困境与路径：智能健身模式下个人数据的保护

徐伟康

（清华大学 法学院，北京 100084）

摘 要：因人而异的智能健身服务以个性化的个人数据采集与利用为基础，其在为用户提供科学指导、带来便利的同时，也易产生各类数据安全问题。认为，传统的“可识别性”个人数据界定与保护方式已失效，“知情—同意”原则被冗长专业的条款架空形同虚设，数据背后的经济价值归属争议引发“控制性”危机，相关立法和司法的滞后难以提供法律保障，智能健身个人数据保护问题亟待解决。提出，要坚持强化数据主体的控制这一总原则，坚持明确治理主体，完善事后救济的监管路径，坚持以技术为支撑，完善技术解决方案的市场路径，最终形成法律与技术双管齐下、相互配合的“监管—技术”的双重保护路径，以更好地保护健身领域的个人数据。

关键词：智能健身；个人数据；保护；知情—同意；监管；技术

中图分类号：G80-05 **文献标志码：**A **文章编号：**1008-3596（2021）05-0001-05

2017 年 7 月，国务院发布《新一代人工智能发展规划》，将人工智能产业发展纳入国家战略。2019 年 8 月国务院办公厅印发《体育强国建设纲要》，明确指出要推动全民健身智慧化发展，鼓励社会力量建设智慧健身中心、智慧健身馆。在政策和需求的双重推动下，应用人工智能、物联网、大数据等新兴技术的智能健身模式应运而生，我国健身行业迎来大发展，截至 2018 年 8 月，智能健身房在国内出现了近 110 家，根据艾瑞咨询机构发布的相关报告分析，预计未来 5 年，智能健身房的年复合增长率将维持在 12%左右[1]。智能健身为人们带来便利的同时，也造成了大量高度敏感的个人数据，尤其是个人健康信息、个人行踪轨迹数据主动或被动地暴露在智能健身程序中。过度收集、不当存储、未经授权的披露和其他严重侵害个人数据的行为频发。本文结合近些年来我国智能健身的发展情况，总结现行的个人数据保护模式和司法实践遇到的诸多问题，旨在构建智能健身个人数据保护路径，使人们在享受智能健身“善假于物”的便利的同时，也能维护个人数据的安全。

1 智能健身的兴起及其对个人数据的侵犯

1.1 智能健身的概述

目前学界对智能健身缺乏统一的定义。瞿迪认为人工智能化体育用品能够在保留基本功能的前提下，主动对用户身份进行识别，对用户使用习惯进行分析和学习，结合体育科学的知识对用户期望进行优化。人工智能运动产品，可以产生个性化指导方案，进行科学的反馈[2]。产业届曾提出智能健身的核心标准是“三合一”，即 App 程序、SaaS 系统、物联网硬件，也就是前端、后台、硬件或互联网＋物联网。前端供用户购买，预留服务和查看数据，通过物联网硬件实现基本功能，收集数据、传输数据，SaaS 系统执

收稿日期：2020-12-17

基金项目：国家社会科学基金重大项目“《中华人民共和国体育法》修改重大问题的法理学研究”（18ZDA330）；福建省社科项目“健康中国背景下福建省社区体育发展模式研究”（FJ2018B105）

作者简介：徐伟康（1994—），男，浙江台州人，在读博士，研究方向为体育法学。

文本信息：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.

行更复杂的数据管理，将消费者和运营商连接起来[3]。智能健身中的“智能”主要体现在两方面。一是场地的无人管理，通过人脸识别和手环刷卡等技术区分用户。用户通过App预约场地、课程，可以自主进入场馆，启动设备，如智能储物柜、智能灯等。二是设备的智能化，通过智能检测设备、运动可穿戴设备等掌握用户在特定运动场景下生成的数据，并通过算法与机器学习帮助用户量身制定课程，提供针对性训练。本文结合学界和产业界的概述以及智能健身的特点，认为智能健身是指科技健身，依靠人工智能和物联网进行场馆管理，利用大数据分析进行实时监测和反馈，具体包括场馆的智能化设计、健身前的智能化检测、健身过程中的智能化监测、健身后的智能化反馈四方面。

1.2 智能健身对个人数据的侵犯

个人数据是指可以直接或间接识别到自然人有关情况的任何数据，包括个人的身份信息、身体信息、心理信息、地点信息、行为信息、社交信息等等。个人数据的保护理论主要源于人格权学说，认为个人数据保护涉及隐私权等基本人权和自由，关乎人性的尊严与人格的自由发展。倘若自然人不能基于自主意思决定个人数据能否被他人收集、储存并利用，无权禁止他人在违背自己意愿的情形下获得并利用个人数据，则个人之人格自由发展与人格尊严就无从谈起，因此需要保障数据主体对个人数据在被他人收集、存储、转让和使用过程中的自主决定的利益[4]。

无人化、一站式服务大大提高了健身房效率，但是也面临个人数据泄漏的风险。以24h智能健身房为例，配备自助接入系统（包括人脸识别），让用户完成从“刷脸入场—自助存储—自主训练—数据记录—离开场馆”一系列的自助服务。用户从一进入场馆的人脸识别开始，个人数据就暴露在智能健身的系统下。每个人的身体状况不同，健身需求不同，健身方案亦不同。智能健身的第一步就是根据每个人的身体测评结果给出精确、科学的反馈。目前，几乎所有的健身房都采用了智能检测系统。软件系统如Kweenew系统，用户可在手机端登录系统，体验全面的身体测评，进行云端数据匹配，自动生成最佳训练方案。硬件系统如早期的Vento健身房，用户通过智能终端机进行身体扫描，读取用户身体的各项指标和肢节长度以及肌群柔韧度、灵敏度和弹跳力等数据，从而建立基础数据档案，教练据此并结合用户的训练需求提供指导服务。

智能健身过程离不开对运动状态的监测和反馈。很多智能健身房引入心率监测设备，甚至采用实时心率投射大屏幕来显示，同时计算卡路里等。根据Green Orange Technology提供的数据，从2017年5月到2018年5月底，使用心率系统的健身房的平均月增长率为20%，平均每个健身房每周使用40次，每次使用45分钟[5]。健身房还会通过监测乳酸阈值和肌肉中氧气供应和氧气消耗的动态平衡了解运动强度和有效运动时间[6]。健身结束后，所有运动数据自动上传到智能终端机，手环或者其他可穿戴设备与之配对，对用户的出勤、统计、练习、进程等数据进行统计分析并给出反馈。

智能健身最大的亮点是增强健身的技术性和数据性，将以前可有可无的数据实用化。用户的健身数据诸如心率、步数、动作、时长、燃脂效果都将被记录在智能设备中，形成个人健身数据库，使数据呈现更直观，帮助用户更好地实施健身计划。智能健身过程收集的用户数据往往高度敏感，包括个人身份数据、个人生物识别数据、个人健康生理数据、个人位置数据。智能健身依托AI技术形成精准的用户画像，利用这些数据支持促销决策，开展私教服务、营养品推荐等，甚至可能向黑灰产业链盗卖个人数据来谋利。

2 智能健身模式下个人数据保护的困境

2.1 “可识别性”个人数据界定方式的不足

从可识别性的角度看，个人数据是指已识别或可识别到个人（或称为数据主体）的任何数据。传统的通过可识别性界定、保护个人数据的方式在智能健身领域面临新挑战。一方面，可识别个人数据的范围不断扩大，从进入健身房或使用健身App开始，个人健身活动轨迹数据几乎都会被采集记录下来，零散的个人数据记录看似不重要，但通过整体的数据挖掘能够识别到个人，比如单纯的健身房跑步机的跑步记录不能识别到个人，但是与健身房的智能门禁、运动轨迹、心率、能量消耗数据联系起来就可以识别到个人。此外，个人数据不当收集或使用造成的损害是可累积的。数据控制者打包处理的一类个人数据虽然不以识别特定人为目的，但是类别化处理后也会对个人数据主体权利造成侵害，如很多

健身房根据用户训练数据和日常运动数据实时上传云端存储，经过分析加工后用来帮助其开展精准的营销推广。

2.2　“知情—同意”原则适用的无力

无论是《民法典》还是《网络安全法》等法律均强调，个人数据的处理必须经过数据主体的同意，“告知和同意”一直是各国个人数据保护法最重要的机制和原则。其以“理性人”理念为理论预设，该理论认为数据主体作为独立的理性个体，在知情的前提下，能够就是否同意他人收集、使用和转移个人数据做出最大化自己利益的决策[7]。由此认为只要数据主体是在知情的前提下收集和使用授权的数据，就假定数据控制者遵守了“知情—同意”原则。目前，数据控制者通常采用公共隐私政策和许可选项的标准化模型，以符合“知情—同意”原则[8]。根据南都个人数据保护中心发布的《1000 家常用网站及 App 隐私政策透明度测评》，智能健身类 App 普遍存在隐私政策不明显问题，一般来说隐私政策通常在用户注册页面可见，但是 App 采用各种方式规避，导致隐私条款经常被人忽视，此外默认勾选成为大多数智能健身类 App 的普遍现象。大多数数据主体对于专业冗长的隐私条款，并不具备深入阅读与理解的能力，面对频繁的数据授权请求，一般会不假思索地点击“同意”选项，实质上“知情—同意”权利被架空了。同时健身领域采集数据具有特殊性，由于每个人的健身方案不同，用户为了享受根据自己的身体“私人定制”的健身服务，不得不“出卖”个人的数据。

2.3　“控制性”理论的失效

传统个人数据法律保护的核心是个人对数据的控制，形成了以人格权和隐私权为依托的保护路径。在大数据时代，个人数据的经济价值越来越受到重视，个人数据的财产属性愈发突出，形成了个人数据财产权保护的路径[9]。为了获得健身服务，人们自愿或非自愿地贡献了个人数据，个人数据早已脱离了数据主体的实际控制。有观点指出，数据主体能控制的是数据背后的经济价值，那数据背后的经济价值究竟归谁所有其实存在争论。在健身领域中，除了单纯的年龄、性别、身高、体重、BMI 等基本数据，很多的健身数据是耗费健身用户一定的体力和脑力取得的，依照洛克的劳动价值理论，有关数据的经济价值归用户所有。但是健身房依靠智能设备对个人健身数据记录、采集，并进行大数据分析和机器学习，似乎也构成了劳动。从这个角度，健身房应该享有收集和利用健身用户的个人数据所产生的经济价值，但这跟个人数据的保护是完全相悖的。

2.4　立法和司法的滞后

目前我国个人数据保护的法律体系存在立法碎片化的问题，《网络安全法》《宪法》《刑法》《民法典》《消费者权益保护法》和相关司法解释都涉及个人数据保护。但每个部门法都有各自的立法目的和价值取向，现有的法律主要是应对互联网对个人数据的侵害问题，难以直接照搬到智能健身领域。实践中，个人数据保护主要以刑法规制或民法中人格权规制为主。刑法具有谦抑性，一味的刑法先行不利于数据治理格局的形成，严格的刑法规定也难免造成法律执行的空洞化和裁量空间的过大化，还会导致责任规范与行为规范的脱节问题。人格权的保护方式只针对公开公民隐私、侵害个人数据并造成损害后果的行为，对于数据主体在数据收集、存储和利用过程中的决定权、知情权、保密权和更正权，以及在未造成损害后果时获得救济的权利，都未在人格权体系下充分体现。实际上智能健身企业并不需要公开用户的个人数据来营利，而可以通过对用户健身数据进一步挖掘、深加工来获利。在这种情况下，按照现有的司法实践，其行为并不构成对数据主体的隐私等人格权的侵犯，不承担侵权责任，但这显然是不合理的。

3　智能健身下个人数据保护的路径选择

3.1　总原则：强化数据主体的控制

目前，诸多研究认为，构建个人数据保护体系，有必要区分个人数据的多重利益。如张新宝教授的“两头强化，三方平衡”理论，通过分类个人数据，实现数据保护和一般数据使用之间的平衡[10]。范为博士借鉴“欧美改革法案中‘情景’和‘风险’的路径”，认为数据控制者可以“在相应场景中”合理地收集、使用和流转个人数据[11]。此外，还有观点认为对于特定的个人数据，他人是否有权收集、储存和使用，应当根据当时的环境，从规范的角度进行判断[12]。这些理论的基础都认为在大数据时代，个人数据除具有人格利益外，亦具有极高的经济价值与公共价值。

个人健身数据敏感度强、识别度高，一旦脱离主体将不可避免损害人格权与人格尊严，必须站在严格保护数据主体的立场上，把权利理论作为数据保护的载体。个人数据是人的延伸，对其保护要回到个人控制中来。个人数据亦应当由数据主体掌控，体现个人的意志，建立在人的尊严基础上[13]。保障数据主体对个人数据的收集利用过程中的自主、自治、自决，应是智能健身时代个人数据保护的应有之义。具体而言，当智能健身房获取个人数据时，需要以数据最小必要为原则。《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》指出运动健身类移动应用最小必要信息仅包括：基本健康资料（性别、年龄、身高、体重），用于给出运动和健康建议；个人运动信息，用于展示运动过程状态；精准定位信息，用于实时确定用户位置和展示用户的轨迹；账号信息，用于标识用户。智能健身收集个人数据原则上仅限于以上必要的信息，在收集过程中要列明具体的功能场景，如训练反馈，以及与功能场景一一对应的个人数据收集目的、方式、范围，不仅需要用户明确、具体的同意，同时要赋予用户被遗忘权，用户有权随时删除智能健身应用上留存的数据。

3.2 监管路径：明确治理主体，完善事后救济

现代规制理论认为，一个产业要发展，既需要发挥行业自律，也需要加强政府“有形的手”。诸多个人数据泄漏事件的发生提示我们，个人数据“知情—同意”原则不能仅仅停留在企业自律层面，应该强调行政监管的作用。当前我国虽然有诸多部门涉及网络与数据监管[14]，但是根据职权划分，每个部门在履行职能时基本都只注重本部门、本领域的利益，导致数据安全漏洞不断。杨春然教授提出在国际奥委会等组织内部，应当单独设立专门的隐私保护委员会[15]，以保护运动员隐私。其实，不光竞技体育领域，在大众健身中也需要相应的数据监管机构，来明确监管职责。建议在省一级的群众体育主管部门加设一个专门的健身数据保护机构，明确个人健身数据的界定标准，规范健身领域对数据的收集和使用，做好事前预防。

此外，完善个人数据安全事件的事后救济措施同样重要。《网络安全法》第43条规定，公民发现自己的数据出现风险或有可能处于风险中时，可以自行启动自救程序，要求网络运营者删除、更正相关的个人数据，网络运营商也应采取措施删除或纠正它们。针对实际中网络运营商响应个人请求不及时，考虑建立“删除和修改”的应急响应机制，智能健身类应用企业应任命具体的数据安全负责人，以在发生数据安全事件时及时进行应对或开展补救工作。应急预案应当尽量覆盖可能发生的各类数据安全问题，包括但不限于内部上报、原因调查、数据恢复、影响评估、上报监管机构、通知受影响的数据主体等等。

3.3 市场路径：构建技术解决方案

智能健身的技术特征，决定了对个人数据的利用是一种可以用技术衡量的规范性操作[16]。目前，学界提出了多种技术解决方案：一是隐私增强技术（privacy enhanced technologies），增强隐私的透明性，使用户清楚自己在健身过程中什么数据被收集、将被用于何种目的、将储存多长时间，保障用户的“知情—同意”权。二是通过设计保护隐私（privacy by design），在产品设计中，将个人数据保护嵌入技术、物理基础设施、商业准则的设计标准中加以保护[17]。欧盟《通用数据保护条例》认为匿名化是经过处理后，单独数据无法识别到数据主体的处理方式[18]。应强制智能健身企业应用匿名化技术，尤其在传输前环节加强匿名化处理，注重隐藏用户身份和敏感数据，如此既能满足数据利用，又能防止数据与个人的关联。同时智能健身设备获取个人年龄、性别、身高、体重、BMI、心率、步数、燃脂效果、健身动作及时长等敏感数据应当本地化，禁止上传至企业云端。总之，智能健身模式下的个人数据保护，法律与技术两者缺一不可。要构建“监管—技术”的双重个人数据保护路径，不断完善，达到技术的便利与数据安全的最佳耦合状态。

参考文献：

[1] 智能健身房兴起，能否取代教练[EB/OL].(2017-11-12)[2020-01-20]. http://www.sohu.com/a/203882830_99916246.

[2] 瞿迪.人工智能化体育用品发展研究[J].体育文化导刊，2018(6):104.

[3] 智能健身房快烂大街了，你们对它有什么误解[EB/OL].(2018-08-17)[2020-01-20]. http://www.lanxiongsports.com/posts/view/id/12721.html.

[4] 徐伟康，徐艳杰，郑芳.大数据时代运动员数据的法律保护[J].天津体育学院学报，2019，34(5):456.

[5] 智能化健身之路该怎么走[EB/OL].(2018-07-01)[2020-02-20]. http://www.sohu.com/a/238720044_422035.
[6] 丰佳佳.健身产业智慧化发展在提速[N].中国体育报,2020-03-03(6).
[7] 齐爱民.个人数据保护法研究[J].河北法学,2008,26(4):15.
[8] 徐伟康,田思源.反兴奋剂活动中个人数据保护的研究[J].天津体育学院学报,2020,35(3):276.
[9] 刘德良.个人数据的财产权保护[J].法学研究,2007(3):80.
[10] 张新宝.从隐私到个人信息:利益再衡量的理论与制度安排[J].中国法学,2015(3):38.
[11] 范为.大数据时代个人数据保护的路径重构[J].环球法律评论,2016(5):92.
[12] 丁晓东.个人信息权利的反思与重塑:论个人信息保护的适用前提与法益基础[J].中外法学,2020,32(2):339.
[13] 高富平.个人信息保护:从个人控制到社会控制[J].法学研究,2015(5):84.
[14] 刘素华.大数据时代的公民数据信息安全规制问题研究[J].法治研究,2018(6):57.
[15] 杨春然.论大数据模式下运动员隐私的保护[J].体育科学,2018,38(2):82.
[16] 徐伟康.从《互联网技术影响下体育消费发展的特征、趋势、问题和策略》看疫情之后我国体育消费发展的新取向[J].体育学研究,2020,34(4):95.
[17] CAITLIN P H,NANCY M,MCGRAIL K M. Privacy by design at population data BC:a case study describing the technical,administrative,and physical controls for privacy-sensitive secondary use of personal information for research in the public interest[J]. J Am Med Inform Assoc,2013(1):25.
[18] 刘雅辉,张铁赢,靳小龙.大数据时代的个人隐私保护[J].计算机研究与发展,2015(1):229.

Dilemma and Path: Protection of Personal Data Under Intelligent Fitness Mode

XU Weikang

(School of Law, Tsinghua University, Beijng 100084, China)

Abstract: The intelligent fitness service is based on the personal data collection and utilization, which provides scientific guidance and convenience for users, and also easily produces various data security problems. The author thinks that the traditional definition and protection of "identifiable" personal data has been invalid, the principle of "inform-consent" has been performed practically no function by tediously long professional terms, the dispute of economic value ownership behind the data has caused a "controlling" crisis, the lag of relevant legislation and judicature cannot provide legal protection, and the problem of intelligent fitness personal data protection needs to be solved. It is proposed that we should adhere to the general principle of strengthening the control of the data subject, adhere to the clear governance of subject, improve the supervision path of expost relief, insist on the technology as the support to improve the market path of technical solutions, and finally form the dual protection path of "supervision technology" of law and technology, so as to better protect the personal data in the field of fitness.

Key words: intelligent fitness; personal data; protection; inform-consent; supervision; technology