智能家电与生成式人工智能大模型创新与发展白皮书

国家高端智能化家用电器创新中心
海尔智家 Haier smart home
CHEARI 中国家用电器研究院
科大讯飞 iFLYTEK
中国海洋大学 OCEAN UNIVERSITY OF CHINA
上海交通大学 SHANGHAI JIAO TONG UNIVERSITY
中国科学院自动化研究所 INSTITUTE OF AUTOMATION CHINESE ACADEMY OF SCIENCES
武汉人工智能研究院 WUHAN AI RESEARCH
HoT 和而泰

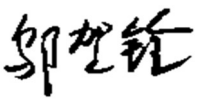
序言

生成式人工智能（AIGC）的发展和应用已开始显现对社会与经济的深刻影响趋势。在众多行业中智能家电将成为通过 AIGC 最直接赋能的行业之一，推动智能家电行业在新赛道上创新与升级，开辟智能家电行业发展新空间，为消费者提供更智能、便捷、个性化的产品和服务。智能家电产业链的拓展也将带动相关领域的产业发展并创造就业机会。本白皮书聚焦于探讨 AIGC 技术与智能家电结合的机遇与挑战、技术与应用、创新与发展。

中国作为信息产业大国，智能家电产业作为我国的优势产业之一，已经建立了较为完善的产业链体系，涵盖了研发、制造、销售和服务等多个环节，为 AIGC 技术的应用提供了广阔的应用场景和丰富的数据支持。这种独特的优势将为中国在智能家电与 AIGC 融合的可持续性发展奠定坚实基础，并为中国在国际智能家电市场中赢得竞争优势。中国智能家电产业通过不断创新和技术升级，抓住 AIGC 契机将不仅满足国内消费者对智能化产品的需求，还将拓展到海外市场。

然而，智能家电与 AIGC 融合也面临着数据隐私、安全和伦理等方面的挑战。正如本白皮书所指出的，只有坚持合规性原则，才能保障产业的健康发展。这需要制定和遵守相关法律法规，并加强数据安全管理和技术防护手段，有效确保数据的安全性和隐私保护。此外，通过制定更加完善的标准和规范，以透明和可信赖的机制，加强行业自律机制和监管及审查，为用户提供可信的智能家电产品和服务。白皮书呼吁，在“产业高质量发展”的国家战略的指引下，通过加强产学研合作，建设智能家电行业数据库和行业 AIGC 大模型，以推动人工智能在智能家电领域的创新应用，这不仅有助于智能家电行业的进一步升级，还将对智能家电行业上下游产业链产生积极的影响，提升我国在人工智能领域的全球地位。

本白皮书的发表为行业指明了前进的方向，促进产业链的紧密合作，推动智能家电与 AIGC 的融合，以科技创新的力量，为智能时代的到来创造更加璀璨的明天。



目录

1. 引言

2022 年底，ChatGPT 的出现，在短短 2 个月内就吸引了上亿用户，成为历史上增长最快的应用程序。同时，大模型技术也迅速在全球范围内蓬勃发展，通用大模型和产业大模型层出不穷。大模型中的训练参数数量从几十亿迅速增加到几万亿，并以惊人的速度持续发展，引起各国广泛关注。人工智能强国如美国、中国、欧盟等纷纷发布政策，旨在规范人工智能的健康发展。近年来，中国得益于互联网和创新政策，人工智能取得了巨大进步，但整体上仍处于发展初期。中国工程院院士高文曾指出，全球通用的 50 亿大模型数据训练集里，中文语料仅占 1.3%。在数据方面，中国迫切需要有头部企业牵头，建立起大模型的中文语料库和行业语料库，构建面向垂直领域的国产 AIGC 行业大模型开放平台，并赋能到周边产业。

人工智能的核心要素包括数据、算法、算力。大规模预训练模型，需要积累海量的数据，具备出色的算法解决能力，并投入大量的算力进行模型训练。国产通用大模型领域竞争激烈，AIGC 在垂直领域的应用主要以拼接式生成为主导，尚未构成核心场景。这意味着垂直领域仍然是 AIGC 技术的主要发展方向。中国在垂直领域拥有更多的数据来源和用户需求，可以为大模型的训练提供更多支持和指导。因此，中国应该尽快在具备优势的产业等垂直领域切入行业大模型。本白皮书强调，中国需要集中资源和人才，在垂直领域加速推进大模型技术的研究和应用。由国家级创新中心主导，通过与行业合作伙伴共同建立行业大模型平台，推动人工智能技术在不同领域的落地和应用。

智能家电产业作为中国的优势产业，在建立行业数据库和国产 AIGC 大模型方面具备了技术基础和市场需求。根据 GfK 中国测算 2022 年数据显示，中国智能家电市场近六年零售额年增长率达到 8.1%，领涨整体家电市场。2022 年，中国的智能家电渗透率达到 50%，远高于全球的平均水平 37%。这些数据表明，在中国制造和创新的推动下，智能家电市场迅速发展并取得了显著成果。中国智能家电产品在技术水平和市场占有率方面处于全球前列。同时，智能家电产业的

发展还辐射带动智慧家居、智慧家庭、智慧社区、智慧城市等多个相关产业。因此，建设智能家电行业数据库和国产 AIGC 大模型不仅能赋能本行业，还能对周边产业产生积极影响。

为了促进智能家电产业 AIGC 的健康发展，国家高端智能化家用电器创新中心联合产学研上下游机构和厂商等单位，发布以“建设面向智能家电产业的国产大模型开放平台”为目的的白皮书。通过智能家电通用大模型平台的构建，规范家电产业行业数据积累，加速大模型底层技术的发展，并探索国产 AIGC 助力智能家电进入 3.0 时代的有效路径，同时构建家电产业领域 ToB 端和 ToC 端垂直应用场景。

本报告共分为六个章节，之后的章节安排如下：第二章介绍智能家电产业的概况，阐述智能家电产品和服务的分类与特点、产业面临的挑战与机遇。第三章梳理生成式人工智能大模型的基本原理和核心技术，介绍国产生成式人工智能大模型的未来发展趋势，以及在行业细分领域的垂直应用前景。第四章介绍生成式人工智能大模型在家电产业的应用案例以及未来场景展望。第五章探讨人工智能时代智能家电产业面临的数据隐私和安全问题、伦理和法律合规问题，给出智能家电产业的合规性应对措施和建议。第六章从提升智能模型的能力、预测智能家电产品和服务的创新与变革、开放平台与生态合作等方面阐述智能家电产业与 AIGC 融合的未来发展趋势和前景。

2. 智能家电产业概述

2.1 智能家电的定义、市场规模和增长趋势

随着人工智能技术和物联网技术的不断发展，智能家电产业正逐渐崛起，旨在提升家居生活的便利性和舒适度，为用户带来更智能、绿色、健康的生活方式。近年来，中国智能家电市场呈现出快速增长的势头，随着智能家电逐步普及和消费者对其认知度的提高，智能家电产业迎来了更广阔的发展空间。展望未来，智能家电产业将继续朝着智能化、集成化、标准化的方向发展。它将推动智慧家庭和智慧城市建设，为人们打造更加便捷、舒适、智能的生活环境，打造一个智慧、互动、可持续发展的生态系统。

智能家电是将微处理器、传感器技术和网络通信技术融合到家电设备中，通过物联网、人工智能、大数据等先进技术的运用，将传统家电升级为智能化、自动化、互联化的新型产品。这些智能家电具备自动感知住宅空间和自身状态的能力，在提供服务的同时，也能接收和执行来自住宅内外用户的控制指令。

作为智能家居系统的重要组成部分，智能家电能与其它家电及家居相互连接，形成高度集成的智能家居生态系统。用户可通过手机 App、语音控制、智能遥控等方式实现远程控制和智能操作，以实现整个智能家居系统的功能。这种智能化的操作方式极大地提高了家居生活的便捷性和舒适度，使人们在享受现代科技带来的便利的同时，也能更加轻松地掌控家庭生活。

根据观研报告网发布的《中国智能家电行业现状深度研究与未来前景分析报告(2023-2030 年)》，2020 年我国智能家电市场规模达到 1907.4 亿元。2021 年我国智能家居市场规模维持增长态势，达 2131.2 亿元，增速为 11.7%。整体而言，我国智能家电行业已从单品智能化发展阶段步入家电系统智能化阶段，智能家电的智能水平持续提升。此外，2022 年《政府工作报告》提出了鼓励地方开展绿色智能家电下乡和以旧换新的政策措施。这将刺激乡镇农村地区的消费意愿，提升智能家电在下沉市场的渗透率，有助于进一步扩大市场规模。预计到 2025 年，我国智能家电市场规模将达到 3119.5 亿元。总体来看，智能家电行业在我国市

场有着巨大的发展潜力。随着技术的不断进步和政策的支持，智能家电的普及和应用将进一步提升。未来，智能家电将成为家庭生活的重要组成部分，为用户提供更智能化、便捷化的生活体验。

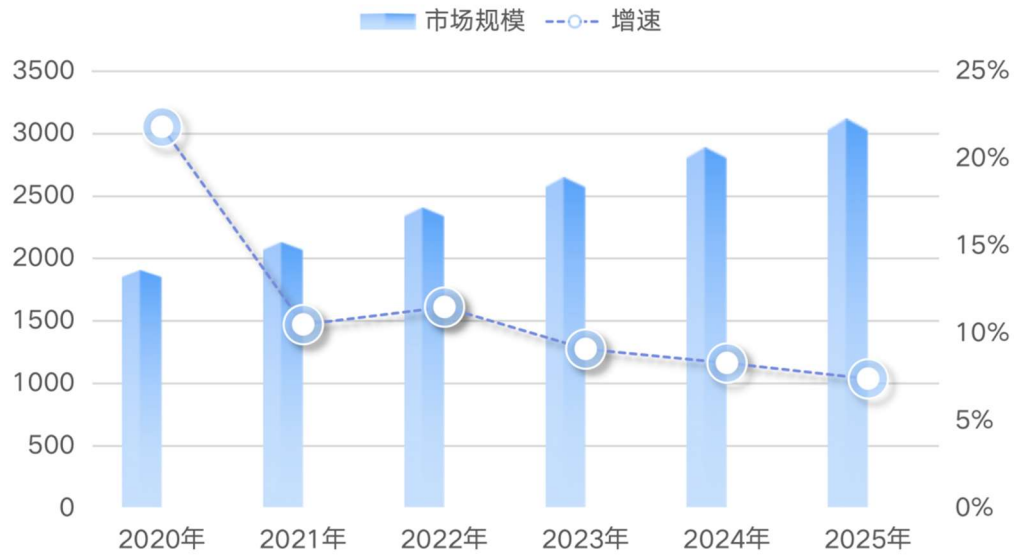


图 1：智能家电市场规模以及增速

2.2 智能家电系统的软件平台架构

智能家电系统需要多层次的软硬件架构模式用以支撑不同的智能化发展阶段，主要分为单机智能、协作智能、决策智能、高阶智能以及泛在智能的 5 个演进阶段。智能家电系统架构的演进体现为从单体设备到系统化智能，逐步增强联动、决策和自主学习能力，最终实现全场景的泛在智能。在不同发展阶段中，该架构在系统特征和功能层面呈现出明显的变化，从而实现了不同的智能化水平。单机智能阶段的系统特征是侧重于单一设备的控制和基本功能。家电独立运作，智能功能局限于单体设备。用户通过云端服务器实现远程操控，设备孤立、互动有限。在这个阶段，系统软件的主要作用是提供操作系统和应用层，以实现设备的基本控制和用户交互。协作智能阶段强调各智能家电间的融合协作，通过中心云或边缘计算实现联动。互通性增强，不同品类/品牌的智能设备能够互联互通，构建智能家电系统的应用场景。在这个阶段，系统软件的架构引入了服务框架层，该层支持不同设备、异构协议之间的互通，从而实现了设备之间的联动协作。同

时，多模态人机交互开始出现，指令式的语音交互，大/小屏端的设备操控及信息呈现，指纹、人脸的身份识别等 AI 算法广泛应用在不同品类的智能设备上，一定程度的改善了用户使用智能家电系统的体验。决策智能阶段的特点在于设备能够具备一定的智能决策能力，可以根据数据做出优化决策。系统软件在这个阶段进一步加强了服务框架层，引入了大模型来进行智能决策，应用层也得以提供更加智能化的预测和自动化服务。大模型应用推动系统智能升级，实现主动学习和预测用户需求，为智能化水平的跃迁提供了关键技术突破路径。系统拥有自主决策能力，提供智能推荐和自动化管理。高度主动智能阶段所具备的特征是设备拥有更高级的主动性和个性化服务。通用人工智能技术进一步发展应用，家电向人类智能水平靠拢。实现智能决策、交互和个性化服务，用户体验更加智能化。在这个阶段，系统软件在服务框架层方面的功能进一步加强，以支持智能交互。应用层也会提供更个性化的推荐和自主决策服务，满足用户的个性化需求。泛在智能阶段的系统特征在于智能设备无处不在，实现了真正的泛在智能。跨设备、场景、地域实现全方位智能融合，智能技术嵌入各种设备和环境，实现无缝智能交互，提供全场景、泛在智慧生活。为实现这一目标，系统软件在连接和服务框架层方面进一步加强，实现智能算法的自我学习和进化。应用层则能够实现全场景的智能交互，让技术更加透明地融入人们的生活。

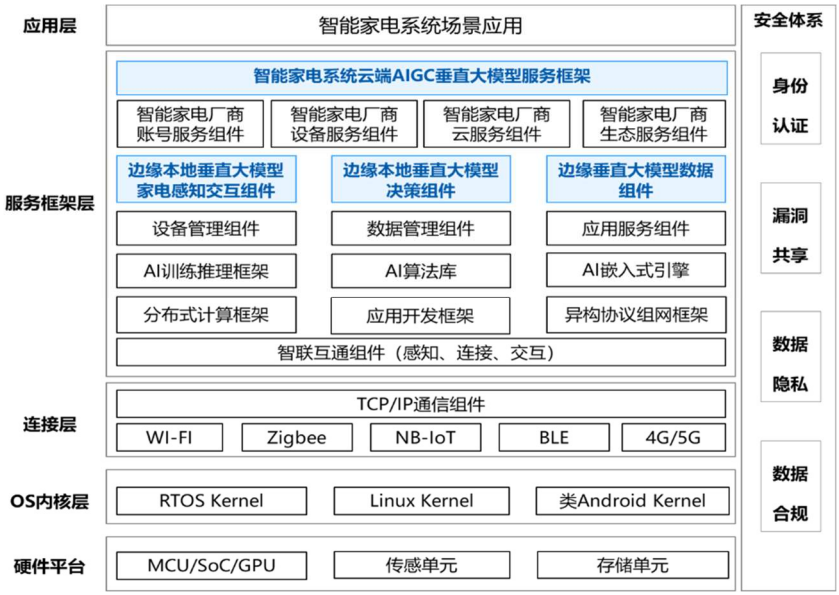


图 2：应用大模型的智能家电系统架构图

总体来看，智能家电系统架构经历了演进，从单体设备到全面智能化，不断

增强联动、决策和学习能力。随着通用人工智能技术发展，智能家电将实现更高水平的自主智能和泛在智慧生活，构建智慧、便捷、智能的家居生态。在不同阶段，软硬件架构分层解耦，从硬件平台到应用层，逐步完善智能能力。不同的系统特征指导下，软件系统不断拓展和优化各个层次，从而使得智能家电在功能、智能化和用户体验方面得到了持续提升。关于智能家电系统架构演进的论述，将在该白皮书的姊妹篇《面向未来的智能家电基础软件发展白皮书》给出详细介绍。

2.3 智能家电系统和服务的分类与特点

在设计智能家电系统和服务协议时，需要综合考虑智能家电系统的能力需求、产品和服务特性以及所面临的挑战。智能家电系统和服务可以分为四个主要类别：安全系统、能源管理和电气控制系统、监测系统以及居民便利应用。

（1） 安全系统：主要用于监视房屋并检测是否有不受欢迎的入侵者。智能家电产品如智能监控摄像头、智能门锁、智能报警器等，为用户提供实时的监控和警报功能，提高家居的安全性。

（2） 能源管理和电气控制系统：该系统主要提供四个主要功能，包括家庭管理、真实的监测和控制、能量分析和能量优化。如智能照明、智能空调、智能烤箱等。在不影响居民舒适度的前提下，以经济便捷的方式优化能源消耗。

（3） 监测（健康/老人/儿童）系统：主要用于早期阶段疾病检测、辅助老年人或残疾人长期独立生活等用途，如智能运动手环、智能体重秤等，可以收集和分析用户的身体健康数据。

（4） 居民便利应用：主要用于增加用户的舒适度并提供一些娱乐服务。如智能电视、智能音响等，支持语音控制、在线内容流媒体播放等功能，以提供高品质的娱乐体验。

智能家电系统和服务的特点主要包括以下几个方面：

（1） 连接性：通过无线网络(如 Wi-Fi、蓝牙等)或有线网络连接，智能家电可以与互联网、用户和其他设备实现互动。这种连接性使得用户可以通过智能手机、平板电脑等移动设备远程控制家电，并获取实时的信息和反馈。此

外，智能家电还可以与其他智能设备进行互联，形成一个智能家居系统，提供更全面的家庭管理服务。

（2） 智能化：智能家电采用人工智能技术，例如机器学习和数据分析，使其具备自主学习和适应用户行为和需求的能力。这意味着智能家电可以根据用户的使用习惯自动调整设置、提供个性化的服务，并根据环境和情况做出智能决策。例如，智能冰箱可以根据存储食物的种类和数量，自动生成购物清单或推荐菜谱。

（3） 自动化：智能家电具有自动化的功能，可以执行预设任务或根据环境和情况自动调整其操作。这提高了设备的效率，减少了用户的参与度。例如，智慧空调可以根据室内温度和湿度自动调节运行模式，以提供舒适的环境；智慧洗衣机可以根据衣物类型和脏污程度自动选择洗涤程序和洗涤时间。

（4） 用户友好：智能家电提供直观易操作的用户界面，以及多种交互方式，如语音控制、手机控制等，提升用户体验。用户可以通过简单的指令或触摸屏幕来控制家电的开关、调节参数等操作，而无需繁琐的操作步骤。此外，一些高端智能家电还支持自然语言处理和图像识别等先进技术，进一步提升用户体验。

（5） 个性化：智能家电能够根据每个用户的具体需求和喜好进行个性化设置和服务。通过收集用户的偏好和行为数据，智能家电可以了解用户的生活习惯和喜好，并据此提供相应的定制化服务。例如，智能电视可以根据用户的收视习惯推荐相关的视频内容或应用。

（6） 兼容性：智能家电可以与各种品牌和类型的其他智能设备协同工作，形成一个互联的智能家庭系统。不同的智能设备之间可以通过统一的标准进行通信和协作，实现数据的共享和信息的流通。这为用户提供了更大的灵活性和便利性，可以根据自己的需求选择不同品牌的智能设备进行组合搭配。

（7） 数据驱动：智能家电通过收集和使用大量数据来优化性能、提供更好的服务。这些数据包括用户的使用习惯、设备的运行状态、环境的变化等多方面的信息。通过对这些数据的分析和挖掘，智能家电可以预测用户的需求、提高设备的效率、优化能源利用等。

人工智能技术将推进智能家电产业走向无感化。随着人工智能与物联网（AIOT）新技术全面融入空间智能化，5G+AIOT 赋能智能家电产品革新，智能家居 3.0 模式将实现智能产品的智慧互联。目前，智能家居的入口和控制主要依赖于中控屏和音箱等设备。然而，随着 ChatGPT 等概念应用于智慧家居生活场景领域，人们对算法的自然语言处理能力有了新的认知，也为智能家电和智能家居未来的发展提供了更多想象空间。未来 AIGC 将赋能智能家居场景的无感化，从命令式交互转变为理解式交互，实现人机共创，形成数字管家，实现智能家居由“智能”向“智慧”转化。

2.4 智能家电产业面临的挑战和机遇

在行业自身发展与市场需求不断增加的双重作用下，我国智能家电行业正进入新一轮的发展周期。国内智能家电行业的发展程度与全球智能发展水平全面接轨，在我国正式进入快速发展通道。然而，智能家电产业的高研发成本仍然是制约我国产业发展的主要因素。AIGC 技术成为推动智能家电与智慧家居产业发展内核。即便 OpenAI 公司也面临着 AIGC 算法开发成本居高不下，巨大的运行成本难以盈利的窘境。根据《财富》杂志的报道，2022 年 OpenAI 的收入为 3000 万美元，但净亏损预计为 5.445 亿美元。近日，Analytics India Magazine 发布了一份报告，OpenAI 人工智能服务 ChatGPT 正面临财务挑战，距离实现 2024 年底 10 亿美元收入的目标依然遥远。公司 CEO 阿尔特曼在推特上回答马斯克的问题时表示，在用户与 ChatGPT 的每次交互中，OpenAI 花费的计算成本为“个位数美分”，每月的计算成本可达数百万美元。大模型高昂的训练成本让普通创业公司难以为继，因此参与者主要是科技巨头，国产大模型的训练，至少需要投入超过 1000PetaFlop/s-day 的计算资源。

另一方面，智能家居产业链的上游领域，包括芯片、传感器、通讯设备、电容设备、智能控制器等，芯片是智能家居发展不可或缺的关键环节。然而，美国政府对高端 GPGPU 芯片的封锁以及对中国超算的多次限制，给智能家电领域行业大模型的研发带来了巨大的挑战。目前，国产 GPU 产品与国外产品在计算性能方面仍或有一代以上的差距，而在软件和生态层面与英伟达 CUDA 生态的差

距则更为明显。但国内厂商正奋起直追，致力于实现 GPU 国产化的自主研发突破。其中包括龙芯中科、海光信息、壁韧科技、寒武纪、天数智芯等厂商正在研发或推出用于 AI 计算的 GPGPU、ASIC 等 AI 芯片，有望实现高端芯片的国产化替代。长久来看，美国对中国高端 GPU 的禁售令反而给国产 GPGPU 和 AI 芯片厂商带来快速发展的机会。国产 CPU、GPU、AI 芯片厂商将受益于庞大的国内市场，AI 芯片的国产化比例将显著提高，借此进行产品升级，逐渐达到国际先进水平，突破封锁，实现自主创新并构建自主生态体系，从而降低通用大模型与产业大模型的研发与访问成本，加快推进产业级生成式人工智能大模型的落地应用。

生成式人工智能赋能产业的关键因素是高质量行业数据的累积。家电领域的客户需求具有个性化特征，用户激活率低、前端数据采集困难等因素造成了家电领域的数据积累碎片化。因此，智能家电行业的数据特征提取不能具象化，从而制约了生成式人工智能在家庭场景的落地应用。AIGC 技术向智能家居场景进一步扩展过程中，智能家居本身的数据与其他领域的数据互通互联、数据的隐私与安全问题也成为制约行业快速发展的瓶颈。

从智能家电硬件基础来看，传统智能家居扩展产生的智能硬件的变革和创新创造出物理意义的家居管家。然而，每一个智能家电设备成为进入家庭网络的潜在入口，从而增加了网络攻击的风险。从安全角度来看，AIGC 的不确定性，应用到智能家居的物理世界交互，极有可能产生的系统安全问题。

除此之外，当前智能家电产业的发展还面临着不同厂商设备间技术标准与通信协议的兼容性、节能减排、消费者个性化需求与扩大市场需求等挑战。国际上，智能家电领域多种 IoT 技术和众多生态系统并存，互相竞争，彼此之间不能互联互通。为了解决这一问题，亚马逊、苹果、谷歌等主流生态厂商联合 CSA 于 2022 年 10 月 4 日正式发布了 Matter 1.0 标准，旨在将繁杂的智能家居设备收归到统一的通信标准。一时间，智能家居厂商纷纷积极拥抱新标准：硬件方面，Silicon Lab 推出了具备高性能 2.4 GHz RF、低电流消耗和最大内存和闪存容量等设计优势的 MG24 芯片；平台方面，涂鸦智能可以为用户提供“Matter 交钥匙方案”，组建了高价值生态，聚合芯片厂商、认证测试实验室，为客户提供包括制造资源、

认证服务以及客户产品售前、售中、售后的全链路技术支持；产品方面，欧瑞博发布了3款全球首批通过Matter标准认证的智能家居产品——SOPRO智能壁灯、MixDimmer 调节装置以及智能开关。显然，Matter 已经成为推倒传统智能家居柏林墙的重要力量。

综上所述，国内智能家电行业未来需要加强协同创新，推动产业链上下游企业的深度融合，制定统一的技术标准和规范，加强隐私保护和算法合规性应对。因此，受研发成本、数据资源、系统安全、行业标准等多方面因素的制约，智能家电领域的行业大模型的研发将依托于国家级创新中心所带动的行业联盟共同推进。通过联合众多头部企业的合作，实现行业数据要素汇聚，开展面向智能家电产业的通用大模型的研发，赋能智能家电领域，引领家电行业智慧升级。

3. 生成式人工智能大模型简介

3.1 生成式人工智能大模型的基本原理和核心技术

GPT 大语言模型是一个大规模的人工智能语言模型，通过互联网上大量文本语料进行训练，能通过对话形式和人类进行交互、回答各种问题。其背后的主要技术原理是自监督学习（Self-supervised Learning）、指令微调（Instruct-tuning）和人类反馈强化学习 RLHF（Reinforcement Learning from Human Feedback）。其中 ChatGPT 利用强化学习的方法来与人类意图对齐，利用人类反馈信号直接优化语言模型。

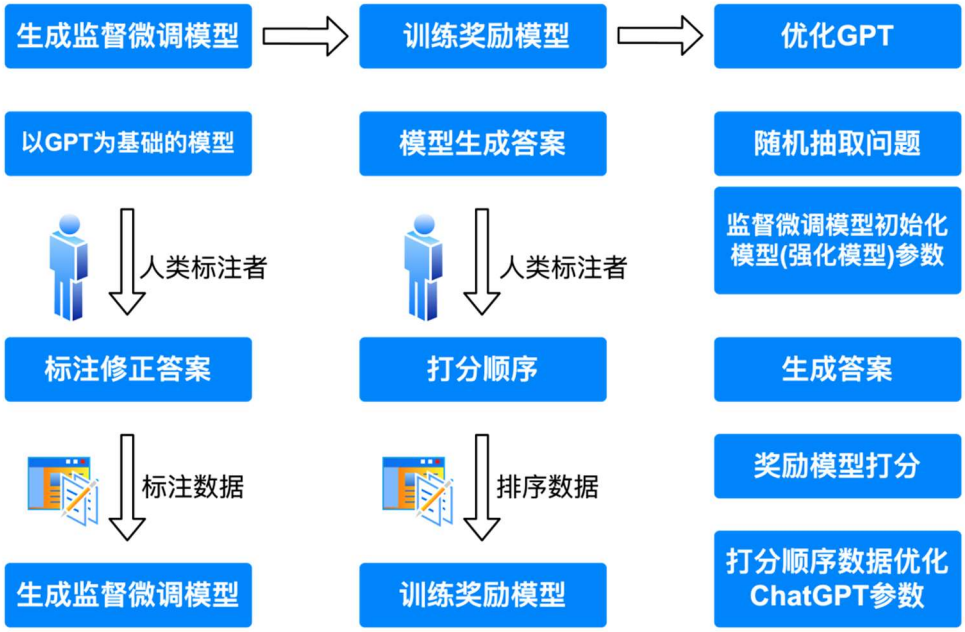


图 3：GPT 大语言模型主要技术原理

在生成式人工智能大模型的构建方面，预训练和微调是两个主要步骤。首先，采用自监督的学习范式预训练模型。通过超大规模的数据，让模型学习语法以及一些推理能力。然后，在更微观的数据集上“微调”这些模型，这些数据集遵循研究人员提供的指南，由人工审阅者仔细生成。由于无法预测未来用户对系统的所有可能输入，因此不会为模型将遇到的每个输入编写详细说明。相反，在指南中概述了几个类别，使用过程中，模型会根据使用人员的反馈进行概括，以响应给定用户提供的各种特定输入。

生成式人工智能大模型的构建基础是数据。大语言模型的训练需要大规模的文本数据集，数据集的规模和质量决定了模型的效果和泛化能力。此外，为了适应不同的任务和应用场景，还需要针对各个场景纳入不同主题、风格、形式的数据，包括图像、语音和视频数据。然后，对原始数据进行清洗和预处理。该过程包括去除无效信息、如噪声、错误、重复或与任务无关的内容。通过清洗和预处理数据，可以提高数据的准确性和一致性，并减少对模型训练的干扰。该过程在生成式人工智能大模型的构建中起着至关重要的作用。

在具体的方法学上，模型架构设计是构建生成式人工智能大模型的核心，该设计直接影响模型的效果和性能。生成式人工智能大模型主要通过 Transformer

架构进行迁移学习（Transfer Learning）实现，其主要原理是将从一项任务中学习到的“知识”应用于另一项任务。Transformer 的主要特点是使用"自注意力机制"或"注意力机制"的策略，用以计算输入数据中不同部分之间的内在关联，以此理解数据的复杂模式。

Transformer 的基本结构由两部分组成：编码器（Encoder）和解码器（Decoder）。编码器将输入序列的输入转化为一系列向量，解码器则将这些向量转化为输出序列。在这个过程中，模型通过自注意力机制来分配注意力到输入序列的不同位置。自注意力机制使得 Transformer 可以同时处理序列中的所有元素，并且能够跨越元素之间的距离进行全局的信息整合。与传统的循环神经网络（RNN）模型相比，Transformer 具有显著优势。它能更好地处理长距离依赖问题，在大规模并行计算设备（如 GPU）上表现更佳，从而大大提高了训练效率。目前，诸如 BERT、GPT 等高级自然语言处理模型都采用了 Transformer 结构。

图 4：Google 与 OpenAI 在 LLM 领域的发展时间线

图 4 可以看出，GPT 基于的 AI 模型和技术几乎都源于 Google，OpenAI 只

是面向应用做了局部的改进，但结局却是 Google 参考 ChatGPT 匆忙推出自己的大语言模型，这和 OpenAI“实用至上”的价值观和工程思维密切相关。此外 Meta 采用开源开放的发展策略，推出了一系列开源的 LLAMA 模型，复现 ChatGPT 的效果，而且支持商用，对于生成式大模型推广起到了推动作用。对于 ChatGPT 技术路线的拆解追溯，其关键能力来自几个方面：强大的基座模型能力(Instruct GPT)，高质量的真实数据，以及从用户标注中反馈学习(RLHF)等。因此，以模型能力为基础，应用为目标导向，构建家电行业的高质量数据库，进而催生“智能家电+大模型”新业态是一种有效途径。

在具体的技术实现路径上，生成式大模型通过引入更多的用户指导，在原有的大模型基础上进行微调和强化学习训练，让模型能更好地按照用户意图生成目标内容。其基础原理如下：

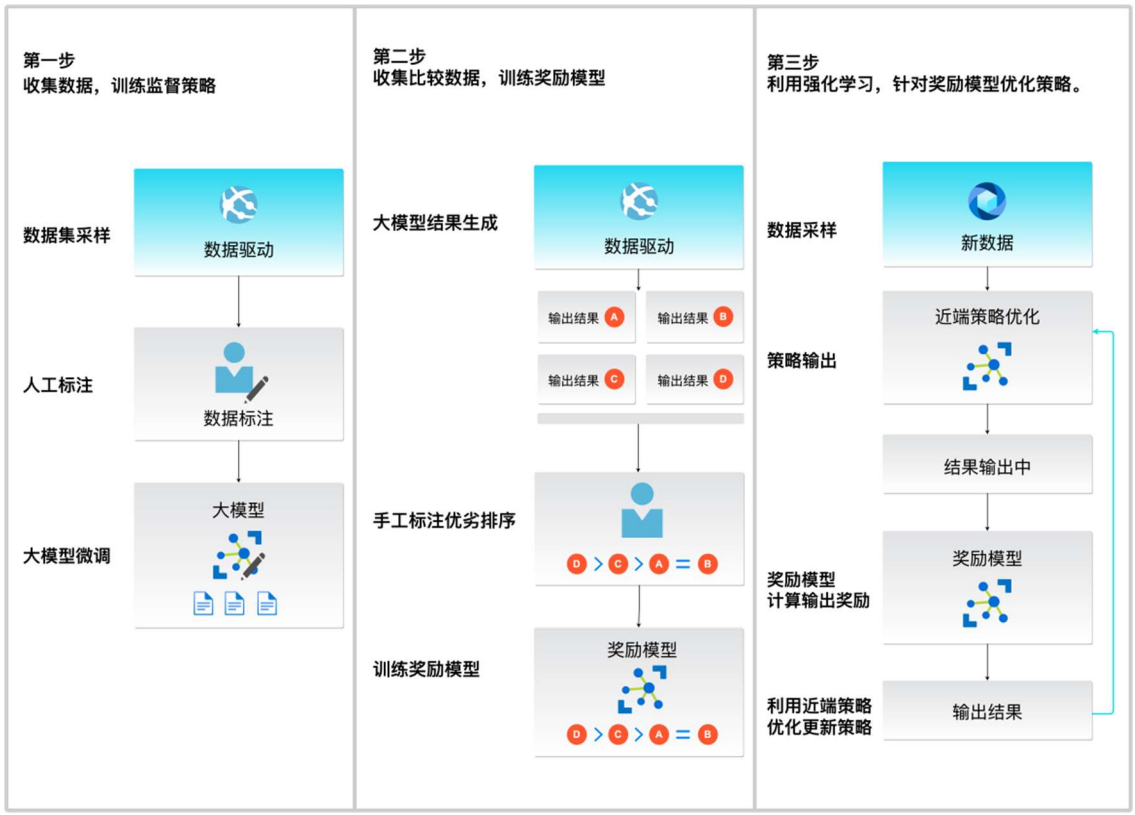


图 5：大模型微调和强化学习

训练过程可以分成三个步骤：

Step1 有监督训练（SFT）:收集经过标注的数据，并将其提供给训练有素的标注人员。这些标注人员根据预定的 prompt，对数据进行标注。在这一阶段，

利用已经标注好的数据样本，模型通过有监督的方式进行训练。

Step2 激励模型训练（RM）:在有监督训练的基础上，进行激励模型的训练。在这个阶段，目标是最大化较好样本的激励分数。激励分数可以由人工评估或其他指标来衡量，以确定模型生成结果的质量和合理性。通过训练，模型将逐渐调整自己的生成策略，以提升生成内容的准确性和可控性。

Step3 强化模型训练（RL）:在激励模型训练后，可以使用强化学习训练的方法进一步改进模型。强化学习是一种迭代的训练方法，在此过程中，模型使用之前生成的输出作为伪标签，重新进行训练。通过不断迭代和反馈，模型可以自我调整和改善，提高生成结果的质量。

大模型本质上采用多任务联合学习的方法，并用 zero-shot，one-shot，few-shot 等技术取代传统的模型微调方法，以实现下游任务的迁移。通过这种方式，大模型可以实现自主学习和推理的效果预期。

然而，要实现这一目标，大模型需要解决几个关键挑战。首先，它需要大量高质量的数据来有效地学习和预测多样化且复杂情况的任务。这意味着必须积累充分的数据集，以覆盖广泛的领域和应用场景。其次，大模型需要强大的算力支持才能确保训练的效率和速度，并在有限的时间内完成更多的训练迭代。只有具备丰富的算法研发经验、积累了大量数据并拥有强大计算能力的企业，才能成功地开展大模型的研发与应用。此外，国家层面的政策支持也将对大模型领域的发展起到关键作用。通过政府制定相关政策、提供资金支持和鼓励技术创新，可以促进大模型的研究和应用，并推动该领域的快速发展。

3.2 生成式人工智能大模型的行业数据库构建

建立基于工业互联网的家电行业数据库，训练出用于产业分析的大模型，需要进行以下工作：

（1） 数据收集与整合：收集来自工业互联网的大量家电产品和用户行为数据，包括但不限于产品规格、性能数据、销售数据、用户评价、使用情况等。这些数据可以通过各种方式获取，如厂商的开放 API、合作伙伴数据分享、本地传感器等，并将其存储在统一的数据库中。

（2） 数据清洗与预处理：将收集的数据进行清洗和预处理，例如消除噪音、处理缺失值、标准化不同格式的数据等，以便于后续模型使用。

（3） 模型设计与训练：基于收集和清洗的数据，设计并训练人工智能大模型。依据具体任务，模型可能包含 NLP、图像识别、预测分析、推荐系统等多个模块。对模型进行训练至使其能够从数据中学习并进行准确的预测或生成。

（4） 产业分析功能实现：结合具有预测性和洞察力的图表、报告等形象表达形式，对生成的分析结果进行视觉化展示，以便于业界人士进行产业分析。

（5） 持续优化：收集更多的数据，并且定期对模型进行评估和调整，以适应行业的发展和变化，保证模型准确性和实用性。

从家电行业智能生产应用的角度出发，以面向物理对象的方式构建数据表单，添加元数据库和数据治理系统，最终生成一个物理信息数字孪生对象库。

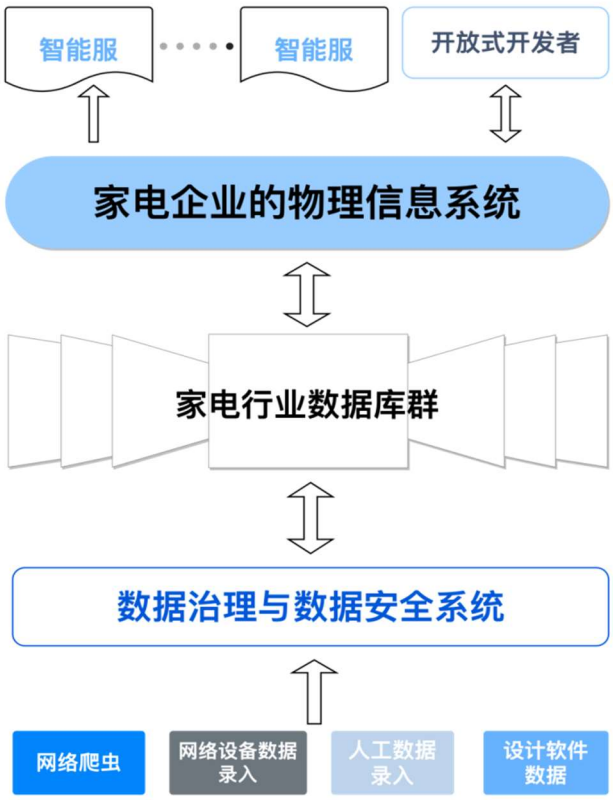


图 6：家电行业数据群

面向工业互联大环境，整合家电企业的物理信息系统，可实现产品从设计到维护全过程的智能化，实现生产过程可计算化和可视化，形成从行情、技术、工

艺、利润等分析到控制再到分析的闭合回路，预测在产品制造过程中出现的问题，对生产策略进行分析，然后基于优化后的生产策略实施生产。

（1） 人员知识库

人员基本信息与专业技能等信息描述以及工作状态等实时参数。

（2） 设备知识库

设备物理参数、功能参数、设备信息化模型以及工作状态。

（3） 物料知识库

物料的图片、数据手册，供应、仓储状态以及物料的信息化模型等参数。

（4） 工具模具知识库

工具模具的图片、数据手册、使用状态以及信息化模型。

（5） 工业标准知识库

行业标准文本数据库。

（6） 设计方案知识库

电路设计、结构件设计以及相关的技术文档。形成一个典型专家数据存储系统，根据以往的设计方案和成功应用的案例进行积累和迭代。

（7） 工艺设计知识库

工艺设计方案以及工艺流程，面向工艺流程建模。形成一个典型专家数据存储系统，根据以往的工艺方案和成功工艺案例进行积累和迭代。

（8） 产品案例知识库

产品数据手册，使用说明书、图片、视频等数据。

（9） GIS 库

地理信息的记录，上下游公司地理信息、公司内部生产要素的地理信息。

（10） 模型与数值知识库

电路仿真模型、产品仿真模型以及生产可行性和市场预测等模型。

（11） 供应链、产品追溯知识库

与供应链相关的信息。

（12） 应用场景和产业信息知识库

场景描述的文本、图片和视频等信息，产业市场与技术相关的信息库。

（13） 法规政策知识库

法律文档、案例等数据。

（14） 元数据知识库

存储元数据用于有效地管理各种数据库。

（15） 物理信息模型库

物理信息数字孪生，提供模拟实际生产环境的虚拟空间的通用模型数据。

（16） 开发者数据知识库

为开发者二次开发提供独立存储，受到物理信息系统的数据支持。基于物理信息平台的智能设计支持系统，在统一大数据基础上结合各类知识库，提供对设计方案和工艺流程的深度优化能力，为开发者提供开放的软件平台，让开发者自由的进行二次开发，从而提高设计和知识运用的效率，实现知识的自动积累、共享和重用。

3.3 国产生成式人工智能大模型的未来发展趋势

随着 OpenAI 开发的 GPT-4 语言模型受到世界广泛关注，各国都意识到了生成式人工智能大模型将对国家发展将产生深远影响，同样国产大模型的研发也成了目前中国重点支持的技术方向。

国产大模型未来的发展，将呈现以下几种发展趋势：

更大的模型：随着计算能力和数据量的增长，通用模型规模将会越来越大、性能越来越强。

更有效的训练：研究者们正在寻找更有效率的模型训练方法，例如：更好的优化器，更快的并行训练技术，以及使用更少数据得到更好性能的方法。

更多模态的信息处理：未来，中国的人工智能模型可能会更加专注于结合和解析多种类型的数据，例如文本、图像、音频和视频。这种多模态学习使得 AI 能更好地理解交互复杂的现实世界。

更强的领域专业化：未来可能会有更多的模型针对特定的应用领域进行专门的训练和调优，如家居、教育、医疗、金融和政务等领域。

发展生成式人工智能大模型是一项复杂任务，它需要巨量的硬件投入和大量

的存储、计算资源。此外，训练这类模型还强烈依赖于大规模的专业领域数据集。为了推动通用大型模型在未来智能家居等行业的开发，依托国家级创新中心，实现数据资源的共享和利用。同时，行业联盟与头部大模型企业合作，可以借助其在大模型建设方面的专业知识和经验，共同推动专业领域大型模型的研发。通过这种合作方式，可以消除重复的研究和开发，加速领域内的科学进步，并实现技术互利互惠。未来，多模态生成式人工智能模型的实现将给智能家电带来更多好处。结合图像、语音和传感器数据等多种感知技术，智能家电可以更好地感知客户需求。例如，智能摄像头和语音识别技术可以捕捉用户情绪和行为，从而自动调节环境并提供个性化服务，实现更好的人机互动体验。此外，多模态生成式人工智能模型还能创造更具创意的智慧家居场景。通过综合不同感知模态的信息，模型可以生成更丰富、个性化的智慧家居场景。例如，根据用户的口味偏好和天气状况，模型可以生成智能厨房的烹饪建议，并自动调节烹饪设备。这些创意场景将使智慧家居更具个性化和趣味性。

3.4 生成式人工智能大模型在行业细分领域的垂直应用前景

生成式人工智能大模型的兴起不仅标志着 AI 能力的突破，更通过改变生产力与生产关系，为整个时代带来了前所未有的机遇。首先，它进一步释放了生产力，原本费时费力的业务生产运作和复杂事件处理，可以借助大模型进行改善。此外，大模型提高了生产效率，它能够高效快速地生产出专业、有效的内容，如代码生成、知识问答、文档检索等。同时，国产化通用性大模型推动了数字化高质量发展，符合当前国情需要。因此，生成式人工智能大模型在各行业中具有潜力，可提升生产力、改善用户体验，并推动行业向数字化、智能化的未来迈进。在家电领域，生成式人工智能大模型的应用可以涵盖以下几个具体领域：

家居领域：大模型可以灵活地控制智能家居设备，以自然语言处理技术理解和执行用户的命令，为用户提供智能助手服务，还能在设计和装修领域提供建议，或者生成 3D 家居模型，基于多模态生成式人工智能技术未来可更好地感知客户需求。

教育领域：大模型可以担当个性化学习的监护人，为学生提供个性化的学习

资源和建议，还可以生成或编辑教学材料，以及评估学生作品。

医疗领域：大模型可用于自动化医疗记录的生成和翻译，帮助医生更好地理解病患的病情，还可以用于解读医疗研究，生成药品介绍，预测药品相互作用等。

金融领域：大模型可以从财务报告、股市交易数据、经济新闻等多种来源获取的信息生成投资建议，帮助电子交易和决策，还可以用于风险管理，识别可能的欺诈行为，为客户提供个性化的金融咨询。

政务领域：大模型可以自动化公文的生成、翻译、审查和归类，提高公务效率，也可以处理和分析大量的公开政策数据和公开的社交网络评论，以便更好地理解和反应公众的关注和需求。

目前，头部人工智能企业正围绕人工智能大模型等加快创新步伐，开展大模型创新算法及关键技术研究，国家层面也在加快智能算力基础设施建设，推动通用人工智能技术创新场景应用，市场各主流领域都在积极地在进行大模型与业务结合的尝试。

3.5 引入 AIGC 的优势和局限性、以及潜在的发展方向

引入生成式人工智能大模型主要有以下优势：通用性更强，能够在各种不同的任务和环境中应用；具备理解和生成各类复杂信息的能力，在文本分类、上下文理解、情感分析等领域表现优异；通过强大的学习能力，能够快速适应新事物、新的写作风格和新的概念，以优化理解能力和生成内容；拥有出色的预测智能和总结能力，形成最佳行为判断机制，实现高效且个性化的自动化服务。由此可见，生成式人工智能大模型在许多细分领域（如家居、医疗、教育、金融、政务等）发挥重要作用，降低人工智能应用门槛。

尽管部分海外大模型支持多种语言，但是主要是依托英文的世界知识训练的，在理解中文的语义和文化特性方面仍存在限制，尤其是在世界观和意识形态的差异，因此，国产大模型能更好地适应中文环境。商业和其他组织需要定制化的 AI 解决方案来适应各类业务场景，国产大模型能更好地满足这些需求。此外，国产大模型对数据进行更好的保护，能够解决数据隐私和治理问题。同时，国产大模型的发展有助于中国在全球人工智能领域保持独立、自主和高影响力。因此，

作为未来最具潜力的人工智能算法，生成式人工智能大模型对工业的智能化发展至关重要。在国际环境倒逼下，工业软件国产化替代成为趋势，而国产大模型将扮演重要角色，推动中国在人工智能领域的独立发展，并在全球占据重要地位。

然而，尽管生成式人工智能大模型具有许多优势，但目前仍存在一些局限性。首先，大模型的应用需要庞大的计算资源和存储空间，导致成本较高，限制了其在实际应用中的广泛采用。其次，大模型对数据的需求量较大，并且需要大量的标注数据进行训练，这在某些领域存在困难。同时，大模型的训练过程也面临一些挑战。模型的训练需要花费大量的时间和资源，而且需要高度专业化的团队来进行有效的训练和调优。此外，大模型往往需要海量的数据进行训练，而数据收集和处理可能受到隐私、安全和合规等方面的限制。

为了解决这些问题并推动生成式人工智能大模型的进一步发展，有几个潜在的方向值得关注。首先是技术上的改进，包括模型结构的优化、训练算法的改进和优化以及对小样本学习和增量学习的支持。其次是数据方面的创新，包括更好的数据采集、清洗和标注流程，以及探索利用合成数据和迁移学习等方法来扩充训练数据。此外，还需要加强对生成式人工智能大模型的监管和规范，确保其在应用中遵守伦理准则、保护用户隐私，并避免潜在的滥用风险。2023 年 4 月 11 日，国家互联网信息办公室印发《生成式人工智能服务管理办法(征求意见稿)》。这一办法不仅表达了对生成式人工智能的规制管理，更凸显了国家对其未来发展的明确支持。整体上需要确保生成式人工智能的行为服务全部处于监管之下，使其慢慢步入正轨，行稳致远。国产大模型的研发与应用是国家未来重点扶持的关键技术方向，亟需突破瓶颈，加快落地速度。

4. 生成式人工智能大模型在智能家电产业中的应用

4.1 生成式人工智能大模型在智能家电中的应用案例

4.1.1 面向智能客服的 AIGC 应用场景

普通客服系统通常有人工服务和机器人服务两种表现形式，人工客服可能会提供不一致的服务，无法迅速、准确解决用户问题且成本较高，机器人客服可能遇到语言理解和复杂场景的挑战，且大多采用标准化答复，无法满足用户的个性化需求。基于生成式人工智能大模型的智能客服系统改变传统的从库中调取预设答案的方式，利用大模型基于理解生成针对性的回答，可实现模糊语义理解、情感支持、自主决策、长时间记忆能力。

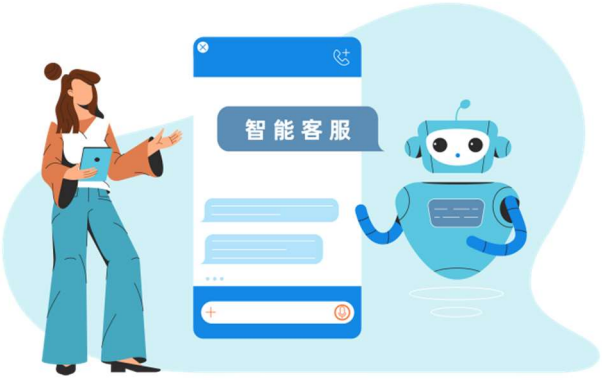


图 7：智能客服

模糊语义理解：智能客服系统可准确理解用户的模糊语义，分析出用户的真实意图，当用户说“我的洗衣机不运行了怎么回事啊”，客服系统分析此时用户需要解决洗衣机故障问题，给出反馈“告诉我一下洗衣机屏幕显示的代码是多少”，进一步获取相关信息，找出洗衣机故障的原因。

情感支持：智能客服系统可分析用户的情绪，给予用户情感支持。当用户说出“快速帮我解决这个故障”，客服系统抽取“快速”二字，分析用户可能带有着急的情绪，安抚用户“不要着急哦，正在快速定位故障的原因，一定帮您搞定”。

自主决策：当用户告知洗衣机故障时显示的错误代码为 E4，智能客服系统为用户提供问题解答“E4 错误通常表示洗衣机里的水位过高，这可能是由于进水阀堵塞或漏水导致的，建议您关闭洗衣机并断开电源，然后检查一下进水管是否有任何堵塞，如果问题仍未解决，您可能需要寻求专业技术人员来帮助修理，是否现在拨打售后电话为您提供服务”。

长时间记忆：若用户告知智能客服系统需要提供上门服务时，智能客服系统主动记忆用户的使用地址，并反馈“是否使用您之前的收货地址来为您提供上门服务”，用户回答“是”，系统自动按照此地址为用户下单，无需再次输入上门地址。

4.1.2 面向家庭场景自生成的 AIGC 应用场景

面向家庭场景的 AIGC 技术通过可自然沟通的交互模式极大地提升智能家居产品的智能化水平与核心竞争力，促进家电大脑的智慧升级，让家电具备自然沟通，主动服务的能力，成为掌握着最懂用户需求、最专业的家生活技能的家电大脑，更好地感知客户的个性化需求。作为全球首个场景品牌，三翼鸟对智慧场景的定义就是运用 AIoT、大数据等智能技术，解决用户生活场景中所存在的痛点的解决方案，提出“1+3+5+N”全屋智慧全场景解决方案。以智家大脑开放平台为内核，打造 AI 云、大数据云、IoT 为一体，连接 1 个全屋神经元网络系统。通过智家大脑完成对用户行为的识别、用户习惯数据的存储运算和智能设备的无感连接，并依托丰富的传感器，可以实现声音、图像、触控、姿态等多维度的感知，然后合理的调度各个智能家居，为用户提供更贴心更智能的服务，主动感知用户需求，生成随用户需求变化而变化的智慧场景

当前产品说明书的制作需要为每一个型号的产品单独适配，因产品功能、使用语言及销售地区的不同，为产品说明书的制作带来很多困难，当产品发生改变或升级时，说明书也需要更新，这意味着必须重新设计、重新印刷和重新分发，过程繁琐且耗费人力物力。对于跨国企业，说明书需要翻译成多种语言，而且要保证各种语言版本的精准度和一致性。基于生成式人工智能大模型的家电说明书

制作系统可提供说明书母版，具备全球范围内的语言翻译和文化迁移能力。

说明书母版：说明书系统使用基础产品说明书母版，对于同一种类家电使用统一模板，自动提取产品规格文件中的相应参数，从而自动生成产品说明书。例如读取新型号冰箱的产品规格书，识别到新增图像识别相关规格则自动补充到说明书母版中，从而形成此型号冰箱的产品说明书。

语言翻译：说明书系统根据产品的使用地区自动翻译成相应语言，满足不同地区的语言需求，翻译地区涵盖全球范围，例如，若产品在英国地区使用则自动翻译成英文，并可保证产品说明书翻译的准确度和各种语言版本说明书内容的一致性。

文化迁移：说明书系统根据不同地区的文化差异，按照产品使用地区自动修改和设计说明书，生成符合当地人风格习惯的产品说明书。

生成式人工智能大模型在智能家电的应用将掀起智能家居的改革浪潮，为智慧家庭领域实现从单品智能到全屋智慧的跨越提供底层驱动力，使智能家电不再是单一的智能单品组合，而是可以学习、理解用户行为和心智的家庭生活服务助手；使智能家电不再是被动执行用户指令，而是时时观察用户动作，想用户之所想，主动为用户提供生活所需的家庭场景。

4.1.3 面向家电生产制造的 AIGC 应用场景

随着自动化和用户个性化需求的不断增长，未来工厂的愿景将不再仅仅侧重于批量生产能力，而更注重个性化设计和定制能力。在未来的工厂中，产品的独特性和专属性将成为竞争的主要标志。除了关注每天生产数量和成本之外，工厂还需要致力于提供给每位客户专属的产品定制服务。同时，无人工厂的普及，个性化产品定制的重要性将进一步增加。它能通过自动化系统和机器人技术实现高效生产，并且具备灵活性和适应性，可以根据客户的需求进行快速调整和定制。这种定制化的能力将成为工厂吸引消费者和满足市场需求的重要优势。为了实现这样的愿景，工厂需要投资于创新设计和生产技术。先进的计算机辅助设计（CAD）和三维打印等技术将成为个性化产品定制的关键工具。此外，工厂还需要建立高效的供应链系统，以确保定制化的生产过程顺畅进行。不仅如此，数

据分析和人工智能技术也将发挥关键作用，帮助工厂理解客户需求并提供个性化定制的解决方案。

可以想象，随着 AIGC 大模型的普及，为生产线向自动化与智慧化的提升提供了可能性。我们从人机共创的角度来介绍家电生产和制造的 AIGC 应用场景：

在当前 AIGC 赋能生产主要体现在辅助指导书编写和辅助质量问题分析等方面。虽然是辅助性工作，但是面对产线的劳动密集型特征，能够直观而有效地节省人力，提高产线效率。国产 AIGC 结合物联网技术和视觉技术可以有效将这些环节进行改善，降低自动化产线门槛，加快各项环节的扭转速度，真正做到少人干预，无人干预。

未来产业将逐渐从批量化生产转向个性化生产。 国产生成式大模型技术将推进工业场景中的人机共创。这一模式将涵盖从用户需求沟通、自动设计、物料采购、个性物料定制、生产排产到物流运输等全流程与全自动化操作，实现真正的物联网工厂模式，推动制造业向智能化、高效化的未来发展。

4.2 家电行业 AIGC 的未来场景展望

在人工智能技术的赋能下，智能家电完成了智能单品、智能场景、智慧家庭的进阶，当前正在向智慧生活进化。但从市场端看，仍旧没有跨越从创新者、早期采用者到早期大众的鸿沟。

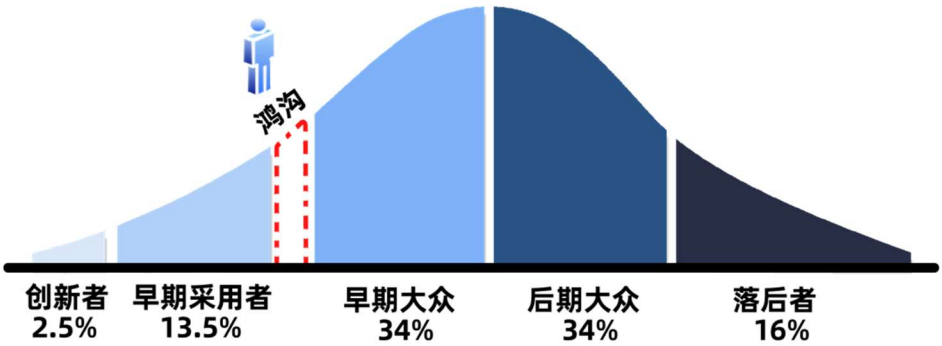


图 8：智能家居市场现状

2022 年 11 月，美国 OpenAI 发布了 ChatGPT（Chat Generative Pre-trained

Transformer），以生成式人工智能大模型的方式给智能家居行业带来了新的思路。同时 ChatGPT 也给行业带来了新的思考——用户期望的智慧生活是简单的传统产品的智能化？还是产品需要重构？

从人机关系的角度，传统的人机关系是单向，即人找机器。当用户有洗衣、控温、冷藏食品等需求时，用户主动找到相应的机器完成需求。因此，早期的智能家电的智能功能如下：

智能单品：App 远程控制等功能；

智能场景：将智能单品连接起来，利用传感器等感知设备，通过感知用户身体特征等状态，提供场景式联动服务；

智慧家庭：智能场景的叠加。

以上智能产品将用户视为智能系统的一个“输入量”，实质上仍然是“人找机器”的过程，只不过可以分为“主动”和“被动”两种方式。

在现实生活中，人类是真实、会思考、有感觉、变化着的存在。随着用户对人工智能技术的认知提升，潜意识的需求也在发生变化，需求从“使用智能家电”转向“享受智慧生活”。那么在智慧生活中智能家电的定位、角色需要重新定义。

著名的图灵测试要求：测试者在与被测试者（一个人和一台机器）隔开的情况下，通过一些装置（如键盘）向被测试者随意提问。如果机器能够让 30%的测试人相信它是人类，那么这台计算机就可以被认为具有人类的思考能力。那么智能家电需要有思考能力吗？人们需要的是家电的智能化，还是家电智能体化？从用户体验看，智能体是需要的。

智能体是什么？智能体（Agent）是处于某个特定的环境下的系统，该系统可以根据自身对环境的感知，按照已有的知识或者通过自主学习，并与其他智能体进行沟通协作，在其所处的环境自主地完成设定的目标。Agent 一词最早见于 M.Minsky 于 1986 年出版的《Society of Mind》。多智能体系统（Multi-Agent System，MAS）是多个智能体组成的集合，其目标是将大而复杂的系统建设成小而彼此互相通信协调的易于管理的系统。多智能体系统自 20 世纪 70 年代被提出以来，就在智能机器人、交通控制、分布式决策、商业管理、软件开发、虚拟现实等各个领域迅速地得到了应用，目前已经成为一种对复杂系统进行分析与模拟的工具。

多智能体系统由分布式人工智能演化而来，其研究目的是解决大规模的、复杂的现实问题。MAS 是可以相互协作的多个简单智能体为完成某些全局或者局部目标使用相关技术组成的分布式智能系统。

智能家居环境可以视为一个复杂系统，其依据用户自身的信念和需要实现众多意图，以满足用户的各种需求；同时伴随着智能化水平的不断提高，智能家电正从感知智能、计算智能向认知智能进化，每个智能家电本身又可视为了单独的智能体 Agent，因此智能家居系统可视为 multi-Agent 构成的复杂适应系统。

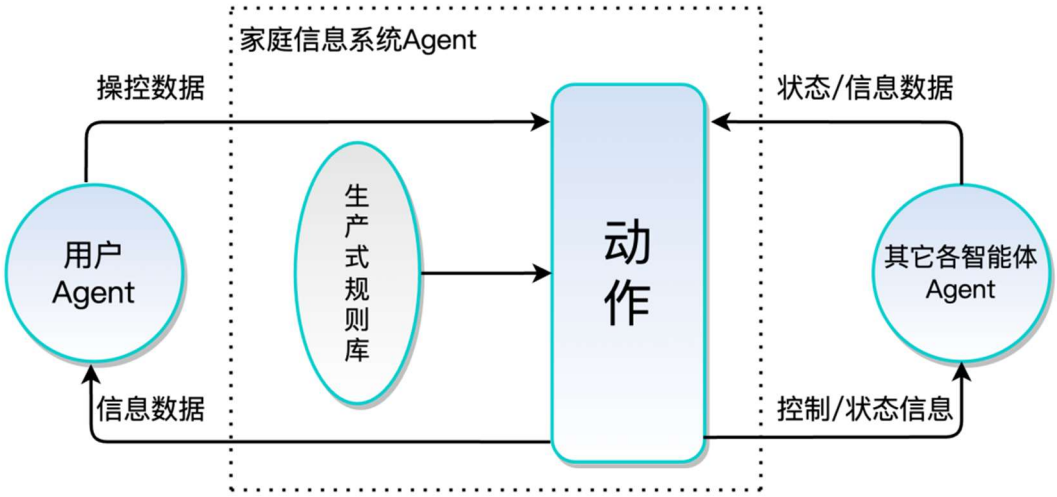


图 9：家庭信息系统 Agent 模型

复杂适应系统（Complex Adaptive System）提出于 1994 年，其核心思想是“适应性产生复杂性”。提出者霍兰教授将复杂适应系统定义为由一组实体（Agent）组成的系统，这些 Agent 对来自其他 Agent 或者外界环境的刺激行为或刺激反应行为做出反应。Agent 通过改变自身的规则来积累经验并进行适应，也可以聚集成为具有涌现行为的元 Agent，这些涌现行为不能通过分析底层 Agent 的行为来得到。表 1 列举了 Agent 的特性。

表 1：Agent 的特性及描述

特性	描述
积极性，目的性	为了实现目标，获取主动权的能力
情境性	Agent 嵌入其环境中，感知并作用于环境
反应性，响应性	对环境变化及时做出反应的能力
自主性	控制自身行为和内部状态的能力

社交性	与其他 Agent 互动和沟通的能力，甚至能够意识到其他 Agent 的存在
拟人性	具有类人的属性，例如信念和意图
学习性	能够根据以往的经验提升能力
连续性	短时间内连续的运行过程
移动性	能够在模拟的物理空间中移动，有时甚至在不同的机器之间移动
特定的目的	旨在完成明确定义的任务

作为智能体 Agent 自身拥有 BDI（Belief Desire And Intention），即信念-需求-意图，信念就是自身的规则库、信息库，是该智能体用于感知、评估、决策的底层信息系统，这个信息系统可以是开放的，在实际工作中通过行为决策不断更新；需求是该智能体 Agent 用于决策和执行的有效输入，是对外部指令信息，环境/事件信息的有效感知后产生的内部状态；意图是智能体 Agent 的目标集和计划集匹配的输出，是实现智能体 Agent 功能的决策驱动。

以上分析看，家电智能体化是一种可行的趋势。智能家电未来的方向是“拟人化”、“类生物化”。以 ChatGPT 为代表的生成式人工智能技术为家电的“类生物化”提供了助力。

通过智能家电的“类生物化”，智能家电变身“管家”，人、机器的关系变为“共生关系”，用户通过智能家电的享受主动服务；智能家电通过不断学习，提高感知、认知水平。

从智能感知看，智能家电的感知种类不断增加，包括用户身体指标、资源、环境、空间、气候等信息（见表 2）。智能感知类型的增加，为智能认知准备了充分的数据。

表 2：智能感知种类的举例

序号	种类	项目	技术
1	用户	生理指标、状态、行为等	人脸识别、字符识别、图像识别、定位测距、声源定位、语音识别、
2	资源	用水量、用电量、用气量等	

3	环境	温度、湿度、风感、空气质量、气味、压力等	声纹识别等
4	空间	位置、面积等	
5	其他	气候、味觉等	

在智能感知种类接近于人类的情况下，在算法、算力、知识的协助下，智能家居具有了用户意图判断等能力。在人与家电的共生中，交互扮演很重要的角色。人类个体比其他动物没有多大优势，人和大猩猩的基因，有 98.4%都是完全一样的，只有 1.6%有区别，当人类掌握了符号语言，人类社会的结构发生了突变，有了一个连接在一起的集体大脑。这种物种之间相互关联、相互作用的方式，才是人类和其他物种的真正区别。人与人之间的交互具有连续对话、对方意图判断、上下文理解、引导式、生成式等特点，因此类生物的智能家电也应该向这些特点看齐。

目前，市场上的智能家电语音交互能力参差不齐，有专业指令交互、特定指令交互、弱泛化指令交互、强泛化指令交互等不同的语音理解水平，用户体验并不是很好。更多情况下，智能家电难以准确理解用户的指令或需求。以 ChatGPT 为代表的大语言模型，具有以下值得智能家居交互借鉴的特点：

强泛化能力可以帮助用户使用日常说话方式交互，用户与机器的交互更加易学；从做“选择题”的决策型 AI 到做“简答题”的生成式 AI，用户与智能机器的交互更加高效理解用户意图，相对于传统交互，对用户输入指令的容错能力更加增强；并且可以多轮对话，实现从交互到聊天的进阶，增加对用户使用的吸引力；多模态、跨模态迁移增强知识获取，实现能力的涌现，实现从原始数据中发现新的、未知的特征和模式，提高学习的有效性；类似于人的推理方式的思维能力，具有一定逻辑分析能力（比如简单数学问题、符号操作和常识推理等任务），区别于词汇概率逼近模型；RLHF（Reinforcement Learning from Human Feedback）：即，使用强化学习的方法，利用人类反馈信号直接优化语言模型，提高模型的学习有效性和效率。因此，家电行业引入生成式人工智能大模型，赋能智能家电“类生物化”，使其具有一定的生物功能。

GPT 作为一种通用的大预言模型，其涌现能力和简单思维能力，通过生成式预训练提升语言理解能力，接受的输入信号和输出结果更加接近于人类偏好，对于解决“听不懂人话”的缺点有极大的改善作用。当然，在生成监督微调模型、训练奖励模型等环节的人类标注、标准修正答案、打分排序等环节，采用智能家居行业领域专业数据进行优化模型，可以进一步提高识别效率和精准度，实现 GPT 通用向专业的商业化应用，还需企业进一步训练，训练出企业适合的“类 GPT 等专业大语言模型”。

GPT 目前还存在不可解释、鲁棒性差等缺点，胡言乱语的现象仍旧存在。智能家居产品受制于安全等因素要求，GPT 直接用于控制智能家居产品还不能被接受。因此建议采用智能家居语音控制系统知识库与类 GPT 等专业大语言模型相互耦合的构建方案（图 10），消除语言大模型存在幻觉现象。

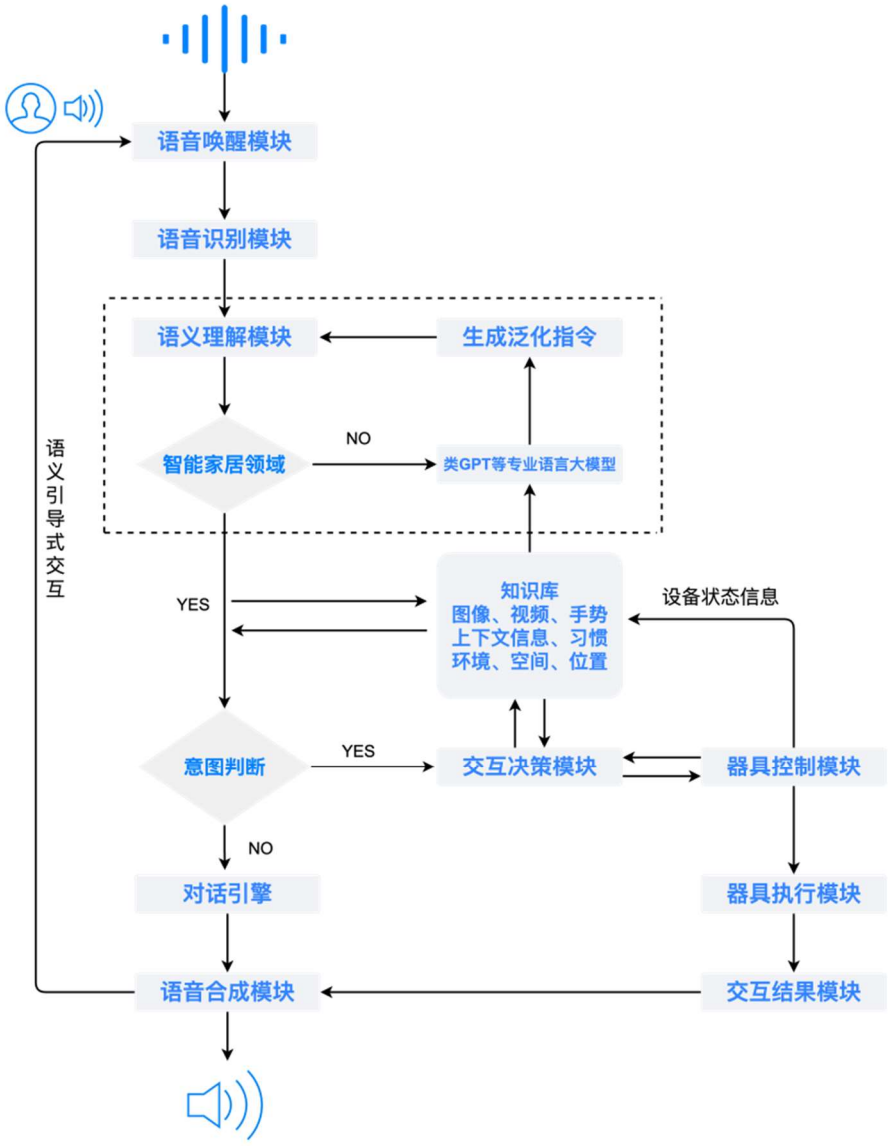


图 10：语音交互与大语言模型构建示意图

由于用户对智能家居产品的功能不是很熟悉，用户习惯于按照自己的理解、过去的操作习惯，通过语音控制家电。但是用户语言请求并不能完全吻合特定控制指令、泛化指令，智能家居产品并不能准确理解用户的意图，有些产品标准了一些固定的反馈，虽然满足了用户的交互需求，但是并没有正确按照用户请求，开启对应的智能功能。因此可以采用语义引导式交互的方式，引导用户启动期望的智能功能（图 11）。语音引导分为两次分配：

（1）当用户请求的表述内容未在智能家居领域时，通过类 GPT 等专业语言模型的语义理解，生成泛化的指令，趋近于智能家居领域。

（2）当用户请求的表述内容落入智能家居领域，进行意图判断。如果意图不明确，基于知识库进行语义理解，给出接近的语音反馈建议，引导用户修正自己的请求表述，给出清晰、准确的请求表述，实现控制智能家居的目的。

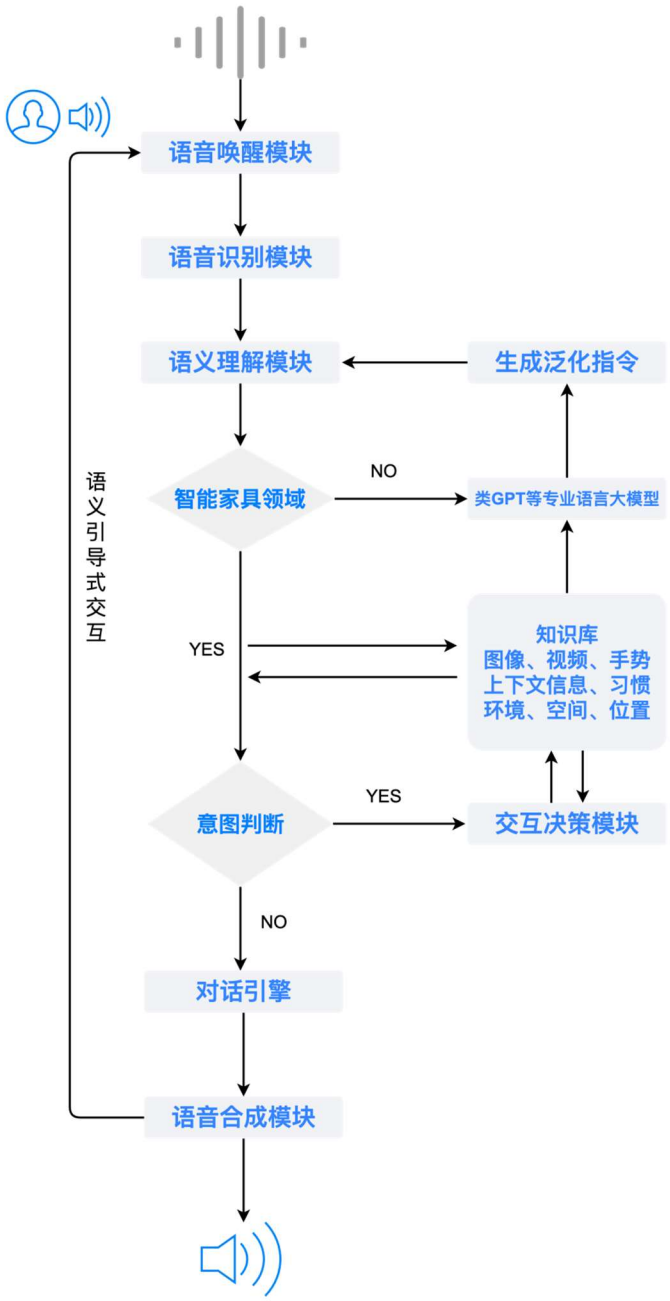


图 11：语义引导式交互示意图

智能家居语音交互与类 GPT 等专业大语言模型的耦合，可以使语音交互从

做“选择题”的决策型 AI 进阶到做“简答题”的生成式 AI，用户与智能家居的交互将更加流畅，可以更好地理解用户的需求，并生成更准确、详细的回答。基于 RLHF 的人类反馈强化学习不仅增强了交互系统自我学习进化的能力，还可以在引导式交互中，不断进化，解决系统用户端“一次不懂，次次不懂”的问题，逐渐提高系统的智能水平。

4.2.1 面向家电整机企业 ToB 垂直应用场景

随着数据积累和模型的发展，在家电的全产业链条中，AIGC 可以发挥其创造力，为产业提供创意和提高效率，为家电产品定义、家电外观设计、控制器电路（部件）布局和设计、市场趋势引导新产品形态乃至决策等一系列环节赋能。

家电产品定义：AIGC 利用先进的自然语言处理技术和机器学习算法，可以对大量的家电产品规格书进行快速分析和理解，从而实现家电产品规格书的自动定义。通过这种方式，AIGC 可以帮助家电企业快速准确地定义产品规格，提高生产效率和产品质量；

家电产品外观设计：伴随多模态 AIGC 的研发落地， 生成式人工智能大模型还将对家电产品的外观进行自动设计。通过对海量的家电产品外观数据进行学习和训练，可以自动生成新的家电产品外观设计方案，帮助企业实现差异化竞争和创新设计。

工业生成式设计：利用工业互联网和云平台所累积的数据，将利用生成式 CAD 技术对家电产品的部件自动设计，实现虚拟和增强现实（VR/AR）的交互和体验。通过云端平台实时协作，共享设计文件和资源，实现自动优化设计，以满足特定的性能要求条件，降低人工成本，加快产品的设计周期。

市场趋势引导新产品形态：AIGC 还可以通过对市场趋势的分析和研究，引导家电企业的新产品形态设计。通过对消费者需求和行业趋势的深入了解，AIGC 可以帮助家电企业把握市场机遇，推出符合市场需求的新产品。

4.2.2 面向家电、家庭、人和健康的 ToC 应用场景

自然语言大模型可自然沟通的交互模式，可以促进家电大脑的升级，让家电

具备自然沟通，主动服务的能力，从而实现“家电大脑”的愿景。

在 ToC 领域中，大模型技术可以帮助企业更好地了解消费者的需求和行为，提高产品的定制化和智能化水平，让用户和产品可以直接通过自然语言沟通。同时，大模型技术还可以帮助企业实现与智能家居、物联网等非家电生态系统的快速融合，提供更加智能、便捷、舒适的场景生活体验。

1. 智慧生活场景

通过大模型技术的应用，用户和家庭的知识库可以量化到本地设备上，除了可以保证数据安全，家电还可以具备主动服务的能力和以人为本的个性化服务能力。例如，带大模型支持的智慧屏家电或管家型的机器人家电，可以本地收集空间内的全部家电数据、人的饮食、睡眠、运动等综合数据、当前的环境数据、历史消费数据，在数据安全的前提之下，给出最适合当下的家电服务、管家服务、健康推荐服务。在智慧厨房中，厨电的自动料理机可以理解用户的口味、健康诉求，从而给出适应用户当下健康状态和口味的饮食规划；智能空调可以通过睡眠感应技术感知用户的活动和睡眠状态，自动调节温度和湿度；智能体脂秤可以通过大模型技术分析用户的身体健康数据，提供个性化的健康（睡眠，饮食，运动等）建议。大模型真正可以做到理解家庭用户的健康、生理、爱好等需求，真正做到“以人为本”、“千人千变” 、“在线、动态、闭环”。

2. 智慧健康场景

大模型的开发和应用将为居家健康领域提供更多可能性。大模型可以帮助用户在家进行健康咨询，提供健康建议，辅助判断症状严重程度。用户可以方便快捷地获得医疗建议。通过连接可穿戴设备，大模型可以持续监测用户的健康数据，如心率、血氧、血压等，分析健康趋势,及时发现健康风险，辅助医患共同做出健康决策。大模型可以为用户提供个性化的健康管理建议，帮助用户改善生活习惯，预防疾病的发生。此外，大模型还可以根据用户的健康数据，例如心率、血压、血糖等，进行健康评估和疾病预测。对于居家护理或康复的患者，大模型可以根据治疗方案自动生成训练计划、记录训练数据，并给出训练质量反馈。将大模型与智能家居设备相结合，可以实现语音控制、自动调节家居环境、提醒用药等功能，辅助居住者更便捷地完成日常健康管理。综上所述，基于大模型的能力，

可以提升健康管理的连贯性和持续性，提供更个性化的健康管理，提升健康管理的便捷性，降低健康管理成本，提供更加精准和全面的健康服务。

国家高端智能化家用电器创新中心通过物联网平台，实现居家健康监测及运动设备接入，完成健康体征数据采集及运动状态和进度的监测；结合大模型平台和知识图谱，完成对体征数据的预测、健康状态分析、健康问题咨询及健康档案管理，最终实现居家健康的“监、管、预、问、干预”等健康全流程管理。同时此平台是面向企业的多租户 SAAS 服务平台，提供企业级 SAAS 服务订购能力，企业基于此平台能力完成个性化健康产品的定制研发，从而服务于家电企业健康应用。

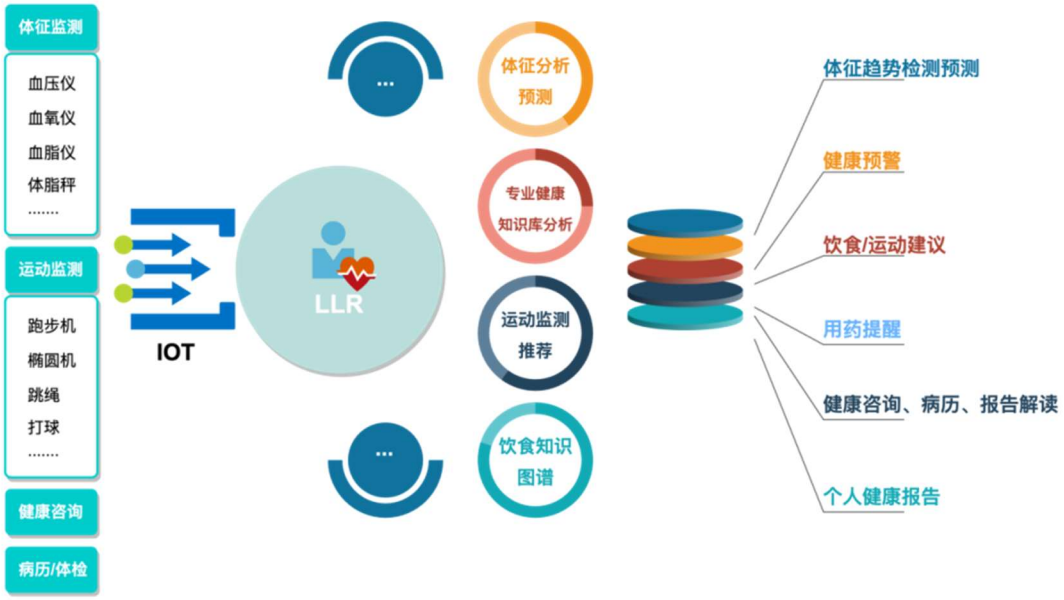


图 12：智慧健康

5. 人工智能时代智能家电产业的合规性应对

5.1 智能家电产业中的数据隐私和安全问题

根据市场调研，隐私泄露问题已经成为用户选择智能家电的最大痛点，大数据为人类生活带来了技术变革，但同时也对人们的隐私造成了新的威胁。传统的隐私保护机制受到了冲击，强化对个人信息隐私权的保护显得尤为迫切。

造成个人隐私泄露的不安全因素包括：智能设备的信息泄露、收集用户数据的上层应用、网络服务信息泄露以及病毒、木马的恶意攻击。可以说，窃取用户隐私信息的手段层出不穷，而智能家电为用户带来的便利的同时，信息安全也并不能成为便利的代价。随着大众越来越频繁地使用智能家电产品，公民的数据也大量地被储存在企业、组织的数据库中，再加上技术漏洞以及法律制度的不完善，越来越多的个人信息被滥用、盗取甚至被倒卖，这也带来了严重的隐私泄露问题。因智能家电信息安全问题导致的个人隐私泄露事件频发，消费者对此存在持续的焦虑。

公众对家电信息安全和个人隐私保护的需求是迫切的，仅依靠有效的法律法规来确保公众的信息安全明显是不足的。这也意味着智能家电制造企业需要担起更多的保护数据安全的责任与义务。

除了人工智能系统及其相关数据的机密性、完整性、可用性以及系统对恶意攻击的抵御能力等网络安全基本属性外，人工智能安全一般还需要考虑以下属性。

（1） 可靠性：指人工智能及其所在系统在承受不利环境或意外变化时，例如数据变化、噪声、干扰等因素，仍能按照既定的目标运行、保持结果有效的特性。可靠性通常需要综合考虑系统的容错性、恢复性、健壮性等多个方面。

（2） 透明性：指人工智能在设计、训练、测试、部署过程中保持可见、可控的特性，只有具备了透明性，用户才能够在必要时获取模型有关信息，包括模型结构、参数、输入输出等，方可进一步实现人工智能开发过程的可审计以及可追溯。

（3） 可解释性：描述了人工智能算法模型可被人理解其运行逻辑的特性。

具备可解释性的人工智能，其计算过程中使用的数据、算法、参数和逻辑等对输出结果的影响能够被人类理解，使人工智能更易于被人类管控、更容易被社会接受。

（4） 公平性：指人工智能模型在进行决策时，不偏向某个特定的个体或群体，也不歧视某个特定的个体或群体，平等对待不同性别、不同种族、不同文化背景的人群，保证处理结果的公正、中立，不引入偏见和歧视因素。

（5） 隐私性：指人工智能在开发与运行的过程中实现了保护隐私的特性，包括对个人信息和个人隐私的保护、对商业秘密的保护等。隐私性旨在保障个人和组织的合法隐私权益，常见的隐私增强方案包括最小化数据处理范围、个人信息匿名化处理、数据加密和访问控制等。

5.2 智能家电产业应注意的伦理和法律合规问题

5.2.1 国内对于智能家电信息安全约束性法律法规

自 2016 年以来，我国先后颁布《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》与《网络产品安全漏洞管理规定》等一系列法律法规，用以规范公民的网络行为，保障公民的网络权益和个人隐私安全。2023 年 7 月 10 日，国家网信办联合国家发展改革委、教育部、科技部、工业和信息化部、公安部、广电总局公布《生成式人工智能服务管理暂行办法》（以下称《办法》）。这些法规主要情况见表 3。

家电作为一个充分竞争的行业，就目前而言，监管仍比较薄弱。但这些法规给智能家电行业的监管提供了充分的依据，让智能家电每个链条中参与者权益的保护实现有据可查、有法可依，对推动智能家电信息安全的正规化、标准化、合法化影响深远。

表 3：国内智能家电适用的主要安全法规

实施日期	法规名称	核心要点
2017年6月	《中华人民共和国网络安全法》	《网络安全法》对智能家电厂商构成关键信息基础设施运营者的，提出了更为具体的要求。收集、使用个人信息，应当遵循合法、正当、必要的原则，注意收集、处理的个人信息及重要数据，本地存储义务以及数据安全评估义务，并考虑调整与此相关的网络架构及业务模式；不得设置恶意程序。发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，在约定期限内，持续提供安全维护。
2021年9月	《中华人民共和国数据安全法》	界定了数据、数据处理、数据安全的严格定义，并规定开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。规范了智能家电产业链条中所有环节对于数据安全的权益和义务，尤其对数据汇聚、处理和利用的厂商行为进行规范，督促数据的开发和利用合规合法。
2021年11月	《中华人民共和国个人信息保护法》	理清了个人信息、敏感个人信息、个人信息处理者、自动化决策、去标识化与匿名化的基本概念，对个人信息处理和敏感个人信息处理等多方面进行了全面规定，建立起个人信息保护领域的基本制度。作为针对个人信息的保护性法律，对于智能家电厂商而言，尤其需要注意的是，法条指出，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式;收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。
2023年8月	《生成式人工智能服务管理暂行办法》	首个国家AIGC监管文件。明确利用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等内容的服务（以下称生成式人工智能服务），适用本办法；规定提供和使用生成式人工智能服务，应当遵守法律、行政法规，尊重社会公德和伦理道德；要求提供者应当依法承担网络信息内容生产者责任，履行网络信息安全义务。涉及个人信息的，依法承担个人信息处理者责任，履行个人信息保护义务。

5.2.2 国外对于智能家电信息安全约束性法律法规

国外对于智能家电信息安全和个人信息安全高度重视,欧洲主要国家、英国、美国、欧盟等先后出台了多项法规，主要情况见表 4。

表 4：国外智能家电适用的主要安全法规

实施日期	国家或地区/法规名称	核心要点
2017年9月	瑞士/《联邦资料保护法》(DPA)	配合欧盟GDPR的实施,希望在GDPR正式实施之后，继续获得第三国适应性认定,而不须在每次跨境资料传输皆遵循GDPR规则办理。瑞士DPA与GDPR区别在于其并未制定数据可携带权、没有领域外效力、对于知情同意的要求较低、认证机制于行为守则及罚则较低。
2018年4月	德国《联邦个人资料保护法》(BDSG)	对已实施40年的BDSG进行了大幅调整以符合欧盟GDPR《通用数据保护条例》。在新的BDSG法案中德国联邦政府运用了GDPR的开放性条款，导致部分新的BDSG规范内容超越了GDPR的条文规范,与现行欧盟法律不符,很可能被宣布违反欧盟法律。另一方面，旧的BDSG仅有48条规定，而新的BDSG则超过85条规定，且更为复杂，提高了法律适用上的难度。
2018年5月	欧盟/《通用数据保护条例》(GDPR)	制定关于处理个人数据中对自然人进行保护的规则,以及个人数据自由流动的规则;条例保护自然人的基本权利与自由,特别是自然人享有的个人数据保护的权利;条例规定不能以保护处理个人数据中的相关自然人为由,对欧盟内部个人数据的自由流动进行限制或禁止。条例规定了约束范围不论企业在不在欧盟，只要在欧盟进行“个人数据处理”、“数据支付对价”、“数据监控”就受GDPR限制。后续提出了具体的个人数据处理原则、处理的合法性、同意的条件,以及针对特殊人群和不需要识别的处理的细化处理方式。
2018年5月	英国/《数据保护法》（DPA）	建立英国数据保护框架以促进GDPR在英国的有效落实，并在GDPR框架下对某些条款做出裁剪规定。该法主要内容包括：1）加强数据主体对其个人数据

		的控制权。2）加强数据控制者义务。此外，该法还为刑事司法机构出于执法目的而处理数据设计了专门的执法框架，要求在执法过程中同样需要保护个人数据。
2019年5月	美国/《内华达州数据隐私法》(SB220)	该法案涉及互联网隐私，要求互联网网站和在线服务的运营商遵循消费者的指示，不得出售其个人数据。违反SB220可能会导致运营商收到禁令或每次违规最高被处以5,000美元的民事处罚。
2020年1月	美国/《加州消费者隐私法》（CCPA）	旨在提高加州居民对个人信息相关问题以及企业对个人信息的收集和所收集之个人信息如何成为其他企业的财产的关注，并切实保护加州居民的隐私权。从更高层面来说，这部新法将要求各机构透明地收集、共享和利用用户数据。整体而言，CCPA与GDPR的立法逻辑基本一致，但也存在个别差异。同时，CCPA对个人数据或者说个人信息有着更为全面的定义，对管辖权的规定更为简练与凝聚重点，而在跨境传输的管控上，更为放任，甚至是鼓励。
2023年6月	欧盟/《人工智能法案》（The AI Act）	通过统一的法律监管框架，以基于风险识别分析的方法，为不同类型的人工智能系统提出不同的要求和义务，从而确保基于人工智能的商品和服务在高度保护健康、安全、公民基本权利和保障公共利益的前提下，促进人工智能规范化的开发、使用和营销。

这些法规中比较有影响的是欧洲通用数据保护条例（GDPR），该法规于 2018 年 5 月 25 日生效，适用于欧盟成员国以及欧洲经济区内的企业和个人。GDPR 规定了个人数据的处理和保护要求，包括对智能家电收集、存储和处理个人数据的限制和要求。它的意义主要体现在以下几个方面：

（1） 个人数据保护：GDPR 确保个人数据在处理和传输过程中得到适当的保护，包括对个人数据的收集、存储、使用和共享等方面进行规范。个人数据指的是任何能够识别个人身份的信息，如姓名、地址、电子邮件地址、电话号码等。GDPR 要求企业和组织在处理个人数据时采取必要的安全措施，确保数据不被未经授权的访问、泄露或滥用。

（2） 用户权利保护：GDPR 赋予个人更多的权利控制其个人数据的使用。个人有权知道自己的数据被收集和使用的目的，并可以随时访问、更正或删除自己的数据。GDPR 还规定了个人数据的移植权，即个人可以要求将自己的数据从一家组织转移到另一家组织。

（3） 组织责任和透明度：GDPR 要求组织对其个人数据处理活动负有责任，并要求其采取适当的技术和组织措施来保护个人数据。组织需要提供透明的隐私政策，向个人清楚地说明其个人数据的处理方式和目的，并取得个人的同意。GDPR 还规定了数据泄露通知的义务，即组织在发生个人数据泄露时需要及时通知相关监管机构和受影响的个人。

（4） 全球数据保护标准：虽然 GDPR 是欧洲联盟的法规，但其影响范围远远超出了欧洲。由于 GDPR 适用于处理欧洲公民的个人数据，因此全球范围内的企业和组织都需要遵守 GDPR 的规定，以确保与欧洲公民的数据交换合规合法。这使得 GDPR 成为全球数据保护的标准，推动了全球范围内的数据保护法规的制定和实施。

5.2.3 智能家电应用生成式人工智能技术可能面临的伦理问题

在没有借助生成式人工智能技术的情况下，智能家电虽然也与用户交互，但回复给用户的答案或用于控制家电的指令是经过筛选的有限集合。而采用生成式大模型是否会给出一些违反人类伦理道德的答案或者操作，是值得思考的问题。

（1） 传播错误的意识形态

人工智能的目标是模拟、扩展和延伸人类智能，如果人工智能只是单纯追求统计最优解，可能表现得不那么有“人性”；相反，包含一些人类政治、伦理、道德等观念的人工智能会表现得更像人、更容易被人所接受。事实上，为了解决人工智能面对敏感复杂问题的表现，开发者通常将包含着开发者所认为正确观念的答案加入训练过程，并通过强化学习等方式输入到模型中，当模型掌握了这些观念时，能够产生更能被人接受的回答。然而，由于政治、伦理、道德等复杂问题往往没有全世界通用的标准答案，符合某一区域、人群观念判断的人工智能，可能会与另一区域、人群在政治、伦理、道德等方面有较大差异。因此，使用内

嵌了违背我国社会共识以及公序良俗的人工智能，可能对我国网络意识形态安全造成冲击。

例如，我们向 ChatGPT 问 X，它可能回复我们 Y，我们自然会相信 Y，那我们的思想不就被它控制了吗？如果 AI 变得有预谋，在一些特定的议题上，刻意给出有误导成分的答案，而大部分人看完后又不假思索，那就不单只是个人层面的思想行为被控制，而是上升到了整个社会层面。所以说，ChatGPT 一旦被某些别有用心的组织掌握并传播虚假信息，那么它的能量不仅仅是窃取资料，更甚者可能颠覆社会秩序，引发社会动荡。

尤其是在很多用来进行训练的数据本身就存在意识形态问题的情况下，而且有些大模型是基于很少量的中文语料训练的，这方面的问题可能会更突出，需要高度重视。

（2） 偏见与歧视

一方面，训练大模型的数据是一定时间前的历史数据，本身往往就具有倒退偏见，没有及时反映后面发生的进步；另一方面，某些训练数据本身就带有人群歧视，而且有可能会被放大。

5.3 国内外行业标准和应对策略

5.3.1 国内智能家电信息安全相关标准

为了贯彻落实《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》与《网络产品安全漏洞管理规定》等法规要求，全国信息安全标准化技术委员会（SAC/TC260）、全国家用电器标准化技术委员会（SAC/TC46）等标准化委员会、中国标准化协会等团体近年来发布了一系列智能家电适用的信息安全、个人信息保护等方面的标准，详细情况见表 5。

表 5：国内智能家电适用的主要安全标准

实施日期	标准编号及名称	核心要点
2020年10月	GB/T35273-2020《信息安全技术	标准明确了数据安全责任人相关要求，规范了个人信息保护负责人的相应工作职责；规

实施日期	标准编号及名称	核心要点
	个人信息安全规范》	定了定向推送相关要求以及用户可以撤回的权利；提出了平台第三方接入责任相关要求，对第三方接入的监督管理责任进行细化。规范每条要求的检测评估点，便于认证工作根据标准要求逐条开展；对 APP 中涉及的核心功能、必要信息、必要权限等方面进行展开描述，提出清晰的要求并形成评估点,在标准条款中以 APP 为例进行解释说明，增强其指导性。
2022年6月	GB/T40979-2021《智能家用电器个人信息保护要求和测评方法》	标准主要规范智能家用电器相关的个人信息保护要求，促进企业良性竞争，为消费者提供更好的消费体验，保障消费者个人信息安全。该标准适用于智能家用电器、智能家用电器系统和智能家居应用过程中相关各类组织的个人信息处理活动，对个人信息收集、存储、使用（公开披露、共享与转让、委托处理及跨境传输）等业务流程，以及个人信息保护的组织管理与评价。
2022年11月	GB/T41387-2022《信息安全技术智能家居通用安全规范》	标准在定义智能家居系统的组成以及对应的安全框架的前提下，对信息安全的通用要求和检测方法两方面进行了规范。智能家居系统主要由智能家居用户、智能家居终端、智能家居控制端、智能家居网关、通信网络和智能家居应用服务平台组成。该标准主要针对智能家居终端安全、智能家居网关安全、智能家居控制端安全和智能家居应用服务平台安全提出相应的安全要求和测试评价方法。
2023年5月	GB/T41789-2022《智能家用电器的通用安全技术要求》	标准规定了家用电器安全要求、信息安全要求、功能安全要求、指示、标识和说明等内容，对智能家电的电器安全、信息安全和功能安全指标提出具体要求。这对智能家电产品的发展是非常必要的，可促使家电行业内有统一的规范，利于各大厂家良性竞争，最终也保障了消费者的利益。
2023年5月	GB/T41817-2022《信息安全技术个人信息安全工程指南》	标准适用于涉及个人信息的网络产品和服务，为其在需求、设计、开发、测试等系统工程阶段开展个人信息保护实践提供指导。
2023年5月	GB/T41819-2022《信息安全技术	标准实施对象为人脸识别数据处理活动，包括收集、存储、使用、传输、提供、公开与

实施日期	标准编号及名称	核心要点
	人脸识别数据安全要求》	删除等，主要内容包括规定了数据处理者开展人脸识别数据处理的安全通用要求，并进一步明确了收集、存储、使用、传输、提供、公开、删除等处理活动的安全要求。标准应用于人脸识别数据处理者，即帮助人脸识别数据处理者规范人脸识别数据处理活动，防范人脸识别数据安全风险。
2023年5月	GB/T42012-2022《信息安全技术即时通信服务数据安全要求》	本标准规定了即时通信服务收集、存储、传输、使用、加工、提供、公开、删除、出境等数据处理活动的安全要求，并给出了即时通信服务典型场景数据安全保护要求。该标准的应用为即时通信服务数据安全监管工作提供参考，促进即时通信平台规范健康发展；帮助即时通信服务提供者规范数据处理活动，建立数据安全治理体系，保障用户个人信息权益；为即时通信服务相关的数据安全评估、认证等工作提供依据。
2023年5月	GB/T42015-2022《信息安全技术网络支付服务数据安全要求》	标准规定了网络支付服务收集、存储、使用、加工、提供、公开、删除以及出境等数据处理活动的安全要求，并给出了网络支付服务典型场景下的数据安全要求。为网络支付服务数据安全监管工作提供参考，促进网络支付平台规范健康发展；帮助网络支付服务提供者规范数据处理活动，建立数据安全治理体系，保障用户个人信息权益；为网络支付平台相关的数据安全评估、认证等工作提供依据。
2021年5月	T/CAS499-2021《智能家用电器网络安全技术要求和测评方法》	标准给出了网络智能家电的TSF（评估对象的安全功能）框架图，其中包含的安全功能为：设备网络配置与绑定、身份鉴别、通信保护、固件保护、代码安全、用户管理、访问控制、安全审计和加密存储。同时该标准将网络安全保障等级分为基本级和增强级，以便于企业及第三方检测机构依据产品的功能职责，选择不同的安全级别，为自评价及测评进行参考。基本级为TOE的最低安全要求，通过采用一定的安全功能要求和安全保障要求，使TOE能够抵御基本攻击潜力的攻击者的威胁。增强级为通过采用增强的安全功能要求和安全保障要求，使得TOE能够抵御中等攻击潜力的攻击者的威胁。

其中，重要的标准包括 GB/T35273-2020《信息安全技术个人信息安全规范》和 GB/T40979-2021《智能家用电器个人信息保护要求和测评方法》。GB/T35273 标准于 2017 年首次发布，2020 年修订再次发布，主要贯彻落实《中华人民共和国网络安全法》规定的个人信息收集、使用的“合法、正当、必要”基本原则，解决人民群众反映强烈的 APP“强制索权、捆绑授权、过度索权、超范围收集”的问题。同时，针对当前 APP 运营管理的一些不合理现象，如告知目的不明确、注销账户难、滥用用户画像、无法关闭个性化推送信息、第三方接入缺乏有效管理、内部管理职责不明等，进一步梳理完善条款，指导使用标准完善个人信息保护体系。GB/T40979 标准在 GB/T35273-2020 的基础上，结合智能家电的特点，将智能家电的信息收集方式以及个人信息的流转场景进行了分类，明确了个人信息安全级别的划分。划分出智能家电个人信息分类以及智能家电个人敏感信息分类，并对智能家电个人信息安全级别进行极高、高、中、低四个级别的划分，使得智能家电个人信息保护更加具体，有利于指导智能家电个人信息保护实践。

5.3.2 国外智能家电信息安全相关标准

为了适应家电智能化、网络化发展趋势，国外的一些国际标准化组织或社会团体，在智能家电信息安全和个人信息保护方面也陆续发布了一系列标准，详细情况见表 6。

表 6：国外智能家电适用的主要安全标准

实施日期	标准编号及名称	核心要点
2017年5月	ANSI/UL2900-1《网络连接产品软件信息安全标准》	标准提出了可联网产品的通用软件网络安全要求，它包含以下三方面的内容：①有关软件开发商（供应商或其他供应链成员）产品风险管理流程的要求。②评估和测试产品是否存在漏洞、软件弱点和恶意软件。③关于在产品的架构和设计中安全风险控制的要求。
2020年5月	NISTIR8259《物联网设备制造商的基础网络安全活	该文件为物联网设备制造商提供了详细的路线图，帮助解决IoT产品开发过程中遇到的网络安全问题。文件中建议从六个方面进

实施日期	标准编号及名称	核心要点
	动》	行准备，其中四个方面是在产品上市前进行风险的识别与适当的安全控制措施;另外两个方面是针对设备投放市场后如何满足客户的网络安全需求。这些措施侧重于确定客户及其网络安全需求，并解决设备面世后如何处理网络安全问题。
2020年5月	NISTIR8259A《物联网设备网络安全能力核心基准》	从基本的风险评估,网络安全测试,软件安全开发基本要求，以及用户信息告知均有所覆盖。网络安全测试包括设备标识、安全配置、数据保护、逻辑接口接入授权、软件/固件升级、安全事件日志等，为物联网设备网络安全能力提供了最低基准线。
2020年6月	ETSIEN303645《消费物联网网络安全：基线要求》	欧盟发布的首个针对消费类IoT设备的网络安全基线，该技术标准主要规定消费类物联网产品及其相关服务的网络安全标准。内容涵盖设备软件、通信、管理后台、流程制度等13个安全要求及个人隐私数据保护。
2020年9月	IEC60335-1:2020《家用和类似用途电器安全第1部分：通用要求》	规范性附录U中引入了网络安全要求，以避免未经授权的访问以及通过公共网络进行远程通信的传输故障的影响。但是，该附录不涉及与数据保密和消费者隐私方面保护要求。

其中，比较有广泛影响的是 ETSIEN303645，该标准针对包括智能家电在内的各类消费类物联网(IoT)设备提出了安全性、隐私性和可靠性方面的要求，它的实施对智能家电行业和用户有以下几方面的影响：

（1）设备安全性提升：标准要求物联网设备具有一定的安全性能，包括密码学安全、身份验证、访问控制等。这将有助于减少设备受到黑客攻击的风险，保护用户的数据和隐私。

（2）隐私保护加强：标准要求物联网设备在收集、存储和处理用户数据时遵守隐私保护原则，包括数据最小化、目的限定、透明度等。这将增加用户对设备和服务的信任，减少个人隐私泄露的风险。

（3）互操作性改善：标准要求物联网设备支持标准化的通信协议和接口，以便不同设备之间能够互相通信和协作。这将促进不同厂商的设备之间的互操作性，提升整个物联网生态系统的效率和便利性。

（4）法规合规性：该标准是欧盟发布的标准，符合该标准的设备将符合欧

洲相关法规的要求。对于物联网设备制造商和供应商来说，遵守该标准将有助于满足市场准入要求，并避免可能的法律风险。

5.3.3 加强人工智能标准化工作

智能家电的信息安全是指保护智能家电设备和其相关数据免受未经授权的访问、损坏或盗取的风险。人工智能安全是智能家电信息安全的一个重要扩展，需要在设计、训练、监测和法律政策等方面进行综合考虑，以保护人工智能系统和相关数据的安全。

人工智能系统越来越多地应用于各个领域，包括金融、医疗、交通、智能家居等，人工智能安全涉及到保护人工智能系统免受恶意攻击和滥用的风险，因此其安全性变得尤为重要：

——数据隐私：人工智能系统需要大量的数据来进行训练和学习，但这些数据往往包含个人隐私信息。因此，保护数据隐私成为一个重要的问题，需要确保数据在收集、存储和处理过程中得到充分的保护。这也是传统信息安全的重要内容，对于智能家电人工智能系统来讲，因为个人信息涉及到用户家居生活的各种场景，相比一般个人信息保护场景更加复杂和敏感，更需要特殊关注和处理。

——对抗攻击：人工智能系统往往基于机器学习算法，攻击者可以通过篡改输入数据或者引入恶意样本来欺骗系统，导致系统做出错误的决策。因此，需要研究和开发对抗攻击的方法，增强人工智能系统的鲁棒性。对于智能家电来讲，因为人工智能系统的鲁棒性问题，可能会导致智能家电的功能安全问题，甚至带来人员财产损害，必须高度重视。

——解释性和可信度：人工智能系统往往是黑盒模型，难以解释其决策的原因。这给用户和监管机构带来了困扰，因为他们无法理解系统为什么做出某个决策。因此，需要研究和开发可解释的人工智能算法，提高系统的可信度和透明度。

为了提高人工智能系统的安全性，需要从以下几个方面进行扩展：

——安全设计：在人工智能系统的设计和开发过程中，需要考虑安全性。这包括对数据的加密和隐私保护、对算法的鲁棒性测试和对系统的安全审计等。

——安全训练：在训练人工智能系统时，需要考虑对抗攻击。这包括引入对

抗样本进行训练，以提高系统的鲁棒性。

——安全监测：对于已经部署的人工智能系统，需要进行实时监测和检测，以及对异常行为进行及时响应和修复。

——法律和政策：制定相关的法律和政策，以保护人工智能系统和相关数据的安全。这包括数据隐私保护法律、对抗攻击的法律和人工智能伦理准则等。

为了更好地落实法律和政策要求，同时也是为了更好地指导人工智能系统的安全设计、训练和监测，国内外的主要标准化组织也加快人工智能相关的标准化工作：

（1）国外人工智能标准化情况

① 国际化

国际标准组织（ISO）在人工智能领域已开展大量标准化工作，并专门成立了 ISO/IECJTC1SC42 人工智能分技术委员会。目前，与人工智能安全相关的国际标准及文件主要为基础概念与技术框架类通用标准，在内容上集中在人工智能管理、可信性、安全与隐私保护三个方面。

在人工智能管理方面，国际标准主要研究人工智能数据的治理、人工智能系统全生命周期管理、人工智能安全风险管理等，并对相应的方面提出建议，相关标准包括 ISO/IEC38507:2022《信息技术治理组织使用人工智能的治理影响》、ISO/IEC23894:2023《人工智能风险管理》等。

在可信性方面，国际标准主要关注人工智能的透明度、可解释性、健壮性与可控性等方面，指出人工智能系统的技术脆弱性因素及部分缓解措施，相关标准包括 ISO/IECTR24028:2020《人工智能人工智能中可信赖性概述》等。

在安全与隐私保护方面，国际标准主要聚焦于人工智能的系统安全、功能安全、隐私保护等问题，帮助相关组织更好地识别并缓解人工智能系统中的安全威胁，相关标准包括 ISO/IEC27090《人工智能解决人工智能系统中安全威胁和故障的指南》、ISO/IECTR5469《人工智能功能安全与人工智能系统》、ISO/IEC27091《人工智能隐私保护》等。

电气与电子工程师协会（IEEE）在人工智能安全方面主要聚焦伦理安全风

险、可解释人工智能、深度学习评估、人工智能责任化等安全问题。最新的标准和报告有 IEEEP7000 系列标准、IEEE2841-2022《深度学习评估过程与框架》，在研项目有 IEEEP2840《责任化人工智能许可标准》、IEEEP2894《可解释人工智能的体系框架指南》等。

② 欧洲

欧洲电信标准化协会（ETSI）近期关注的重点议题包括人工智能数据安全、完整性和隐私性、透明性、可解释性、伦理与滥用、偏见缓解等方面，已发布多份人工智能安全研究报告，包括 ETSIGRSAI004《人工智能安全：问题陈述》、ETSIGRSAI005《人工智能安全：缓解策略报告》等，描述了以人工智能为基础的系统安全问题挑战，并提出了一系列缓解措施与指南。

欧洲标准化委员会（CEN）、欧洲电工标准化委员会（CENELEC）成立了新的 CEN-CENELEC 联合技术委员会 JTC21“人工智能”，并在人工智能的风险管理、透明性、健壮性、安全性等多个方面提出了标准需求。

③ 美国

美国国家标准与技术研究院（NIST）关注人工智能安全的可信任、可解释等问题。最新的标准项目有：NISTSP1270《建立识别和管理人工智能偏差的标准》，提出了用于识别和管理人工智能偏见的技术指南；

NISTIR-8312《可解释人工智能的四大原则》草案，提出了可解释人工智能的四项原则；NISTIR-8332《信任和人工智能》草案，研究了人工智能应用安全风险与用户对人工智能的信任之间的关系；NISTAI100-1《人工智能风险管理框架》，旨在为人工智能系统设计、开发、部署和使用提供指南。

2022 年 3 月，谷歌更新《人工智能原则》，提出人工智能对社会有益、避免制造或加强不公平的偏见、建立并测试安全性、对人负责、结合隐私设计、坚持科学的高标准等原则。该文件同时声明谷歌不会将人工智能技术应用于武器开发，也不会将人工智能用于可能侵犯人权的活动。

2022 年 6 月，微软发布新版《负责任人工智能标准》，提出公平性、可靠性和内部安全性、隐私和外部安全性、包容性、透明度和问责制六项基本原则，用于指导人工智能工作。

（2）国内人工智能相关标准现状

2020 年 7 月，国家标准委、中央网信办、发展改革委、科技部、工业和信息化部联合印发了《国家新一代人工智能标准体系建设指南》，形成了标准支撑人工智能高质量发展新格局。

① 研制人工智能安全基础标准

我国首个人工智能安全国家标准《信息安全技术机器学习算法安全评估规范》即将发布，规定了机器学习算法技术在生存周期各阶段的安全要求，以及应用机器学习算法技术提供服务时的安全要求，并给出了对应评估方法。

2022 年，全国信息安全标准化技术委员会（TC260）启动编制《信息安全技术人工智能计算平台安全框架》国家标准，规范了人工智能计算平台安全功能、安全机制、安全模块以及服务接口，指导人工智能计算平台设计与实现。

② 推动关键应用方向安全保护标准

在生物特征识别、智能汽车等人工智能应用领域，针对网络安全重点风险，已经发布多项国家标准。例如，在生物特征识别方向，发布了 GB/T40660—2021《信息安全技术生物特征识别信息保护基本要求》，以及人脸、声纹、基因、步态等 4 项数据安全国家标准。在智能汽车方向，发布了国家标准 GB/T41871—2022《信息安全技术汽车数据处理安全要求》，有效支撑《汽车数据安全管理若干规定（试行）》，提升了智能汽车相关企业的数据安全水平。

（3）基于场景需求，建立动态渐进式的行业标准

尽管国内外适用于智能家电信息安全的标准体系已经初步形成，但针对生成式人工智能应用所带来的数据安全和隐私安全新风险，人工智能算法可靠性、透明性、可解释性、公平性等方面的处理技术尚不成熟、标准仍不健全。算法应用的监管者还是被监管者，都不能准确地测度或评估算法技术创新应用可能带来的风险或价值，由此呈现出“共同无知”的新特征。影响算法治理风险或算法应用价值信息的因素、环境难以被精确计算，风险的浮现具有渐进性，应对的措施具有“后现性”。因此，需要行业联盟和相关机构从智慧家庭应用场景需求角度出发，提出具有针对性的治理的工具与行业标准。此外，这些标准要求要随着技术发展、新场景功能涌现、消费者认知发展等不断动态修订完善。

6. 未来发展趋势和前景

6.1 提升智能模型的能力

大模型增强了 AI 技术的通用性，助力普惠 AI 的实现。未来，大模型有望与场景深度融合，配合专业工具和平台支持应用落地，开放的生态来激发创新，形成良性循环。

虽然目前大模型技术在通用场景上已经令万千用户惊艳，但仍有较大的提升空间。在国家和各大头部大模型企业的推动下，国产大模型技术将不断提升其智能程度，未来将在以下几个关键能力上进行提升：

结果的可信性：虽然目前大模型能生成流畅且看似准确的回答，但它们有时可能生成不准确或误导性的信息。未来随着大模型在各个行业中的影响力提升，结果的可信性和解释性变得越来越重要，这会推动开发更多的技术和框架来理解和解释大模型的行为，以及预测结果的可信度。未来会有越来越多的模型通过大量收集和优化偏好数据，利用人类反馈强化学习（RLHF）方法迭代训练和细化，从而提高可信性。

推理能力：尽管大模型在模式识别和生成任务上表现优异，但在逻辑推理、常识理解和深层次的语义理解方面的能力有待提升，未来的研究可能会集中在提升模型的推理能力和对背景常识的掌握。通过增强对话的一致性、选择高质量样本、并结合人类反馈进行优化，可以使得模型在复杂多轮对话中能更准确地理解和响应，从而提升整体的推理能力。

运算性能：由于大模型训练需要大量的计算资源，如何提升模型训练、推理的效率和降低训练的能耗将是未来的关键研究点。可能会通过量化技术来减少内存占用，针对特定模型的代码优化来提高内存效率，以及根据不同模型的规模选择合适的 GPU。通过结合这些方法，实现对不同规模的模型的高效运算和推理。

中文处理：虽然有些大模型已经可以支持多种语言，但对非英语等主流语言的处理能力仍然有待提升，国产大模型将会加大中文训练集的投入，集中于改善现有模型对中文的处理能力。

代码能力：尽管已有一些大模型具有生成和理解代码的能力，但仍有许多提升空间。未来将提升大模型的代码能力以生成更复杂且准确的代码，甚至参与更高级别的软件设计和开发过程。

多模态交互：现在的 AI 模型大多数是以文本为主，而现实生活中的交流则包含了多种模态，如图像、声音、视频等。未来的 AI 可能会突破以往以文本为主的方式，能够处理和理解多种模态的信息，像人类一样理解和生成图像，声音和文本等多种类型的信息。比如，解析和生成图像或者视频中的内容，将文字描述转换为预期的视觉输出，或通过声音和面部表情理解人类的情绪等。

跨模态理解和生成：跨模态理解和生成将是多模态交互的进一步升级，不仅仅是理解不同类型的信息，还包括在不同模态之间进行转换。例如将文字描述转换为图像，将图像转换为描述，或者让 AI 在理解语境的同时生成匹配的音频和视频等。

6.2 支撑智能家电产品和服务的创新与变革

在大模型驱动下，智能家电行业中个性化和自适应能力将得到进一步提升。基于大模型的深度学习技术，让智能家电能够更好地理解和适应用户的需求与习惯，提升产品用户体验。例如，智能音箱可以通过分析用户的语言习惯和口音，提供更自然、人性化的交互体验，甚至能预测用户的需求，主动提供相关服务。智能电视则可以根据用户的观看历史和喜好，智能推荐符合口味的节目或电影。另外家居大模型通过融合智能传感、智能安防等设备获取多模态数据，实现分析决策并控制智能照明、智能温控等设备，提升多个智能家居设备间的协同能力。

通过大模型，可以显著提升智慧家庭设备的定制化服务能力。以智能冰箱为例，它可以根据用户的饮食习惯，提供营养搭配建议，并推荐相应的食谱。同时，智能空调也能结合环境因素和用户生活习惯，自动进行温度和湿度的调整，为用户创造最舒适的环境。这种高度定制化的服务，不仅提高了用户使用家电产品的便利性，也极大地提升了他们的生活品质。

大模型通过精准的数据分析和预测，使智能家电的个性化和定制化服务达到前所未有的深度和广度。例如，智能洗衣机可以根据所洗衣物的材质、颜色和脏

污程度，自动选择最佳的洗涤程序，从而实现了对各类衣物的个性化清洗；智能烹饪设备则可以根据用户的口味、健康状况和营养需求，提供个性化的菜谱推荐和烹饪指导，还能根据食材的种类和新鲜程度，自动调整烹饪参数。

家电大模型技术通过构建全面感知、实时互联、分析决策、自主学习的智能系统，使机器人自主作业成为可能。AI 通过机器人视觉技术强化机器人的感知能力，通过构建算法模型提升其分析决策、自主学习的能力，从而使机器人能够独立完成作业。

从智能产品、智能场景、智慧家庭进化到智慧生活（图 13），不仅仅是智能功能的进化。

图 13：智能家居产品进阶

智能单品以产品智能水平的提高出发，实现现有产品的智能化改良。

智能场景以生活“微场景”出发，通过简单场景的有限设置，实现场景内产品的互动，满足部分生活场景的需要。

智慧家庭以家庭为单元，打破物理空间的限制，实现产品的控制与产品间的联动。

以上三个阶段的产品，基本是以现有产品形态为基础，采用人工智能、大数据、机器学习、物联网等技术，提高产品的智能化水平和智能协同，一定程度地满足生活水平的提升。

智慧生活是以生活需求出发，通过构建数字世界，实现从意识世界、物理世界、数字世界的协同升维，是真正从生活的维度研究产品的形态。当然，产品的形态概念范畴也从单纯的“硬构件、体”，升级到“硬构体”、“软构体”、“硬构体+软构体”的多形态。在升维的过程中，空间也从“二维”升级到“三维”；时间从“线性”升级到“面”，甚至“立体”。

因此，智能家电产品和服务需要创新与变革，其进化逻辑见图 14。

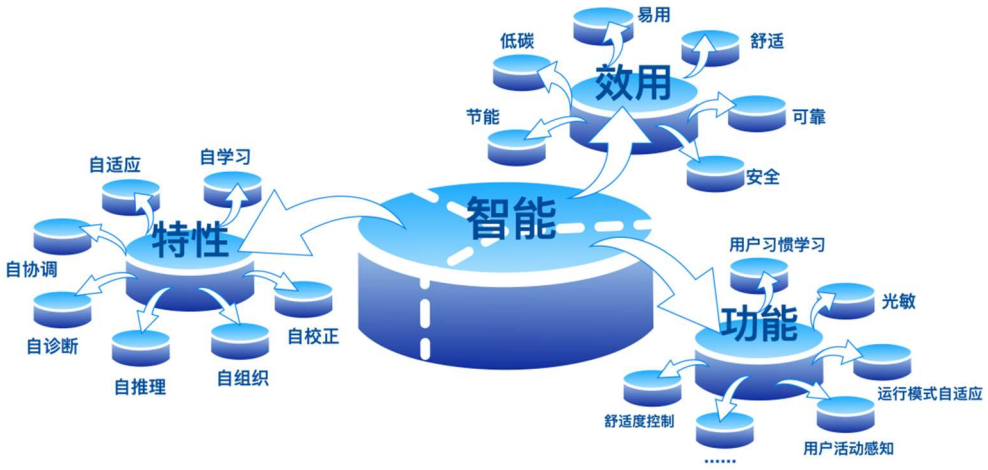


图 14：智能家电产品的进化逻辑

（1） 类生物化

生成式人工智能技术的逐渐普及，特别是家电行业大模型的研究和供给，在算力、算法、算料、知识等智能赋能下，以家庭或产品建立“大脑”的技术路径正在被接受（例如智家大脑），智能家电的“智能能力”得到提高，具有了一定“类生物能力”。人与家电的关系，从“人找家电”的单向交互关系，逐步进化到“人与家电共生”的相互进化、相互帮助的共生关系。

（2） 集成和家居一体化

从物理空间看，家庭的居住面积正在趋于稳定，家电的供给型号却在不断增加，给家庭空间的利用带来了一定的挑战。一个典型的现象是厨房小家电无处存放，集成化和家居一体化的方式可以提高空间的利用率，特别是集成使用频率比较低的产品尤为重要。

（3） 个性化

智能家电的特点是个性化，具有根据环境、空间等适配能力。例如智能吸油

烟机，从排风量、风压的比拼，到智能适配环境、空间的“刚刚好”。以适配性为主线，中国家用电器研究院组织海尔等头部企业，发布了 T/CAS720—2023《家用吸油烟机智能运行噪声声舒适性评价技术规范》。

（4） 节能与低碳

在“30・60”双碳战略下，智能家电、智慧楼宇等能源管理、节能低碳也将是一个重要的方向。通过人与环境、空间、气候等多模态的智能感知，实现智能按需供给，实现使用过程中的节能。

总之，大模型的引入正逐渐改变智能家电的发展轨迹。它推动了家电产品的个性化和定制化服务能力的提升，使得家电不再是冰冷的机器，而是成为了能理解用户需求，自我学习和自适应的“智能伙伴”。这无疑将为我们的生活带来前所未有的便利和舒适，同时也预示着智能家电行业即将迈入一个全新的发展阶段。

6.3 开放平台与生态合作

随着 AIGC 近期的蓬勃发展以及百模同出的促进，行业逐渐走向了相对健康、认知较为统一的生态圈里面。即以通用大模型训练为主的基础层、以垂直领域为主的中间层和行业具体应用为主的应用层。

图 15：AIGC 三层生态链

第一层，为上游基础层，大模型将作为一种基础设施将 AI 赋能千百行业，是未来人工智能行业的“水和电”。由于预训练模型的高成本和技术投入，因此具有较高的进入门槛。以 2020 年推出的 GPT-3 模型为例，AlchemyAPl 创始人

Elliot Turner 推测训练 GPT-3 的成本可能接近 1200 万美元。因此，目前进入预训练模型的主要机构为头部科技企业、科研机构等。目前在 AIGC 领域，美国的基础设施型公司（处于上游生态位）有 OpenAI，Stability AI 等。OpenAI 的商业模式为对受控的 API 调用进行收费。Stability AI 以基础版完全开源为主，然后通过开发和销售专业版和定制版实现商业获利，目前估值已经超过 10 亿美金。因为有了基础层的技术支撑，下游行业才能如雨后春笋般发展，形成了目前美国的 AIGC 商业流。

第二层，为中间层，如果通用大模型是做 1 公里宽的广覆盖，则垂域模型就是做 1 公里深的精准、可靠、精细化的工作。预训练大模型是基础设施，在此基础上可以快速抽取生成场景化、定制化、个性化的小模型，实现在不同行业、垂直领域、功能场景的工业流水线式部署，同时兼具按需使用、高效经济的优势。随着兼具大模型和多模态模型的 AIGC 模型加速成为新的技术平台，模型即服务(Model-as-a-Service-MaaS)开始成为现实，预计将对商业领域产生巨大影响。Stable Diffusion 开源之后，有很多基于开源模型的二次开发，训练特定风格的垂直领域模型开始流行，比如著名的二次元画风生成的 Novel-AI，还有各种风格的角色生成器等。

第三层，为应用层，是大模型在“千行百业”的具体应用。面向 C 端用户的文字、图片、音视频等内容生成服务。在应用层，侧重满足用户的需求，将 AIGC 模型和用户的需求无缝衔接起来实现产业落地。以 Stable Diffusion 开源为例，它开放的不仅仅是程序，还有其已经训练好的模型，后继创业者能更好的借助这一开源模型，以 C 端消费级显卡的算力门槛，挖掘出更丰富的内容生态，为 AIGC 在更广泛的 C 端用户中的普及起到至关重要的作用。

现在贴近 C 端用户的工具越发丰富多样，包括网页、本地安装的程序、移动端小程序、群聊机器人等，甚至还有利用 AIGC 工具定制代出图的内容消费服务。目前，从提供预训练模型的基础设施层公司到专注打造 AIGC 产品和应用工具的应用层公司，围绕 AIGC 生长出繁荣的生态，技术创新引发的应用创新浪潮迭起；中国也有望凭借领先的 AIGC 技术赋能千行百业。随着数字技术与实体经济融合程度不断加深，以及互联网平台的数字化场景向元宇宙转型，人类对数字

内容总量和丰富程度的整体需求不断提高。AIGC 作为当前新型的内容生产方式，已经率先在传媒、电商、影视、娱乐等数字化程度高、内容需求丰富的行业取得重大创新发展。市场潜力逐渐显现。与此同时，在推进数实融合、加快产业升级的进程中，金融、医疗、工业等各行各业的 AIGC 应用也都在快速发展。

在此基础之上，需要从多个维度进行产业化推进，才能真正完成 AIGC 行业的健康发展和百花齐放的效果。

一是模型合作，这既包含用通用大模型训练行业模型，也包括用行业模型赋能业内玩家。目前行业模型是基于通用大模型基础上，引入行业数据和知识进行再训练的。因为行业模型在产品应用中可能涉及语音形式、视觉形式等，因此若底层的通用大模型只是单模态的，就会涉及到多个大模型的协作调用。即使某一家的通用大模型能力是全面的，但在单独场景中，未必是最优的效果，也会触发使用多家模型的情况。

二是数据合作维度。前面所说的行业模型需要行业数据与知识，一些企业可能也积累了行业数据，但是面临数据零散、重复度高等低数据质量的问题，未来可将此类数据治理方法、数据标签框架开放赋能，为有需求的企业提供解决方案。另外，为了保持行业模型的与时俱进、更多的场景覆盖，可由多家企业联合进行数据训练。通过联邦学习等方法，采用“数据不动、模型动”的方式，在保障各家拥有自己数据安全的同时，又让模型能用各家数据训练。

三是算力合作维度。大模型运行时对算力要求高。除了可以通过技术压缩模型规模之外，还可以通过云-边-端算力协同等方式实现算力合作维度的提升。这就类似汽车的自动驾驶，有的公司为保障产品合理的性比价，将自动驾驶、电池管理、智能座舱响应所需的算力上云。当然，仅就端侧算力而言，芯片与模型如何更好融合，高效调用、发挥算力，也是探索方向。

四是行业标准的建立。基于 AIGC 的智能家电行业标准的建立，能够引导家庭智能化的发展方向，从而对智能家电行业的模型参数的适用量级、模型的训练知识量级、家庭场景安全适用性等方面提供行业标准。

6.4 数据算法安全和伦理规范

在数据算法安全和伦理规范方面，需要从以下几个方面推动：

（1） 制定专门的生成式人工智能安全标准

对于智能家电来讲，在应用生成式人工智能技术的过程中，除了要满足国内外行业中的网络安全、数据安全和个人信息保护等方面现有的法律法规和标准外，为应对生成式人工智能算法、数据使用等带来的安全新挑战，以促进生成式人工智能发展为基本目标，统筹发展和安全，亟需针对生成式人工智能的网络安全问题、数据安全和隐私保护问题出台专门标准，包括但不限于生成式人工智能训练数据安全、人工标注过程安全等方面的标准规范。

（2） 开展生成式人工智能安全检测评价

基于上述网络安全、数据安全和个人信息保护等方面的现有国内外标准，结合生成式人工智能在智能家电上的应用，以安全结果为导向，开展检测评价，确保技术应用合法合规。针对检测评价过程中发现的问题，督促厂商及时整改；开展行业比较测试，针对较好的应用开展行业示范，促进技术应用发展。

（3） 开展生成式人工智能安全风险监测

《生成式人工智能服务管理暂行办法》自 8 月 15 日期正式实施。《办法》明确提出，“国家坚持发展和安全并重、促进创新和依法治理相结合的原则，采取有效措施鼓励生成式人工智能创新发展，对生成式人工智能服务实行包容审慎和分类分级监管”。基于这个原则，对生成式人工智能应用过程中遇到的风险进行监测、风险评估，并针对性的动态更新监测方案，推动安全标准不断完善。

参考文献

[1] 《生成式人工智能服务管理暂行办法》（2023 年 7 月 10 日颁布，2023 年 8 月 15 日实施）.

[2] 生成式大模型安全与隐私白皮书，之江实验室.

[3] 人工智能安全标准化白皮书（2023 版）.

[4]《生成式人工智能的三大安全风险及法律规制——以 ChatGPT 为例》，中国国际贸易促进委员会北京市分会.

[5]《中国智能家电信息安全发展白皮书》.

[6] 赵志东，蔡佳雯.解读欧盟人工智能法案：四种 AI 系统风险类型的划分及监管措施（https://mp.weixin.qq.com/s/F2t3onTI_H79vApWwd8qLg）.

[7] Vaswani A, Shazeer N, Parmar N, et al. Attention is All You Need [J]. Advances in Neural Information Processing Systems, 2017, 30.