全民健身数智化转型背景下智能可穿戴设备用户数据隐私的保护

刘谢慈，林凯莉
（湖南工业大学 法学院，湖南 株洲 412007）

摘 要：为优化智能可穿戴设备在全民健身数智化转型中的应用模式，系统梳理其在健身场景转换中的应用现状后发现，智能可穿戴设备在用户数据隐私的保护上存在数据分级保护机制难以落实、知情同意原则实质架空、用户数据隐私保护意识薄弱、传统数据隐私保护方式滞后等困境，并据此提出优化数据场景化分级保护机制、加强动态知情同意体系构建、完善隐私保护用户共治模式、改进隐私保护技术等数据隐私保护构想，进而推动全民健身数智化的规范有序发展。

关 键 词：体育法；全民健身；智能可穿戴设备；数据隐私；数智化
中图分类号：G80-05 **文献标志码：**A **文章编号：**1006-7116(2024)04-0064-09

The protection of data privacy for smart wearable device users in the context of digitalization transformation of national fitness

LIU Xieci，LIN Kaili
(School of Law，Hunan University of Technology，Zhuzhou 412007，China)

Abstract: In order to optimize the applicable mode of smart wearable devices in the digitalization transformation of national fitness, and systematically combed the applicable condition in the transformation of fitness scenarios with it, and then finds that in the protection of users' data privacy in smart wearable devices shows the following difficulties: the difficulty in implementing the hierarchical data protection mechanism, the substantive overhead of the principle for informed consent, the weak awareness of users' data privacy protection, and the lag of traditional data privacy protection methods. Hence, this paper proposes data privacy protection concepts such as optimizing the data scenario-based hierarchical protection mechanism, strengthening the construction of dynamic informed consent system, improving the co-governance model of privacy protection users, and also improving privacy protection technology, so as to promote the standardized and orderly development of digitalization for national fitness.

Keywords: sports law；national fitness；smart wearable devices；data privacy；digitalization

2021 年 8 月国务院印发《全民健身计划(2021—2025 年)》指出，要“提供全民健身智慧化服务”“支持开展智能健身、云健身、虚拟运动等新兴运动”。体育总局办公厅于同年 10 月随即印发《“十四五”体育发展规划》,在强调推动全民健身数智化发展同时提出“推进‘互联网+健身’‘物联网+健身’”的重要部署。在此背景下，智能可穿戴设备因其可以帮助人们改变身体活动行为，提高训练的依从性，促进和刺激积极的生活方式[1]，提升全民健身公共服务供需适配性，被视为助力全民健身数智化转型的重要手段。智能可穿戴设备是人工智能技术与物联网技术相结合的重要科技产物，常见的类型包括智能手环、智能手表、智能眼镜、智能运动鞋等。这些设备通常是将传感器、芯片等硬件嵌入普通运动设备中，使其获得健康数据采集、数据分析、行为指导等功能，从而实现运动行为监测、辅助用户科学健身的目的[2]。在全民健身数智化

收稿日期：2023-12-14
基金项目：湖南省哲学社会科学基金项目(21YBQ067)；湖南省教育厅科学研究重点项目(23A0421)；湖南省体育局科技项目(2023KT0107)。
作者简介：刘谢慈(1990–)，男，副教授，博士，硕士生导师，研究方向：体育法学、诉讼法学。E-mail：liuxieci@qq.com

转型中，智能可穿戴设备常用于公众运动数据记录、生理数据分析、健身方案推荐、健身行为指导、健身数据交流分享等方面，中国田径协会与华米科技共同成立的田径运动联合实验室就是智能可穿戴设备在全民健身数智化转型中应用的典型代表[3]。

然而，这些智能可穿戴设备在推动全民健身数智化转型的同时，也暴露出一个值得关注的问题——设备在使用过程中会实时采集用户心率、血压、睡眠这类涉及用户生理健康、疾病状况等具有高度隐私性的个人数据信息，类似数据大多与个人生理状况直接相关，是与特定个人相关联、反映个体特征、具有可识别性的符号。与传统健身场景中用户主动向健身机构提供的个人数据相比，智能可穿戴设备的数据采集行为具有实时自主性、精确性和整合性，其直接以身体监控为目的，涉及的个人健康数据表现出高度敏感性[4]。目前，对智能可穿戴设备应用中数据隐私保护的研究集中于分析医疗型可穿戴设备可能涉及的数据隐私安全问题及其保护方式[5]。鉴于此，本研究从智能可穿戴设备在数智化健身场景中的应用入手，探究智能可穿戴设备在全民健身数智化转型进程中的应用优势、应用风险、保护困境以及用户数据隐私的保护路径，以期扩充智能可穿戴设备中数据隐私保护的研究场景，完善全民健身数智化转型中用户数据隐私的安全保障，推进全民健身数智化建设。

1　健身场景转换中智能可穿戴设备的应用现状

1.1　智能可穿戴设备在数智化健身场景中的应用优势

全民健身数智化转型是借助数字智能技术实现全民健身公共服务体系中的技术内嵌、认知革新、价值耦合，从而转换全民健身公共服务体系治理范式的动态发展过程[6]。在这个转型过程中，通过智能可穿戴设备、VR 虚拟现实技术等场景要素的介入，进一步整合各类用户与场景资源、拓展健身空间，健身活动场景由线下逐步转换为线上线下同步进行。智能可穿戴设备因其较低的价格和简易的操作模式成为助力全民健身数智化场景转换的理想载体，在优化健身服务供给上体现出多元价值。与传统健身模式相比，通过智能可穿戴设备赋能实现健身场景转换的数智化全民健身模式具有便捷化、个性化、精准化的特征[7]。首先，智能可穿戴设备具有便携性及附身性特征，用户只需佩戴智能可穿戴设备即可在无感状态下实现对健身行为的记录。用户可随时通过智能可穿戴设备获取运动时间、运动轨迹等运动大数据以及心率、能量消耗等生理大数据，实现便捷化健身管理。其次，个体的健身目标、运动习惯、身体机能各有不同，而传统健身方式同质化严重，无法满足个性化的健身需求[8]。智能可穿戴设备基于对用户健身行为特征的捕捉分析，并结合用户所提供的健身目标及健身偏好等，可以生成具有针对性的健身方案，相较于传统健身模式更具个性化。最后，传统健身模式较为重视健身的“习惯化”和健身训练的反复性，忽视适时的动态调整[9]。智能可穿戴设备通过对全健身过程的追踪记录能形成可视化健身数据，持续追踪用户各项指标变化，完善用户健身数据库，依据动态化数据对健身模式进行适时调整，实现精准化健身。

1.2　智能可穿戴设备在数智化健身场景中的应用风险

智能可穿戴设备的逻辑架构包括场景感知、传感器信号处理、智能系统数据处理 3 个阶段(见图 1)，其对全民健身赋能的基本原理是用户主动使用智能可穿戴设备进行健身行为记录，利用智能可穿戴设备的传感器进行场景感知，在对感知到的外界刺激进行处理后通过生物传感器将生理信号转化为电信号，最后采用 Wi-Fi、蓝牙或其他小范围通信协议等发送到终端处理器，并在处理器中进行数据计算分析从而实现数据反馈，为用户提供健身行为记录、健身指导等服务。在智能可穿戴设备的逻辑架构中，用户数据是连接各环节的重要对象，数据流动的过程相较于传统健身模式在空间范围和时间长度上都存在延伸，故数据的安全保障工作相较传统健身模式更为重要。然而，从智能可穿戴设备的应用现状来看，数据非法采集、数据泄露的风险居高不下。

其一，在硬件安全方面，智能可穿戴设备需要通过大量的传感器来感知并处理外界刺激，这些传感器的安全性是否得到保障关系到智能可穿戴设备用户的数据隐私安全。有研究发现，部分可穿戴设备中的传感器存在着未经用户明确同意而持续收集用户各种数据的情形[10]。作为智能可穿戴设备必备的核心组件，陀螺仪也被证明存在窃听风险，其能通过测量智能可穿戴设备周围环境中的声学振动，利用机器学习和信号分析处理技术对用户语音信息进行还原，这就增加在无法访问真实麦克风的情况下窃听电话附近语音的可能性[11]。这类硬件安全问题使得智能可穿戴设备赋能全民健身数智化转型时，出现对用户数据过度采集、非法采集、非法共享等数据隐私安全威胁。

其二，在软件安全方面，智能可穿戴设备内存资源的有限性使得工程人员只能采用轻量级的隐私保护措施。传统的隐私保护措施无法直接部署在智能可穿戴设备有限的存储空间中。诸如数字签名等隐私保护技术必须经过轻量化改造后才能应用于智能可穿戴设备中[12]，而轻量化后的系统在风险管理的范围和深度

上都将受到一定的削弱。同时智能可穿戴设备必须依托于一定的操作系统，而目前智能可穿戴设备的操作系统，例如 Andriod 等高度地暴露于已知的零日漏洞之中，智能可穿戴设备对于这些漏洞的继承大大降低其中的用户个人数据隐私安全性[13]。这类软件安全问题使得智能可穿戴设备在赋能全民健身数智化转型时，出现数据安全保护措施薄弱、数据库易被攻破、数据泄露现象频发等数据隐私安全威胁。

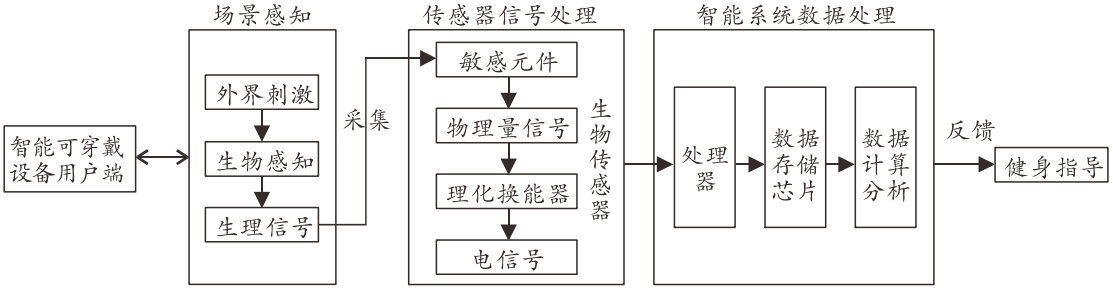

图 1 智能可穿戴设备逻辑架构

2 智能可穿戴设备应用中数据隐私的保护困境

目前智能可穿戴设备被广泛应用于全民健身、医疗监护、休闲娱乐等诸多场景，用于记录用户身体行为从而为用户提供精准化服务。伴随着大量数据被智能可穿戴设备所采集分析，用户数据隐私是否能够得到保障成为其在不同场景应用过程中必须考虑的问题。由于全民健身场景中产生的数据内容具有特殊性，加之健身大数据的迅速发展，使得此场景中用户数据隐私保护相较其他场景面临一系列现实困境。

2.1 机制层面：法律留白造成数据分级保护机制难落实

基于深入分析公众健身需求、监测健身状态、推送健身信息等目的，智能可穿戴设备赋能下的数智化全民健身服务需要广泛采集用户身份信息、位置信息、运动习惯等数据，该过程所涉及的数据不仅包括可穿戴设备用户的身份信息、生理信息、健康信息、位置信息等与其自身直接关联的数据信息，也包括用户个人数据以外的周围环境数据。相较传统健身模式下所采集的个人数据，通过智能可穿戴设备所采集的数据体量更为庞大，数据范围更为广泛，而数据采集的特点决定在全民健身数智化转型中应对这些数据进行更为严密的保护。为平衡此过程中的数据利用与保护，应按全民健身活动中所产生数据的敏感程度对其进行保护。从现有法律对个人信息分级保护的趋势来看，2020 年出台的《民法典》提出对于个人信息和个人私密信息的分别保护，2021 年出台的《个人信息保护法》也在个人信息处理者义务中要求个人信息处理者应对个人信息实行分类保护。这些规定虽构成我国个人信息保护的基本框架，但作为基础性法律，其对个人信息分类标准、敏感信息的识别等仅做出原则上的规定，缺乏对实践层次的具体指导。可见，相关实施细则和配套制度的匮乏对可穿戴设备所收集的全民健身数据分类分级保护机制的落实造成阻碍。倘若个人信息分类分级保护制度无法落实将会导致用户个人数据难以得到精细化的管理与保护，个人数据的泄露、滥用风险也将难以得到管控。

2.2 平台层面：平台霸权实质架空知情同意原则

知情同意原则是全民健身数智化转型中保护用户个人隐私的核心原则，数据处理者利用智能可穿戴设备对用户的相关信息进行采集、传输、交互等一系列操作时，必须告知用户其处理信息的目的、方式等并获得用户的同意。但在实际操作过程中，知情同意原则的应用存在着一系列困境。

1)隐私条款的平台导向致使用户知情权受限。

相较传统全民健身数据收集模式的线下告知、人工说明方式，借助智能可穿戴设备进行的数智化数据采集模式通常以设备内置的用户隐私协议对数据采集范围、目的、处理方式等进行告知。而智能可穿戴设备的用户协议的篇幅往往较大，界面偏向于平台友好型，对隐私条款的表述较为笼统，甚至存在隐瞒部分信息处理风险的情形，用户难以自主决定其信息如何被处理，所以用户的自决权被削弱。智能可穿戴设备中的部分软件还存在用户初始登录界面未显示或弹出隐私政策的问题，用户难以了解其隐私协议内容，知情权受到大幅限制。

2)平台地位优势致使用户同意权受限。

传统健身模式下，体育职能部门对公众健身数据的采集往往通过问卷调查、线下访谈等形式进行，所获取的公众健身数据以公众的积极配合为前提，即在体育职能部门收集数据时已经过公众自主同意，公众对数据收集行为能充分行使同意权。而借助智能可穿

戴设备进行用户健身数据采集时，相关数据的收集、处理规则在用户使用前已嵌入设备内部，即用户进入可穿戴设备平台时就必须与平台方签订一系列关于个人数据收集、处理等条款。在这种模式下，可穿戴设备的平台方处于优势地位，用户想要接受更优质的全民健身服务就必须接受这些条款，一旦其拒绝这些条款就面临着无法使用设备的困境。用户为了能够正常使用智能可穿戴设备一般都会进行广泛授权，难以真正自主选择是否同意其收集、处理信息。

3)知情同意原则未贯穿数据生命周期致使用户数据掌控权丧失。

全民健身数智化转型中，体育职能部门需对借助智能可穿戴设备所获取的数据进行处理分析乃至二次处理。对比传统全民健身模式下的小范围数据，数智化全民健身模式由于涉及的数据规模庞大，数据流转度进一步提升，数据可控性下降[14]，因而难以通过一对一告知的方式持续向用户告知数据处理方式及处理结果。此时通过智能可穿戴设备平台向用户进行数据跟踪汇报，并获取同意成为一个可行之策。然而，智能可穿戴设备中的用户协议、隐私协议集中于数据收集阶段、数据反馈阶段，而对收集后的数据将会受到何种处理以及处理的方式较少提及，这使得知情同意原则没有发挥出规范信息处理过程的具体功能。体育职能部门为了能够更好地利用数据，需对已收集到的用户信息进行二次处理以及内部共享，在此过程中理应获得用户的二次许可，而由于全民健身数据处理的高频次性、场景复杂性等特征，使得无论是通过智能可穿戴设备平台进行同意获取还是由体育职能部门直接告知都将极大影响全民健身数据的利用效率，导致实践中各类数据未经二次授权即进行二次处理或通过“一揽子”同意的方式限制用户权利的现象比比皆是，用户自其数据被收集后即丧失对自身数据的掌控权。

2.3　用户层面：隐私疲劳诱生用户隐私保护悖论

全民健身数智化转型的顺利进行，与公众的积极参与紧密相关。公众通过智能可穿戴设备对自身数据进行记录、追踪，将原本无法作为客观思考对象的用户活动与体验通过数据化呈现[15]，从而量化自我实现对自身的深度认知和有效管理，为全民健身数智化转型提供重要的数据支撑和政策参考。在此过程中，用户健康信息、行为习惯等个人隐私信息不可避免地处于智能可穿戴设备平台的技术凝视之下。一方面用户渴望通过智能可穿戴设备接受更高水平的全民健身服务，另一方面又充满对自身数据隐私泄露的担忧。此时用户的隐私关注行为和隐私疲劳行为不仅形成数据隐私保护上的悖论，还进一步影响用户参与全民健身活动的热情。

1)隐私管理难降低用户自我防护意识。

与数智化全民健身模式相比，传统全民健身模式中所涉及的数据范围较小，数据内容敏感程度较低，隐私管理方式简单，用户可通过拒绝提供隐私数据等方式对自身数据进行保护。但随着全民健身数智化的推进，智能可穿戴设备中数据富集、关联和共享导致在线隐私管理日益困难,用户隐私设置操作日趋复杂。冗长的隐私保护协议、复杂的隐私权限管理设置以及大量泄露的信息致使用户开始质疑自己是否有能力保护好自身的数据隐私，甚至对数据隐私保护问题采取类似“默认同意”的放任自由的态度[16]。这种放任自由的心态降低用户对隐私保护的主观能动性，使得体育职能部门及智能可穿戴设备的平台方无法及时根据用户的反馈对隐私政策进行调整，同时也减少其所受到的用户监督。

2)隐私救济难致使用户放任侵权行为。

一方面，在借助智能可穿戴设备实现全民健身数智化转型的过程中，用户与数据处理者之间存在明显的信息不对称。由于用户缺乏相关专业能力、数据处理者掌控关键技术等原因，加之智能可穿戴设备使用过程中的隐私侵权行为具有很强的隐秘性，用户往往只知道被侵害的结果，却无法得知自己的数据何时被泄露，故而在发生隐私侵权行为时用户难以提供足够的证据支持自己的诉求[17]。另一方面,《个人信息保护法》第 69 条虽规定，处理个人信息侵害个人信息权益造成损害，信息处理者应当承担损害赔偿等责任，但在智能可穿戴设备中健身企业对用户数据的处理并不一定会直接造成用户的财产损失，故用户难以通过此途径进行维权。在实际数据处理中，健身企业可以通过对用户健身数据的进一步挖掘与加工而获利，由于这种行为按照现有法律规制框架难以要求其承担侵权责任，导致用户遭受隐私侵权行为时难以寻求有效救济[18]。“救济难”导致用户即便遭遇侵权行为，大多也会因为潜在的维权成本和难以预估的维权结果而选择性忽略。

2.4　技术层面：技术局限导致隐私保护方式滞后

由于智能可穿戴设备本质上属于物联网范畴，具备物联网在信息安全方面的不稳定性，其收集到的健康数据并不能直接产生价值，只有在收集特定主体的数据后进行分析处理，通过数据共享使相关数据在不同场景中应用，作用于不同利益相关主体，才能产生内在或者外化的价值力量[19]。这一信息利用过程中的数据流动以用户为核心，将用户使用期间所产生的数据作为流动对象，基于数据生命周期理论可将用户数

据的主要流动阶段分为数据采集、数据利用、数据存储等阶段[20]。

1)数据采集阶段的过度采集风险。

数据采集是智能可穿戴设备中数据流动的起始点。为了全面获取用户数据，智能可穿戴设备会对用户进行全方位精准化跟踪。当下许多智能可穿戴设备较少为用户提供数据存取控制权限，用户难以确定其数据采集范围,无法视情况决定部分数据的采集与否。同时,由于智能可穿戴设备往往不具备情景识别能力，在用户由公开场合进入私人领域时，极可能发生可穿戴设备未提醒用户而导致用户不愿被采集的隐私信息被迫上传。由此可见，倘若缺乏对智能可穿戴设备数据采集行为的合理性控制，用户的隐私信息可能面临被过度采集的风险。

2)数据利用阶段的外部攻击与匿名失效风险。

体育职能部门对智能可穿戴设备中的数据利用通常包括数据上传与数据集成两个环节。数据上传是体育职能部门获取智能可穿戴设备所采集的数据，实现数据利用的必经途径。智能可穿戴设备的数据上传常采用安全性较低的蓝牙、Wi-Fi、红外传输等路径[21]，Zig Bee 和 NFC 等少部分方式虽安全性更强，但存在网络不稳定和应用度不高的问题[22]。除却上传路径不稳定外，智能可穿戴设备在数据上传过程中还存在数据传输标准未统一、缺少数据分级安全保障措施等问题[23]。一旦数据平台受到外部攻击，其中的用户个人数据隐私将存在严重的泄露风险。数据集成是实现跨应用的数据集合与利用，从而实现信息共享与信息互动的前提基础。但随着机器学习算法的进一步发展，传统匿名技术因加密方式的简单性而导致数据匿名存在“失灵”风险[24]。

3)数据存储阶段的永久滞留风险。

由于智能可穿戴设备的计算和存储能力有限，大量用户的个人信息、运动记录等数据往往在第三方平台进行存储，而大部分的智能可穿戴设备并未授予用户查询、更正、删除信息或撤销同意的权限，以致于用户个人信息数据及隐私信息长期被存留于平台中。当用户的隐私信息流入云端后，无法仅通过切断电源或者关掉开关就可以“停止侵害”，隐私信息将会在不同主体间反复流动[25]。由于用户无法彻底地擦除其向智能可穿戴设备所提供的个人信息数据，这些在特定情境下收集的用户生理信息、健康信息等隐私信息将永久地滞留于储存平台，被无可预测地应用于其他目的和场景之中。

3 智能可穿戴设备应用中用户数据隐私的保护路径

以智能可穿戴设备推动全民健身发展是数字体育时代引领我国体育事业实现高质量发展的重要手段。为更好解决智能可穿戴设备在助力全民健身数智化过程中可能产生的隐私侵犯问题，亟需进一步完善智能可穿戴设备用户数据隐私的保护路径。

3.1 法律统筹：优化数据场景化分级保护机制

全民健身数智化转型中所产生的庞大健身数据敏感程度不一，相较传统全民健身场景更需对用户数据隐私进行精准化保护。对此过程中所收集的全民健身数据进行分类分级是精准保护用户数据隐私、协调各方利益的重要手段，有助于体育职能部门在利用用户数据推进全民健身数智化转型时平衡信息收集与利用之间的关系。

1)健全静态类型化数据保护机制。

由于智能可穿戴设备在用户隐私保护方面没有专门的指南，因此构建智能可穿戴设备所收集的全民健身数据分类分级标准，一方面应以数据利用流程及需求为参照，另一方面应以个人数据安全为价值取向，在促进智能可穿戴设备应用于全民健身活动发展的基础上维护用户数据隐私安全。具体而言，应以《民法典》和《个人信息保护法》等隐私权保护相关的法律法规为框架，细化智能可穿戴设备收集的全民健身数据类型，进行统一分类识别，在法律层面上构建逐层细化的智能可穿戴设备数据保护法律体系。可采取“定义+列举”模式，结合数据的可识别性和关联性对数据进行分类；可将智能可穿戴设备中的数据分为与个人隐私关联较深且具有可识别性的敏感数据、具有可识别性但与个人隐私关联较小的识别数据以及可识别性和关联性较弱的一般数据 3 大类[26]。敏感数据应包含用户为使用智能可穿戴设备所提供的地址、个人电话号码、用户系统账号等账户信息，智能可穿戴设备所采集到的用户睡眠、心率、脉搏等个人生理数据，用户在使用智能可穿戴设备过程中所产生的运动轨迹、运动时长、运动习惯等健身数据。识别数据应包括用户年龄、性别、身高等个人可识别信息。一般信息应包括智能可穿戴设备所采集到的诸如温度、湿度、噪音值等用户周围数据。在此基础上再以致害风险作为分级依据，可参考《健康医疗数据安全指南》中的五级分级法，将数据分为 5 种安全等级(见表 1)，对各类数据逐项展开敏感程度分析，确定数据泄露、非法使用或遭受其他非法侵害时可能影响的程度，最终确定该数据应该采取的安全保护措施级别。

表 1　智能可穿戴设备数据分级表

安全级别	含义	影响对象 个人合法权益	示例
一级数据	可完全公开使用的数据，包括可以通过公开途径获取的数据	无危害	例如可穿戴设备采集到的环境湿度、气温、海拔等周围环境数据
二级数据	可在较大范围内供访问使用的数据	较小危害	例如用户对外分享的健身数据、社交数据等自主公开数据
三级数据	可在中等范围内供访问使用的数据，如果未经授权披露，可能对可穿戴设备数据主体造成中等程度的损害	一般危害	例如用户姓名、身高、性别等仅具有识别意义的数据；经过部分去标识化处理但仍可识别的数据
四级数据	在较小范围内供访问使用的数据，如果未经授权披露，可能会对可穿戴设备数据主体造成较高程度的损害	较大危害	例如用户产生的非对外公开的健身数据；用户地址等可以直接标识个人身份的数据
五级数据	仅在极小范围内且在严格限制条件下供访问使用的数据，如果未经授权披露，可能会对可穿戴设备数据主体造成严重程度的损害	严重危害	例如用户产生的非对外公开的生理数据；用户指纹、声纹等生物识别信息；具有高度隐私性的其他数据

2)嵌入动态场景化保护机制。

智能可穿戴设备所收集的全民健身数据在利用过程中涉及个人健康管理、运动行为指导、公共卫生监测等场景，包含私人领域及公共领域，不同场景下用户数据的隐私判断标准存在一定区别，仅采取静态分级保护方式具有局限性。在场景理论下，个人信息保护的内在逻辑是动态地保护个人信息安全，在界定隐私信息以及界分一般个人信息时摆脱“全有或全无”的固定思维模式，根据数据处理行为发生时的具体场景进行综合评价，判断该处理行为针对的行为对象是否属于个人的隐私信息[27]。具体而言，应解构智能可穿戴设备数据隐私的场景类型，细化在不同场景下的差异化规范内容，将智能可穿戴设备数据的利用场景以数据主体、数据处理者、数据处理目的、数据性质等维度进行场景划分，在此基础上选择适当的保护手段。例如，日常健康管理场景和运动指导场景所产生的用户数据性质存在一定的差别，因而对用户数据隐私保护力度也存在不同的需求。健康管理场景更注重对血压、心跳等用户生理数据的分析和处理，为实现数据处理的目的应授予数据处理者对生理数据较大的处理权限，适当降低对生理数据的保护等级，方便数据处理者对用户数据进行分析处理。此时，用户的识别信息、运动数据等由于与数据处理目的关联性较弱，应适当调高安全保护级别。相比之下，运动训练场景更关注用户所产生的运动数据，数据处理者需以用户广泛的运动数据为基础，故应适当降低运动数据的保护等级，给予数据处理者更大的权限。动态场景化保护机制充分关注用户的合理期待和容忍度，对数据处理风险进行实时评估，能够有机统一数据保护与利用，均衡用户与数据处理者之间的利益，多维度考察各方主体在数据生命周期中的责任分配，将保护用户数据隐私变成数据处理的前置要求。

3.2　平台规制：加强动态知情同意体系构建

在利用智能可穿戴设备实现全民健身数智化的过程中，用户知情同意权得到保障是保护其数据隐私的前提。《个人信息保护法》第 13~18 条对知情同意系统进行较为详细的阐述，但在智能可穿戴设备场景中仍应立足可穿戴设备数据处理的具体特点，从处理场景出发，全面动态地细化、完善智能可穿戴设备中个人数据处理的知情同意制度。

1)充分告知数据处理事项，提高数据处理透明度。

充分告知用户其个人数据的处理规则是确保用户知情权从而实现用户数据自决的前提。首先，体育职能部门利用智能可穿戴设备进行全民健身数据收集前，应告知用户数据的收集目的、处理方式、数据用途，以及在数据生命周期过程中用户数据可能遭受到的侵害及相关的救济方式，保证用户可以充分了解与其个人数据处理有关的情况及相应的风险。其次，应采用易读方式进行告知。体育职能部门应引导智能可穿戴设备厂商对隐私协议进行优化，从用户的角度出发采用清晰通俗的表达方式进行告知。例如采取分段式告知的方式，将篇幅较大的隐私协议进行分割，当用户操作涉及到相关隐私内容时再将该部分隐私协议以弹窗的方式告知用户。在协议内容上，有关部门应提供具有较强可读性的告知协议示范文本或为数据处理者编写隐私协议提供指导。最后，数据处理者可采用多元化的告知方式，鼓励用户积极了解与自身权益相关的数据处理操作。

2)完善分级动态同意体系，保障用户信息自决权。

目前常见的同意模式中，信息处理者往往采取一

次性同意的方式，通过“一揽子”协议要求用户在首次使用智能可穿戴设备时进行统一授权，对于后续的数据流转、数据二次利用等操作用户无法真正知情，更不具有自决权。为确保用户享有全过程的自决权，一方面应要求体育职能部门承担持续披露义务，通过直接告知或借助智能可穿戴设备平台进行告知，确保用户在不同阶段均有权选择是否允许处理者对其个人数据进行操作。在此基础上，要求智能可穿戴设备厂商增设“部分同意”的选项，允许用户可选择仅授权数据处理者收集、处理其获得享用服务所必须的数据，以防止数据处理者过度收集用户数据。另一方面应将同意规则与数据分级原则紧密相连，对不同级别的数据采用不同的同意标准。例如，需要对用户隐私信息进行处理(包括隐私信息的收集、一次处理、二次处理、对外流转)时，应通过弹窗等合理的告知形式取得用户单独同意和周期性授权后再进行处理，用户对个人数据处理授权同意具有有效期，在有效期过后如果用户未进行再次授权，则应视为用户取消授权。通过信息处理者与用户之间的双向交流，用户可根据个人偏好选择知情同意的方式同意或取消对数据的授权，有利于用户实时了解个人数据的处理情况，从而弥补原有概括同意模式中用户无法掌握信息流向的弊端。

3.3 用户协同：完善隐私保护用户共治模式

在全民健身数智化的浪潮下，可穿戴设备产生的隐私信息体量愈发庞大，而用户隐私保护意识的薄弱使得用户数据隐私遭受风险，为利用用户隐私信息牟利者提供可乘之机。为加强用户数据隐私的保护，应引导用户积极参与，形成用户与数据处理者之间的双向反馈，提高隐私保护实效。

1)提高用户自我防范意识。

智能可穿戴设备的用户作为数据的生产者，是核心隐私相关者[28]，也是数据隐私安全风险的最终承担者，其对自身隐私的重视程度深刻影响着数据隐私的保障效果，因此在保护用户数据隐私的过程中，亟需各关联主体协助用户树立正确的隐私保护观念。对健身企业而言，一方面应在隐私协议中、用户协议中强调用户数据的重要性以及其处理行为对用户数据的影响，引导用户提高对自身数据的重视程度；另一方面通过在智能可穿戴设备中内置隐私保护教程及隐私管理教程的方式向用户进行隐私教育，提高用户自我防范意识。对工信部门而言，应充分利用国家网络安全宣传周等契机加大宣传力度，在全社会形成良好的隐私保护氛围，利用社交网络平台的接口与宣传作用，加速推进公民隐私素养的提升，从而促使可穿戴设备的潜在用户养成隐私自治习惯，提高隐私自我保护水平；对用户自身而言，应拓宽“事前保护”+“事后保护”的认知视野，加强隐私自我保护意识。在“事前保护”方面，用户应通过接受数字素养培训等途径对个人信息权、医疗健康信息保护政策、数据隐私保护制度等形成一定的基础认知，养成在使用智能可穿戴设备前仔细阅读隐私条款的习惯，通过审慎核查条款充分了解智能可穿戴设备采集隐私信息的范围、方式、用途及权利保障等方面的内容，尤其注意个人信息的使用范围和使用目的。在“事后保护”方面，一旦用户发觉自身数据隐私被泄露或非法使用，应积极寻求救济路径以维护自身合法权益，如及时向相关部门进行投诉，要求智能可穿戴设备厂商停止不当行为并采取补救措施等。当有关部门的处理无法弥补自身损失时，用户应通过仲裁或诉讼的方式寻求进一步救济。

2)完善个人数据同意撤回机制。

《个人信息保护法》第 15 条、第 16 条规定个人信息处理的同意撤回权以及信息处理者的义务，但规则较为简略，尚未形成系统性的同意撤回权机制[29]。同意撤回机制是指用户在约定或法定的允许撤回个人数据情况发生时，有权要求数据处理者无条件删除其个人数据的机制。通过细化个人数据同意撤回机制的实施程序、具体内容、行为后果，厘清相关的定义、标准、边界，为保护智能可穿戴设备中个人数据隐私提供监管基础。个人数据同意撤回机制的建立有助于改善用户的弱势地位，促使数据处理者谨慎对待用户数据，加强对用户隐私信息的保护。在完备的用户撤回权机制之下，数据处理者为获得用户持续、稳定的信息授权，定将更加重视用户体验，提高对用户个人信息保护的关注度。数据处理者应充分履行告知义务，明确告知用户其所享有的权利，使得用户认识到同意撤回权的存在，不得对用户行使同意撤回权增设限制条件，明确向用户表达撤回权的具体内容以及其行使撤回权的后果，并提供便于操作的撤回窗口或撤回选项，使用户能够便捷实现个人数据同意撤回权。在用户撤回同意后，数据处理者应立即停止收集用户数据并对已经收集处理的数据停止处理，确保同意撤回权的有效性。

3)优化侵权举证及追责机制。

由于智能可穿戴设备用户与数据处理者之间地位不对等，智能可穿戴设备用户数据隐私被侵害后面临着举证困难、维权成本高、维权效果差等问题，削弱用户维权意识，故应优化用户数据隐私的救济路径。一方面，应合理分配举证责任。由于可穿戴设备用户与数据处理者之间存在信息鸿沟，导致用户难以对其侵权行为进行举证。数据处理者应在内部建立内部数

据合规机制，在日常数据处理中进行合规整改。如此一来，既可以在日常数据处理工作中贯彻数据保护理念，又可以在用户数据隐私受到侵害时提供证据支持。结合《个人信息保护法》第 69 条中规定的个人信息侵权行为适用过错推定的归责原则，一旦用户数据隐私出现损害，通过举证责任的合理分配有效维护用户权益。另一方面，国家应加大个人数据隐私受到侵害后的法律救济力度，加大对违法行为的打击力度，加强侵害个人数据隐私的法律追责体系[30]。在全民健身数智化的过程中，用户的健身数据具有极大的潜在价值，其中所蕴含的隐私信息更是关系到用户重大利益，巨大的经济利益面前较低的违法成本很难对健身企业产生震慑作用。为进一步保护用户的数据隐私，应提高损害赔偿标准，设置惩罚性赔偿制度，加大对健身企业违法收集、利用用户数据的约束。

3.4　技术革新：改进隐私保护技术，全流程加强数据安全

仅通过制度化的方式无法解决由于技术而引发的问题，全民健身数智化转型中由于智能可穿戴设备本身技术局限而引发的隐私风险应通过技术的改进来弥合。就智能可穿戴设备中的用户数据而言，其数据流动周期涉及多方主体，每个环节都存在隐私信息泄露风险，故应立足于数据生命周期理论采取相应技术手段予以应对。

在数据采集阶段，应限制数据采集范围，嵌入自动场景切换设置，将用户在使用智能可穿戴设备过程中可能面临的复杂场景风险提前在设备中植入，当用户由公开场所进入私密领域时自动切换至弱收集模式，降低用户隐私信息过度收集的风险。同时可采用匿名技术生成与用户相对应的密钥用来切断用户与隐私信息之间的直接联系，将用户标识信息与用户的敏感数据分别储存，使得第三方无法通过数据推测用户身份，平衡用户数据的隐私性和数据可用性之间的关系，从而有力保障用户的数据隐私。

在数据利用阶段，上传数据时可采用文本、图像加密等技术构建具有安全行动性的数据传输系统，通过数字签名、密钥验证等方式对传输过程进行加密，通过单向哈希函数更新用户匿名信息，保证用户身份隐私。集成数据时可采用基于属性集加密、层次性属性集、角色时空访问等访问控制技术，建立基于角色的访问控制与动态的访问控制相结合的访问控制模型，对数据处理者的访问行为进行控制、记录，从而限制数据处理者对数据的越界使用。同时通过规定匿名认定标准、数据脱敏标准来确保匿名行为的有效性，通过匿名安全审计的方式对匿名效果进行核验，确保用户数据得到真实匿名处理。此外，可采取 K–匿名、T–close 匿名等多种匿名技术去除用户识别信息，通过动态匿名方式保证用户标识性信息与隐私信息的分离。

在数据存储阶段，一方面可以借助访问控制模型对数据访问者进行记录，防止用户隐私信息流入云端后无法追踪。同时通过乱码数据覆盖、随机化噪声处理等扰乱技术，防止销毁后的数据被他人通过技术手段回复，损害用户数据隐私。另一方面，可以采用防火墙技术与入侵检测技术相结合的方式，防止因外界攻击而造成用户隐私泄露。通过在网络层的对外接口控制来实现网络安全保护，最大限度阻止网络黑客访问可穿戴设备数据存储网站，防止网络中不安全因素蔓延至可穿戴设备服务平台而随意篡改、移动及删除重要个人信息，对来自内部、外部的攻击提供实时保护，从而在个人信息受到侵害之前进行拦截和处理，以进一步提高信息安全。

在全民健身数智化转型背景下，智能可穿戴设备可以满足用户多样化的健身需求，提供科学的健身指导。但若智能可穿戴设备收集的个人隐私信息得不到全面保护，或无法对侵害个人数据隐私的行为进行有效规制，将会造成体量庞大的个人隐私信息被无限制的收集、集成、交互、侧写，从而严重损害用户权益，违背国家的个人隐私保护政策。未来研究还需要进一步对不同体育场景中智能可穿戴设备的应用及隐私保护等问题进行精耕细作，以便更好地促进科技服务于体育事业的发展，为智能时代体育事业与科技融合筑牢根基。

参考文献：

[1] 陈骐，刘泳庆，肖书明，等. 当前我国体育工程领域的研发需求情况分析[J]. 中国体育科技，2021，57(4)：3-23.

[2]霍波，李彦锋，高腾，等. 体育人工智能领域关键技术的研究现状和发展方向[J]. 首都体育学院学报，2023，35(3)：233-256.

[3] 中国新闻网. 中国田协与华米科技成立联合实验室 大数据助力全民健身. [EB/OL]. (2020-05-09)[2024-01-19]. https://www.chinanews.com.cn/business/2020/05-09/9179636.shtml

[4] 满洪杰，郭露露. 可穿戴设备中的个人健康信息保护——以同意为核心的研究[J]. 法学论坛，2023，38(2)：121-131.

[5] 何晓琳，钱庆，吴思竹，等. 健康医疗可穿戴设备数据安全与隐私研究进展[J]. 中华医学图书情报杂志，2016，25(10)：32-37.

[6] 冯靖媛,李荣日. 全民健身公共服务智慧化转型升级的逻辑理路、现实样态与践行方略[J]. 沈阳体育学院学报，2024，43(1)：1-7.
[7] 朱元利，赵皎卉，蔡勇. 智慧健身服务的四元空间模型：内涵特征、理论框架、关键问题与解决策略[J]. 北京体育大学学报，2022，45(12)：43-55.
[8] 徐伟康，郑芳. 我国智能健身的发展：逻辑阐释、实践检视与促进对策[J]. 西安体育学院学报，2023，40(1)：69-77.
[9] 徐伟康,林朝晖. 人工智能与全民健身融合发展的价值逻辑、现实困境与优化路径[J]. 上海体育学院学报，2022，46(10)：9-22.
[10] DINCELLI. "Wearable devices and privacy concerns：Data collection，analysis，and interpretation[M]//. Devjani S，RUKHSANA A. Privacy concerns surrounding personal information sharing on health and fitness mobile apps. Hershey，PA：IGI Global，2021：83-111.
[11] MICHALEVSKY Y，BONEH D，NAKIBLY G. Gyrophone：Recognizing speech from gyroscope signals[C]// 23rd USENIX Security Symposium (USENIX Security 14). 2014：1053-1067.
[12] 刘强，李桐，于洋，等. 面向可穿戴设备的数据安全隐私保护技术综述[J]. 计算机研究与发展，2018，55(1)：14-29.
[13] 倪雪莉，王群，梁广俊. 智能穿戴设备的安全与隐私威胁研究[J]. 信息网络安全，2022，22(10)：98-107.
[14] 冯俊翔，郑家鲲. 数字技术嵌入全民健身公共服务负效应的形成与消解[J]. 体育学刊，2024，31(1)：1-9.
[15] 刘于思，杜璇. 在“量化自我”与“质化自我”之间：智能可穿戴系统技术实践中的数据解读与互动[J]. 湖南师范大学社会科学学报，2023，52(2)：123-133.
[16] 刘鸿莹，张春龙，曲靖野，等. 隐私疲劳视角下智能穿戴设备用户隐私信息保护行为的影响因素研究[J]. 情报科学，2022，40(7)：37-47+54.
[17] 阿力木江•依明. 大数据时代个人信息权益的私法救济困境及其反思[J]. 征信，2023，41(1)：50-59.
[18] 徐伟康. 困境与路径：智能健身模式下个人数据的保护[J]. 河北体育学院学报，2021，35(5)：1-5.
[19] 胡瑶琳，余东雷，王健.“健康中国”背景下的健康医疗大数据发展[J]. 社会科学家，2022(3)：79-87.
[20] 许天颖. 数据智能化规训：可穿戴设备的隐私风险与保护[J]. 江西社会科学，2022，42(12)：162-170.
[21] 吴丹，马乐. 基于可穿戴设备的医疗健康数据生命周期管理与服务研究[J]. 信息资源管理学报，2018，8(4)：15-27.
[22] 倪雪莉，王群，梁广俊. 智能穿戴设备的安全与隐私威胁研究[J]. 信息网络安全，2022，22(10)：98-107.
[23] 刘露，杨晓雷. 新基建背景下的数据治理体系研究——以数据生命周期为总线的治理[J]. 治理研究，2020，36(4)：59-66.
[24] 焦艳玲. 智能穿戴技术下的个人健康信息保护[J]. 福建师范大学学报(哲学社会科学版)，2023(5)：101-111+172.
[25] 许天颖. 人工智能时代的隐私困境与救济路径[J]. 西南民族大学学报(人文社科版)，2018，39(6)：166-170.
[26] 毕文轩. 论对可穿戴设备收集数据的法律定性及保护路径[J]. 中国科技论坛，2021，1(5)：156-167.
[27] 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[J]. 当代法学，2022，36(1)：3-14.
[28] 粟丹. 论健康医疗大数据中的隐私信息立法保护[J]. 首都师范大学学报(社会科学版)，2019(6)：63-73.
[29] 郭少飞. 论个人信息法律体系下的基因信息保护[J]. 暨南学报(哲学社会科学版)，2023，45(5)：59-72.
[30] 齐海晶，曲靖野. 智慧图书馆个人信息保护政策合规性评价指标体系构建与对策研究[J]. 情报科学，2022，40(12)：152-160.