《生成式人工智能服务管理办法（征求意见稿）》发布

生成式AI发展划了安全和规范底线

► 本报记者 张伟

4月11日，国家互联网信息办公室就《生成式人工智能服务管理办法（征求意见稿）》公开征求意见，引发业界热议。

生成式人工智能，是指基于算法、模型、规则生成文本、图片、声音、视频、代码等内容的技术。

“征求意见稿出台正当时。”业内人士一致表示，近期，以ChatGPT为代表的生成式人工智能（AIGC）“高烧不退”，现在距离真正落地和产业应用还有一段距离，国家层面适时征求行业意见，规范发展方向，实现一网管理，是众望所归。

“主要是强调安全性。”中国广告协会数字元宇宙工作委员会秘书长贾振丹指出，强调个人信息、企业信息、政府信息等大数据的安全性，几乎贯穿征求意见稿始终。“这只是征求意见稿的第一版，包括罚款范围也只是在1-10万元以内。实际上未来的几版会更加细化，然后惩罚的条例也会更加清晰。”

“AIGC和元宇宙都不是法外之地，要被监管和治理，和平行的现实世界一样，法律法规将贯穿始终。”贾振丹说。

“与任何新技术一样，AIGC同样会带来数据安全、隐私风险和算法安全等问题。”奇安信集团副总裁张卓指出，全球范围内发生了多起因使用ChatGPT导致的数据泄露事件，各国逐步开始重视AIGC数据安全风险的监管审核。征求意见稿的发布，意味着国家对AIGC的监管治理已经提上日程。

事实上，在全球范围内，各国都在逐步重视对于AIGC的监管力度。美国方面已经开始研究是否需要对ChatGPT等人工智能工具实行检查。美国商务部4月11日就相关问责措施正式公开征求意见，包括新人工智能模型在发布前是否应经过认证程序。而意大利、加拿大等国监管机构也先后宣布将关注ChatGPT及其背后公司OpenAI带来的数据安全风险，并将开启监管调查。

张卓认为，征求意见稿的发布以及全球范围内对于AIGC的监管力度加强，意味着数据安全和隐私保护已经成为AIGC发展的前提和关键。随着AIGC技术的日益成熟和普及，企业应该更加重视数据安全和隐私保护问题，在开展相关业务时积极寻求专业的网络安全技术和咨询服务的支持，确保业务的安全和可靠性。

对于征求意见稿中要求“利用生成式人工智能生成的内容应当真实准确”“采取措施防止生成虚假信息”等内容，中国科学院科技战略咨询研究院研究员、中国科学院大学公共政策与管理学院教授肖尤丹提出，AIGC作为当前人工智能技术应用的重要领域值得相关政策决策者高度关注，但是由于该技术仍然处于快速发展之中，是否有必要立即制定门槛如此之高的应用管理要求，“还有待商榷。”

“征求意见稿对提供者责任设定也过于严苛，甚至对于现行法律法规尚未明确规定的情形，也适用行政处罚。”他提出，根据《行政处罚法》的规定，“尚未制定法律、行政法规的，国务院部门规章对违反行政管理秩序的行为，可以设定警告、通报批评或者一定数额罚款的行政处罚”。但是征求意见稿还规定了“责令暂停或者终止其利用生成式人工智能提供服务”等“限制开展生产经营活动、责令停产停业、责令关闭、限制从业”处罚。

此外，肖尤丹还认为，征求意见稿中对调整对象的表述尚比较模糊，未合理区分技术、产品与服务，仅界定了生成式人工智能是一种技术，但是未界定技术与产品的关系，同时还将研发、利用生成式人工智能产品纳入适用范围。“混淆了面向特定公众的人工智能产品研发服务与面向不特定公众以特定人工智能产品为基础提供信息生成服务。”

他举例说，比如“在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取措施防止出现种族、民族、信仰、国别、地域、性别、年龄、职业等歧视”，并非是“提供生成式人工智能产品或服务”而是研发或者优化人工智能产品或服务。“这将导致该办法在未来适用上存在较大的灵活性和不确定性，或将对人工智能研发和应用产生不利影响，值得探讨。”

而在赛智产业研究院院长赵刚看来，征求意见稿明确了诸多内容。如，明确内容虽然是AI技术生成的，也同样要遵守法律法规的要求，尊重社会公德、公序良俗。明确对AIGC服务提供者利用AI生成内容要采取措施来保证内容的合规合法，包括在算法设计、训练数据选择、模型生成和优化、提供服务等阶段均要采取相应措施。明确加强对AIGC服务提供者的管理，包括安全评估、算法备案、信息披露、内容标识等。明确加强对AIGC用户的规范，包括用户实名、用户信息保护等。明确优先采用安全可信的软件、工具、计算和数据资源，促进我国AIGC技术和产业发展。

“国家划个了底线，有利于AIGC技术创新和产业健康规范发展。”他说。

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。

此前已经启动企业测试的“通义千问”大模型在2023阿里云峰会上正式亮相。

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。

码上读报 扫码阅读全文

全面注册制 有望重塑资本市场生态

4月10日，随着首批10家主板注册制企业上市鸣锣敲钟，我国股票发行注册制改革全面落地，这是我国资本市场改革中的又一重要里程碑。

从试点起步，到存量扩围，再到全市场推行，我国资本市场走出了一条尊重注册制基本内涵、借鉴全球最佳实践、体现中国特色和发展阶段特征的注册制改革之路。

注册制改革带来的变化是全方位、根本性的，给市场参与各方带来了实实在在的获得感。数据显示，截至去年年末，注册制下上市公司合计达1075家，IPO融资1.2万亿元，均占到试点注册制以来全市场的一半以上。第一家同股不同权企业、第一家未盈利企业、第一家红筹企业……一大批过去在核准制发行条件下无缘在境内上市的企业，开启了资本市场新征程。一批处于“卡脖子”技术攻关领域的“硬科技”企业登陆科创板，吸引了更多社会资本投早、投小、投科技；创业板更加聚焦成长型创新创业企业，近九成新上市公司为高新技术企业。

《经济日报》2023.4.11
刘晓峰 祝惠春 李华林 彭江

专利聚活力 经济添动力

2月13日，位于江苏苏州的信达生物制药集团的实验室里，研发人员正在解读实验数据，以评估一款在研新药能否对肠癌细胞或胰腺癌细胞进行有效杀伤，同时不会杀伤正常细胞。信达生物人力资源副总裁高剑锋介绍，信达生物已建立起一条包括36个新药品种的产品链，覆盖肿瘤、代谢疾病等多个疾病领域。目前，信达生物申请专利700多件，其中PCT国际专利申请106件，授权专利144件，在全球多个国家和地区开展专利布局。

像信达生物一样，一大批创新型企业从知识产权创造中获得市场竞争的能量，成为拥有自主创新能力的“尖兵”。截至2022年底，我国国内拥有有效发明专利的企业达35.5万家，较上年增加5.7万家；国内企业高价值发明专利拥有量达到96.8万件，同比增长28.7%。

《人民日报》2023.4.12
谷业凯 原韬雄 刘新吾

隐私计算：让数据“可用不可见”

隐私计算又被形象地称为“可用不可见”的技术，是涵盖众多学科的交叉融合技术，目前主流的隐私计算技术主要分为三大类：以多方安全计算为代表的基于密码学的隐私计算技术，以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术，以可信执行环境为代表的基于可信硬件的隐私计算技术。

4月4日，北京国家金融科技认证中心公布了首批“多方安全计算金融科技产品国推认证”名单，包括蚂蚁集团两项产品在内的首批5项产品通过了该认证。这是国内首次对多方安全计算金融领域应用展开认证工作，也是目前国内唯一针对该领域的“认证”，此次认证结果的发布，意味着数据要素市场的相关市场准入标准和监管体系迎来进一步完善。多方安全计算技术能够在保护数据隐私的同时，实现不同机构之间数据的合法合规融合，实现安全的多方数据查询和分析，进一步打破各方之间的数据壁垒，连接数据孤岛，有效实现数据价值的转化与释放。

《科技日报》2023.4.10
张晔

一束线串起一条链

曾经，整车线束产业链的话语权掌握在合资品牌手中，本土企业采用来图加工模式。如今在昆山，这一局面已经改变。

“随着产业链做大做强，我们掌握了设计权，选哪家供应商，自己定。”昆山沪光汽车电器股份有限公司总工程师吴剑，带领沪光的设计团队和昆山德可汽车配件有限公司的研发人员朝夕相处，同步开发新项目。“我的主要工作是把德可供应的零部件图纸画出来，交给沪光统筹设计。”德可研发人员蒋枭辰说。

要设计出一套整车线束，正是靠产业链上的企业如此联动。在昆山，越来越多的供应商“卡”入沪光牵头的这条链。

作为我国重要的汽车零部件制造基地，江苏苏州昆山拥有汽车产业链配套企业1298家，产业链齐全、配套能力出众，2022年总产值约600亿元。以汽车电路的主体——整车线束为例，仅围绕一家龙头民营企业，就有近50家供应商聚集昆山，在这条成熟的产业链上，上下游分工明确，供需合作紧密。

《人民日报》2023.4.13
王伟健