中国高新技术产业导报/2023 年/4 月/17 日/第 003 版
热点

生成式 AI 成“团宠”如何合规发展

本报记者　李洋

最近，业界流传，不做大模型的大厂很有可能在新一轮洗牌中掉队。

4 月 7 日，阿里云官方宣布，上线自研大模型聊天 AI“通义千问”，并定向邀请企业用户进行测试。4 月 10 日，商汤科技宣布推出大模型体系“日日新大模型”。与此同时，腾讯、华为、科大讯飞等国内科技公司都相继发布 AI 大模型新产品，它们的技术路线各不相同，既有采用类 ChatGPT 模式的，也有采用多模态混合模式的。

值得注意的是，在国内市场如火如荼的同时，“不要登录 ChatGPT!”“暂时远离人工智能和 ChatGPT 概念板块高位股!”最先引爆生成式 AI 的 ChatGPT 正在遭遇各国和地区悄无声息大规模封号。

生成式 AI 大模型未来前景会怎样？国内各大厂商对于 AI 大模型的拥抱态度，会为国内 AI 产业的发展的带来哪些影响？

可为 AIGC 提供有力支撑

“ChatGPT 之所以‘热’的原因除了企业的精彩运作之外，还有一部分原因是其回答问题水平提高出乎意料，而且表现了实事求是。”近日，中国工程院院士、浙江大学教授潘云鹤在人工智能大模型技术高峰论坛上表示。

“AIGC 是对近年来 AI 发展轨迹的归纳。”潘云鹤说，“从实践上讲，只有基于大数据、大知识和大算力的支持，AIGC 才有广泛的发展空间和应用领域，大模型可为 AIGC 提供有力支撑，进而对经济和社会发展产生巨大的影响力。”

据介绍，所谓的 AI 大模型就是一种在大规模宽泛的数据上进行训练后能适应一系列下游任务的模型。

AI 大模型需要的参数量和数据量非常庞大，以 OpenAI 基于深度学习的自然语言处理模型 ChatGPT 为例，它最初的 GPT-1 参数量只有 1.17 亿，到了 2020 年 GPT-3 发布的时候，其参数规模就达到了惊人的 1750 亿。如今，人工智能模型体量已跃升至“万亿级”参数规模，大算力、强算法共同筑起了一道“高不见顶”的技术壁垒，只有深耕 AI 赛道的大公司才有“入场”的资格。

“AI 大模型训练还要依靠互联网大厂。这些大厂自身有资金、算力、数据、生态链，才能形成更好的一个闭环。”北京社科院研究员王鹏认为，各大厂商进行“赛马”，既可以相互促进又可以避免行业垄断；从长远看，对于整个经济社会的智能化转型化有促进作用，从眼前看，有利于形成多个商业模式，从而孵化出更多的好产品和好项目。

各大厂商争相布局

同样是在近日举办的人工智能大模型技术高峰论坛上，华为云 AI 领域首席科学家、国际欧亚科学院院士田奇谈道，过去几年，华为主要聚焦打造“盘古”系列的预训练大模型。其大模型诞生分两个阶段：第一是预训练阶段，由海量数据来运行链路的通用底座基础模型；第二是针对下游的千行百业的具体任务，基于行业数据进行微调。

从发展关键节点看，华为于 2021 年开始立项做盘古大模型；同年 4 月发布了盘古 NLP 大模型、盘古视觉大模型、盘古科学计算大模型；同年 9 月，推出用于药物研发细分场景的大模型；2022 年，与能源集团合作发布了盘古矿山大模型、盘古气象大模型、盘古海浪大模型、盘古金融 OCR 大模型。

此外，近日，阿里巴巴发布的“通义千问”是一款类似 ChatGPT 的大型预训练语言模型，具有广泛的知识储备和普适性，在训练过程中学习大量文本数据，从而具备跨领域知识和语言理解能力，适用于不同场景的需求。

商汤“日日新大模型”包括自然语言生成、文生图、感知模型标注以及模型研发功能。商汤称其大模型从 2019 年开始研发，目前整体参数量达到 5000 亿，今年目标达到万亿。其中，中文语言大模型应用平台“商量”目前参数量为 1800 亿。在超长文本的理解能力方面，在向“商量”提供长达 24 页的《中国专利法》PDF 文件后，“商量”能够快速理解相关法条，并回答用户提出的问题。

据悉，科大讯飞也将于 5 月 6 日发布“1+N 认知智能大模型”。“1”是指 1 个通用认知智能大模型算法研发及高效训练底座平台，“N”是指应用多个行业领域的专用大模型版本，并且将有望带来“N”个场景的示范性产品，或将推动 AI 认知大模型从“可用”阶段迈入“常用”阶段。

潜在需求巨大

各大厂商的争相布局，无疑释放出各行各业对 AI 大模型的潜在需求巨大。

“AIGC 一定不会只用于聊天、画画，而会转向更有价值的应用领域。”潘云鹤建议及时布局实体经济的 AIGC，如新产品、新流程、新药物的智能设计生成；文化艺术的 AIGC，如广告、动漫、影视、绘画、音乐、儿童教育的智能内容生成；城乡发展的 AIGC，如城市规划、美丽乡村、线上会议、生态推演等智能模拟生成。

萨摩耶云科技集团首席经济学家郑磊认为，AIGC 在多方面、多模态方面已经实现的功能，可以大幅提高工作效率，有些功能甚至远远突破了人力工作受到的时间、速度、能力限制，在产业数字化转型方面具有赋能实体经济部门的作用。“在工业方面可以在智能工厂方面有较深入的应用；在消费级也有很多应用，除了用于终端消费者，也可为电商平台赋能，为商家和客户提供更周到、高效、丰富体验的服务功能。”郑磊说。

“面向 AI 时代，所有产品都值得用大模型重新升级。”4 月 11 日，阿里巴巴集团董事会主席兼 CEO、阿里云智能集团 CEO 张勇表示。据了解，阿里巴巴所有产品未来都将接入“通义千问”大模型，进行全面改造。在张勇看来，如同工业革命一样，大模型将会被各行各业广泛应用，带来生产力的巨大提升，并深刻改变人们的生活方式。

“一家企业的想象力终归是有限的，释放 AI 潜力要靠无数人探索。”张勇透露，阿里云会将 AI 基础设施和大模型能力向所有企业开放，帮助更多企业用上大模型，让每家企业都能基于“通义千问”，拥有具备自己行业能力的专属大模型，共同推动 AI 产业的发展。

腾讯方面表示，在这个时间点推出大模型体系，是希望吸引更多下游用户，自然语言模型能够把各种垂直类的任务串联起来，用多模态混合的模式迭代行业场景。

合规管理提上日程

正当 AIGC 市场如火如荼发展之时，业界也开始关注到其潜在的风险，尤其是数据安全和隐私保护。

国家互联网信息办公室近日发布的《生成式人工智能服务管理办法（征求意见稿）》中，明确了提供者在提供服务过程中，对用户的输入信息和使用记录承担保护义务；利用生成式人工智能产品生成内容的提供者，应当对生成式人工智能产品的预训练数据、优化训练数据来源的合法性负责；对于运行中发现、用户举报的不符合该办法要求的生成内容，除采取内容过滤等措施外，应在 3 个月内通过模型优化训练等方式防止再次生成等。

“AI 大模型开发过程中存在一些隐患，比如在数据隐私保护上，生成的结果可能出现错误或不适当的内容，而且社会各阶层对这种大模型的应用是否会大面积取代人类劳动有顾虑，有关其对社会产生的冲击和一系列技术伦理问题，尚需时间进行深入研究和验证。”郑磊认为，AIGC 与人型机器人之间的技术融合研究需要进行必要的技术伦理审查。

王鹏认为，生成式 AI 合规发展需要满足以下几个条件：第一，要对敏感的个人隐私数据、

行业数据、公共安全数据要脱敏脱密，使之符合法律法规的要求。第二，要避免出现行业垄断，影响行业公平竞争，为此，有关部门要提前做好预警研判。三是产业链上各方企业要成立行业性自律组织，加强行业培训和日常评估监测，避免法律风险的产生。