服务时却只能被动接受用户协议，无法真正理解并控制自己的数据。目前，许多科技企业只是在软件下载过程中为客户提供通用权限替代方案，而不是设置菜单式的选择。用户协议和隐私规则经常以复杂的方式表述，使得消费者无法选择预定义默认值以外的任何内容。在没有完善监管机制的情况下，这些平台有可能滥用收集到的个人生物信息，不仅出于商业利益，也可能因技术缺陷导致信息泄露。此外，由于元宇宙中的法律体系尚未健全，用户在面对个人生物信息侵权时缺乏有效的法律救济。用户在维护自身合法权益时，不仅需要对抗科技公司的技术优势，还面临着缺乏有效申诉渠道的困境。

同时，服务提供商也会通过各种方式规避自身的侵权责任。在世界范围内都有广泛影响力的“索尼案”中，技术中立的概念被美国法院确定为网络冲突的普遍适用标准。避风港规则，也称为技术中立规则，本质上是一种豁免规则，免除仅提供纯技术的网络服务提供商的侵权责任。[21] 一般来说，技术中立豁免应考虑以下因素：第一，有关技术可用于侵权以外的目的；第二，技术服务提供者缺乏检测和禁止用户侵权行为所必需的技术技能和资源；第三，技术服务提供者在提供技术时，没有表现出鼓励或帮助违法者实施违法行为的意愿。尽管技术中立原则是一个抽象的原则，但科技企业经常援引它作为避免采取适当行动的理由，即所谓“技术客观性的看似合理的外表”，[22] 使其成为科技企业规避责任的工具。在元宇宙这样一个新兴且高度技术依赖的环境中，科技企业可能会依赖技术中立原则作为防御盾牌，而忽略了其对用户个人生物信息保护的责任。

（四）个人生物信息在元宇宙中的跨国利用风险

虽然元宇宙的开发公司隶属于不同国家，但区块链、NFT 等元宇宙基础技术并没有明显的国家属性。由于元宇宙具有广泛而包容的特性，世界各国的用户都可以加入不同的元宇宙系统当中。不同国家的用户在元宇宙当中的活动可能会涉及不同国家的利益，元宇宙的治理因此存在国家层面的管辖权冲突。[23] 在跨境收集、使用、流通和保护元宇宙用户个人生物

[21] 参见林凌：《构建元宇宙敏感个人信息二元保护机制》，载《传播法治研究》，2023 年第 2 期。
[22] 熊进光、贾珺：《元宇宙背景下数字侵权法律问题的境遇及应对》，载《上海法学研究》集刊，2023 年第 5 卷。
[23] 参见张钦昱：《元宇宙的规则之治》，载《东方法学》，2022 年第 2 期。

信息时，元宇宙开发者所在国家的法律可能与其他国家的法律相冲突。

首先，元宇宙的用户和开发者来自多个国家，每个国家都对从用户那里收集的个人生物信息等敏感个人信息拥有管辖权。由于每个国家对于敏感个人信息的保护法律不一，各国通常将在本国境内产生的个人生物信息存储在受本国法律保护的服务器中。[24] 但在元宇宙环境中，一旦敏感个人信息被存储在开发者所在国家，可能会触及到信息来源国家的安全与隐私问题。其次，由于不同国家个人信息的价值观和保护水平存在差异，用户在元宇宙中应有权选择其个人生物信息的存储地，以便更好地保护自己的隐私。但在现行的法律框架下，用户难以拥有对个人生物信息存储选择的控制权。再次，尽管元宇宙为用户提供了虚拟社会交互的平台，但由于个人生物信息的滥用可能导致的伤害最终会反映到现实世界，寻求司法救济成为另一大挑战。受害者可能会在决定是否向开发者所属国家寻求法律救济时遇到障碍，因为元宇宙的跨国法律执行和争议解决机制尚不完善。[25]

（五）对个人生物信息侵权的去中心化追责风险

在元宇宙环境下，用户的个人生物信息不仅跨越了物理空间，也跨越了法律边界，当这些信息遭到侵权时，侵权行为往往难以追溯到具体的责任人。元宇宙的数据存储和流通往往依赖于分布式的区块链技术，数据的管理和控制权分散在众多节点上，任何单一节点的失效或恶意行为都可能影响到整个系统的安全和数据的完整性。[26] 此外，区块链上的数据一旦被记录，更改极为困难，即使数据存在错误或者侵犯了个人生物信息的相关权利，也难以从系统中完全抹除。

作为去中心化的机构，区块链不受任何一个人或中心化组织的控制和监督，当有人在区块链上发布包含非法内容的信息时，由于算法限制与多次传递，很难识别出实际的侵权者，导致追责成本很高。当收集到的个人生物信息被泄露或非法利用，这些个人生物信息在元宇宙中依靠区块链技术流通速度非常快，并且难以确定泄露者或非法利用者的真实身份，也就陷入了追责困境。[27] 由于元宇宙参与者遍布全球，即便能确定侵权行为，受害者在法律追责和寻求补偿的过程中，也可能因为地理位置、法律差异、执法难度等问题面临巨大障碍。同时，元宇宙中的智能合约和自动化决策系统可能进一步加剧追责困境。这些系统的自动化操作一旦触发侵权，责任归属的判定不仅涉及技术层面，更涉及到法律和伦理层面的深层次问题。因此，如何在保护个人生物信息的同时，确保技术发展和创新的自由度，是元宇宙发展过程中必须解决的重要课题。

四、元宇宙背景下个人生物信息保护路径

[24] *See* Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory LJ*, *64*, 677.
[25] 参见于洋：《论个人生物识别信息应用风险的监管构造》，载《行政法学研究》，2021 年第 6 期。
[26] *See* Li, X., Wang, Z., Leung, V. C., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks: A survey and outlook. *ACM Computing Surveys (CSUR)*, *54*(3), 1-38.
[27] 参见李晶：《元宇宙中通证经济发展的潜在风险与规制对策》，载《电子政务》，2022 年第 3 期。

（一）重构个人生物信息概念：新增“可识别”的内涵

在上文中提到，在我国《个人信息保护法》的体系内，元宇宙沉浸式技术收集到的个人生物信息应该归类为一般敏感个人信息，因其不具备“唯一性”和“稳定性”，所以并不属于生物识别信息。这就导致在保护元宇宙个人生物信息时需要应用一般敏感个人信息的“人格尊严、人身财产安全受到侵害（危害）”的法定标准进行判断，在个案中结合具体情况对敏感度进行具体分析。然而，个案分析在实践中具有较大的不确定性，需要付出大量的时间成本和司法资源，平台也可能因为额外支出的成本而尝试更加隐蔽的侵权方式进而规避审查。

解决这个问题有两种途径。一是提出一个新的概念，将元宇宙背景下的个人生物信息归类为“生物可识别信息”进行保护，列入《个人信息保护法》第二十八条的明确列举范畴，将其作为第八种“特殊敏感个人信息”。因为该类信息在元宇宙环境下具有个人身份的强关联性，财产价值远超于一般敏感个人信息，泄露或非法利用会对用户造成严重损害，所以可以作为特殊敏感个人信息的一种予以特别保护。但此种解决方法也具有很明显的弊端，新概念的普及和被广泛接受需要很长时间，经过反复论证才可以应用，不利于目前个人生物信息的保护。

第二种方法就是重构已有的“个人生物识别信息”之概念，拓宽其原始边界，将“生物识别信息”中的“识别”扩大解释为“已识别”和“可识别”。元宇宙背景下的个人生物信息，因其可以间接识别用户身份，具备纳入解释的条件。当前，个人生物识别信息中的“识别”在我国学界的语境下仅仅指的是“已识别”，但在全球立法范围内，欧盟《通用数据保护条例》和美国加州《消费者隐私权法案》已经将“可识别”的概念纳入其中。例如，《通用数据保护条例》第 4 条第（14）项在圈定个人生物识别信息应当属于自然人的身体、生理、行为特征方面之后，进一步指出个人生物识别信息应当“能够识别（allow）”或“确认识别（confirm）”到自然人。[28] 其中，“能够识别”恰好与“可识别”的概念相符。国内相关法规，如《信息安全技术生物特征识别信息保护基本要求》（GB/T 40660—2021），也倾向于将“可识别”纳入个人生物识别信息内涵，强化对用户生物信息的保护。因此，应当祛除“唯一性”的特征，新增“可识别”的内涵，将元宇宙平台收集的个人生物信息纳入“个人生物识别信息”的法律规制之中。[29]

（二）建立去中心化身份

个人生物信息一旦重构，就应纳入生物识别信息的法律保护范畴，并针对元宇宙背景构建全新的法律框架，对如何在去中心化环境中实施身份认证进行系统性规划，建立去中心化

[28] Article 4 (14) of GDPR: ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

[29] 参见张晨原：《元宇宙发展对个人信息保护的挑战及应对——兼论个人生物识别信息的概念重构》，载《法学论坛》，2023 年 3 月第 2 期。

身份等互联网可信身份责任模型，从验证层、应用层和信息层三个技术层面完善责任监管。[30] 尽管注册方法越来越多，但一些学者认为，理论上，元宇宙可以将“根化身”定义为身份的综合集合，结合所有数字身份。用户可以访问的项目和材料可以基于这个“根化身”进行配置。然而，为了确定可以存储所有身份信息的系统的身份标识符，元宇宙显然需要更多的协议，这份工作也相当困难。政府介入和监管元宇宙的一个基本起点是主权和管辖权，为了在全球范围内创造一个安全且不可触碰的身份，各种区块链技术是当前行业实践背后的根本驱动力，根化身用户穿越多个元宇宙并参与所有系统的能力可以使全球或至少实质性的价值交换系统成为可能。[31]

同时，在身份本身去中心化之后，数字身份认证吸收了传统身份认证所不具备的积极内容，如特定的身份服务、特色的财产流通、信息经济价值等，值得进一步研究。一个可能的解决方案是，探索赋予用户主权身份，主权身份只能由它所认证的人来控制，这是一对一独特的个人身份认证方式。这种形式的身份认证需要根据虚拟空间规模，构建信任框架，并以信任框架为基础设计精确的认证模式。[32] 通过确保用户对其数字身份的完全控制权，增强对其个人生物信息的保护。主权身份意味着用户可以自主管理自己的生物信息，选择何时、如何以及与谁分享这些信息，有助于防止对个人生物信息未经授权的使用和潜在的滥用，保障用户在元宇宙中的隐私权和数据安全。

（三）完善 My Data 数据模式

需要访问元宇宙的用户将在很长一段时间内保持“登录”状态，而元宇宙的平台创建者可以随时随地持续观察和跟踪用户的活动。因此，元宇宙平台必须遵守更严格的数据安全保护要求，“以个人为中心”的数据保护和治理范式也将成为主流。作为大数据和征信领域的一种新的法律合规模式，首先由英国提出、近年来在韩国金融业广泛应用的“My Data（本人数据管理）”模式就是其中的典型。[33] “My Data”理念核心的思想在于个人应该控制自己的数据，信息主体可以将自己的信息用于管理其资产和信用等目的，分享来自自身的数字红利。[34] “My Data”帐户包含所有法律上可接受和同意的用户信息，并且有权控制如何将数据从数据源传输到授权系统中的用户。由于帐户的可移植性，用户可以选择和切换运营商服务，从而降低服务提供商锁定的风险，强化自身的数字主权身份。“My Data”的实施最终可以完全简化个人信息的治理结构，弱化对于数据收集平台的依赖。

---

[30] 参见阮晨欣：《法益衡量视角下互联网可信身份认证的法律限度》，载《东方法学》，2020 年第 5 期。
[31] 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《科技与法律》，2022 年第 3 期。
[32] 参见[美]约翰·贝斯特：《数字化金融》，王勇、黄红华译，人民邮电出版社 2019 年版，第 132-153 页。
[33] 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《科技与法律》，2022 年第 3 期。
[34] *See* Kim, E. C., Kim, E. Y., Lee, H. C., & Yoo, B. J. (2021). The details and outlook of three data acts amendment in south korea: with a focus on the changes of domestic financial and data industry. *Informatization Policy*, *28*(3), 49-72.

在元宇宙背景下，“My Data”可以让用户更自由地选择如何与他人交流他们的识别属性，[35] 促使用户在不断在线的元宇宙空间中对自己的个人生物信息拥有更多的控制权。用户可以基于“My Data”账户自主管理个人生物信息，选择性地与第三方共享，并追踪信息的使用情况。用户的数字身份不再受限于单一平台，而是可以在多个元宇宙平台中自由移植和使用，用户成为了自己生物信息的主权所有者，享有完整的控制权和决策权，有效地保护个人生物信息不被滥用。

（四）促进代码与法律相互补强

虽然元宇宙还只是一个理想状态的概念，但现代科技风险的复杂性与不确定性并不否定规范先行的意义。[36] “风险自负”的地位在个人生物信息主体有限理性的影响下逐渐崩溃。“知情同意”范式是当前大多数个人生物信息使用的基础。信息主体必须足够理性，清楚地掌握风险影响，并能够自由选择是否允许其他信息处理者使用它，以使该模型发挥作用。然而，在元宇宙背景下，个人生物信息的主体和信息处理者具有不同程度的信息不对称性。由于个人生物信息和其他信息的复合应用，以及算法黑箱的持续存在，信息主体不可能提前预见危险。实践中信息应用者却往往通过间接强制的方式迫使信息主体做出“同意”，如果用户不同意隐私政策，将无法使用相应的软件。因此，需要通过法律规范来补充技术措施，确保个人生物信息的合理使用和有效保护。

法律应明确指出，在元宇宙这一高度数字化和虚拟化的环境中，个人生物信息的收集、使用和传输必须遵循更加严格的隐私保护标准，包括对数据收集目的的明确界定、对用户的充分告知和明确同意、对收集数据的严格限制等，确保只收集实现预定功能所必需的最小数据集。此外，法律法规应当明确界定信息使用者的责任，防止其通过间接强制方式获取用户同意，真正实现个人生物信息的自主管理和风险防范。[37]法律应规定元宇宙平台在处理个人生物信息时，不仅要确保数据安全，还要保障数据的可追溯性和可审计性，建立透明、可靠的数据处理记录，以便在出现数据泄露或滥用时能够及时追溯并采取措施。此外，鉴于元宇宙中用户身份可能呈现匿名或半匿名的特点，法律应特别强调在这种情境下用户个人生物信息的保护。元宇宙平台在设计和实施身份认证机制时，必须兼顾用户隐私保护和身份安全，避免因技术漏洞或政策缺陷导致用户个人生物信息泄露。最后，考虑到元宇宙的全球性和跨境特征，法律规范还应包含国际合作和数据流通的规则，确保跨境数据交换时个人生物信息的保护不降低，防止数据在全球范围内的非法使用和滥用。

随着元宇宙概念的进一步落地，虚拟空间与现实空间的界限将会越发模糊，元宇宙中产生纠纷、元宇宙中行为对影响现实世界等都需要法律进行规制，人是不可能永远生活中虚拟空间内的，所以元宇宙的创造者和管理者代码与现实物理世界中的法律要进行更多深层次的

[35] 参见[加]亨利·阿尔斯拉尼安、法布里斯·费雪：《金融数智化未来》，王勇、黄红华、陈秋雨译，机械工业出版社 2021 年版，第 162-165 页。
[36] 参见于洋：《论个人生物识别信息应用风险的监管构造》，载《行政法学研究》，2021 年第 6 期。
[37] 参见于洋：《论个人生物识别信息应用风险的监管构造》，载《行政法学研究》，2021 年第 6 期。

互动，相互补强，共同管理，创造良好的元宇宙治理形态。法律介入元宇宙并不意味着抑制其自身的监管能力或行业自律，[38]而是提供一个秩序框架，确保个人生物信息的保护得以在虚拟与现实之间顺畅衔接。这种规制路径的设计与选择的有效性和合理性，需要在未来的实践中不断摸索和完善。

结语

元宇宙为个人生活和社会互动描绘了具有革命性的未来图景，也为个人生物信息的保护带来了前所未有的挑战。在虚拟化、跨界化、去中心化的元宇宙背景下，虚拟社交平台、在线教育互动、数字化医疗咨询和虚拟游戏等场景对个人生物信息的依赖性日益增加。在这些场景中，可能需要收集的个人生物信息包括面部表情数据、视线跟踪信息、心率监测数据、甚至是神经生理反应等，这些信息并不一定具有“已识别个人身份”的“唯一性”，但可以通过“间接关联”识别出用户身份。由于元宇宙沉浸式技术下收集的个人生物信息在当前法律体系中还没有明确的分类，只能根据其形式特征归类为“一般敏感个人信息”。结合个人生物信息在元宇宙中的平台技术风险、信息管理风险、跨国利用风险、去中心化追责风险，应拓宽“个人生物识别信息”的法律概念，将“可识别”纳入其概念范畴内，以提供更加全面、可预测性的保护。结合区块链技术建立去中心化身份，通过确保用户对其数字身份的完全控制权，增强对其个人生物信息的保护。完善“My Data”数据模式，用户可以选择和切换运营商服务，从而降低服务提供商锁定的风险，强化自身的数字主权身份。

本文的研究是想为保护元宇宙中的个人生物信息寻找现有法律体系内的可能性，拓宽法律概念的边界，结合数据时代浪潮下的已有经验，尝试为构建未来的元宇宙生态提供平衡技术进步与个人权利保护的发展性视角。目前对于元宇宙的构想在很大程度上还没有成为现实，对其法律问题的研究仍然是“不接地气”的，难以跳脱出当下固有认知与环境的限制。但这并不意味着对于元宇宙问题的思考是无意义的，元宇宙的许多理念与数字或数智时代不谋而合，或许在元宇宙的模型框架下可以窥见人类未来社会的一角，为智能时代提供一种新的可能性。

[38] 参见朱娟：《我国区块链金融的法律规制——基于智慧监管的视角》，载《法学》，2018 年第 11 期。