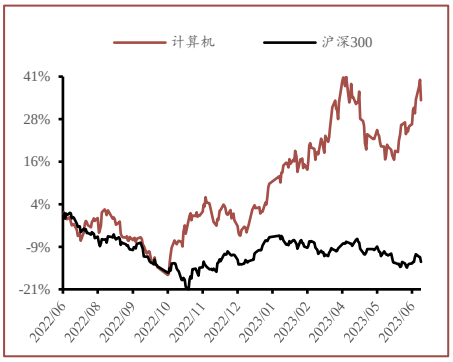
财通证券 CAITONG SECURITIES

AI 监管走到什么阶段了？

证券研究报告

投资评级:看好(维持)

最近 12 月市场表现



分析师 杨烨
SAC 证书编号：S0160522050001
yangye01@ctsec.com

相关报告

1. 《模型成本持续降低，大规模商业变现渐行渐近》 2023-06-19
2. 《AI 带领计算机进入强比较优势阶段》 2023-06-11
3. 《智能汽车行业跟踪：政策扶持，AI 赋能》 2023-06-04

核心观点

- **监管政策推进，行情动能延续：**本周计算机指数小幅下跌 0.13%，跑赢沪深 300 指数 2.37pct，在 31 个申万一级行业中涨幅排名居中靠前，年初至今计算机以 37.31%的涨幅排名第 3。本周网信办发布最新的深度合成服务算法备案清单，对大模型的监管政策进一步明晰，在此催化下计算机板块延续了良好的表现。在其基础上，我们坚定看好板块行情的持续性，并重申前述看好板块的三个出发点：1）基本面提供确定性、2）流动性带来可能性、3）政策力度决定 β 强度。

- **科学的监管实则为创新提供土壤：**本轮 AI 革命发生的实质上源于 OpenAI 对两个技术路线的判断：1）基础算法的规模化（Scale）、2）生成类模型（Generative Model）。如果我们认为 LLM 能真正成为打开 AGI 的金钥匙，那么开发者势必需要在可靠性和性能两大维度上做进一步提升。其中引入新的监管方式，为 LLM 划清合理的边界，对全球开发者来意义重大。中国政府目前强调加强事中和事后监管，在满足备案和审核的基础上降低事前的准入门槛，充分体现了鼓励行业发展，包容审慎监管的政策基调；美国方面则多主体协同，积极推进 AI 监管与现有法律体系的融合；欧洲议会正式通过《人工智能法案》草案，提出 AI 工具的透明度要求，为全球 AI 监管制定者提供了有力的参考。我们认为监管并不扼制创新，科学的监管实则为创新提供更肥沃的土壤。

- **投资建议：**见正文。

- **风险提示：**AI 技术迭代不及预期的风险，商业化落地不及预期的风险，政策支持不及预期风险，全球宏观经济风险。

内容目录

图表目录

1 本周回顾：监管政策推进，行情动能延续

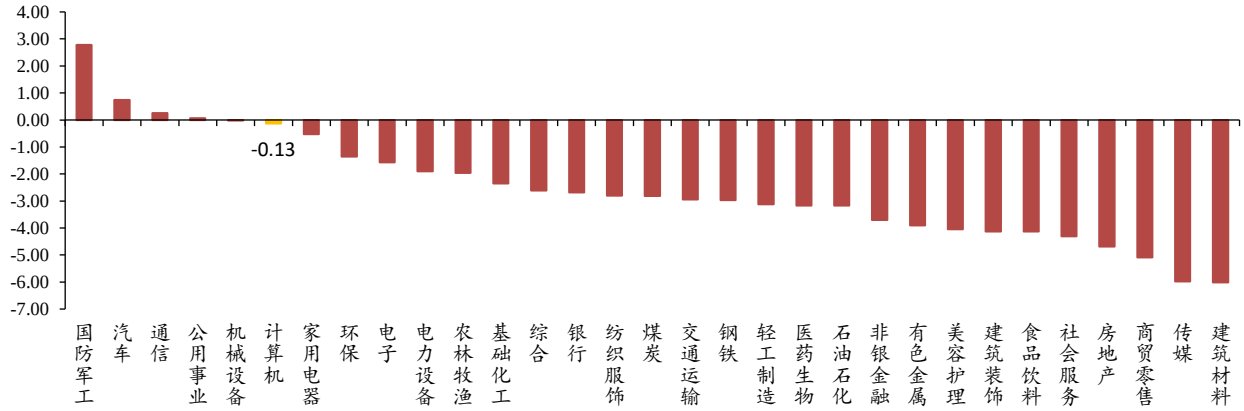
监管政策推进，行情动能延续。本周计算机指数小幅下跌 0.13%，跑赢沪深 300 指数 2.37pct，在 31 个申万一级行业中涨幅排名居中靠前，年初至今计算机以 37.31%的涨幅排名第 3。本周网信办发布最新的深度合成服务算法备案清单，对大模型的监管政策进一步明晰，在此催化下计算机板块延续了良好的表现。在其基础上，我们坚定看好板块行情的持续性，并重申前述看好板块的三个出发点：**1）基本面提供确定性、2）流动性带来可能性、3）政策力度决定β强度。**

图1.计算机板块相对各指数涨跌幅统计（2023.6.19-2023.6.21，单位:%）

代码	名称	近 5 日涨跌幅	年初至今涨跌幅	周相对涨跌幅	年初至今相对涨跌幅
801750.SI	计算机（申万）	-0.13	37.31	-	-
000001.SH	上证指数	-2.30	3.52	2.17	33.79
000300.SH	沪深 300	-2.51	-0.20	2.38	37.50
399006.SZ	创业板指	-2.57	-5.75	2.43	43.06

数据来源：Wind，财通证券研究所

图2.本周各行业涨跌幅统计（2023.6.19-2023.6.21，单位:%）



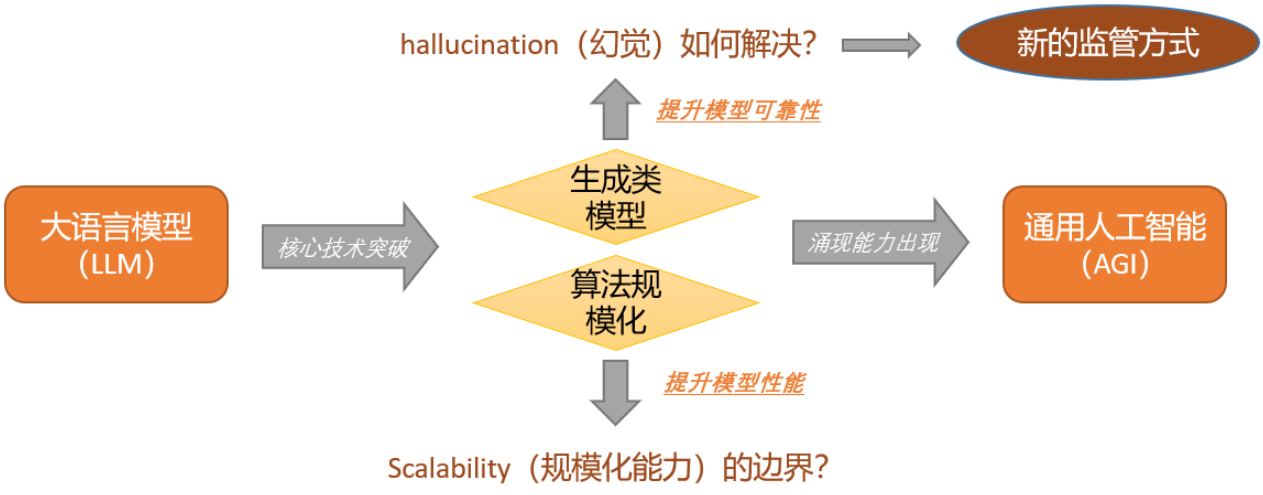
数据来源：Wind，财通证券研究所

2 AI 监管：科学的监管实则为创新提供土壤

科学的监管方式是提升大语言模型可靠性的重要途径。大语言模型（LLM）被创造之初的终极愿景，是实现通用人工智能（AGI）。本轮 AI 革命发生的实质上源于 OpenAI 对两个技术路线的判断：**1）基础算法的规模化（Scale）、2）生成类模型（Generative Model）**。前者用工程化的能力将模型的尺寸和 GPU 强大的并行计算能力进行了耦合；后者通过难度更大但天花板更高的技术路径敲开了 AGI 的大门。然而，技术的突破与未来的潜在瓶颈也正都源于此，LLM 与生俱

来的 hallucination（幻觉）使其输出的内容天生具有可靠性低的特点。**如果我们认为 LLM 能真正成为打开 AGI 的金钥匙，那么开发者势必需要在可靠性和性能两大维度上做进一步提升。其中引入新的监管方式，为 LLM 划清合理的边界，对全球开发者来意义重大。监管并不扼制创新，科学的监管实则为创新提供更肥沃的土壤。**

图3.科学的监管方式是提升大语言模型可靠性的重要途径



数据来源：《Emergent Abilities of Large Language Models》(Jason Wei, Yi Tay 等)，财通证券研究所

2.1 中国：包容审慎、鼓励创新的监管基调，政策呵护 AI 产业发展

政策自上而下角度高度重视本次行业从专用智能到通用智能的技术迈进。4 月 28 日重要会议已指出，要重视通用人工智能发展，营造创新生态，重视防范风险。区别于此前中央经济会议等重要会议中泛指的“人工智能”，本次首次强调“通用人工智能”是对 LLM 开启的 AI 大模型技术路线的高度重视，也标志着行业的发展进入到了全新的阶段。在紧随其后的 5 月，北上深三地也接连发布关于支持人工智能产业政策文件，体现了产业政策对算力、数据、算法、应用、监管等产业发展核心要素及关键环节的难点、堵点的针对性措施。**我们认为各地支持 AI 发展政策接连出台，反映政府对底层技术革新的重视，探索一条界限清晰、包容审慎的监管体系是当前需要落地的核心抓手之一。**

图4.中央及各地政府高度重视通用人工智能行业发展

时间	发布机构	事件
2023 年 2 月 27 日	中共中央 国务院	印发《数字中国建设整体布局规划》
2023 年 4 月 28 日	中央政治局	会议提出，要重视通用人工智能发展，营造创新生态，重视防范风险
2023 年 5 月 23 日	北京市政府	印发《北京市促进通用人工智能创新发展的若干措施》，核心提到为要为通用人工智能的技术发展营造包容审慎监管环境
2023 年 5 月 30 日	上海市政府	发布《上海市加大力度支持民间投资发展若干政策措施》，核心提到要支持民营企业广泛参与数据、算力等人工智能基础设施建设

2023 年 5 月 31 日	深圳市政府	印发《深圳市加快推动人工智能高质量发展高水平应用行动方案（2023—2024 年）》，核心提到要推进“千行百业＋AI”，孵化高度智能化的生产机器人

数据来源：政府官网，财通证券研究所

探索加强事中事后监管，充分鼓励行业发展。大模型的安全可信评估是当前全球开发者和监管方共同面临的难题，有“AI 教父”之称的 Geoffrey Hinton 教授从 Google 离职后多次向大众传达 AI 监管的重要性以及技术上的难点，包括为何打造深度学习检测虚假内容的 AI 系统并不是有效之技。我国目前在 AIGC 内容监管上已经迈出了重要的步伐，2022 年 12 月 11 日，国家网信办发布了《互联网信息服务深度合成管理规定》，提到“具有舆论属性或者社会动员能力的深度合成服务提供者，应当按照《互联网信息服务算法推荐管理规定》履行备案和变更、注销备案手续”，“深度合成服务提供者开发上线具有舆论属性或者社会动员能力的新产品、新应用、新功能的，应当按照国家有关规定开展安全评估”，2023 年 4 月 11 日关于《生成式人工智能服务管理办法（征求意见稿）》公开征求意见，6 月 20 日网信办也根据《互联网信息服务深度合成管理规定》，将智谱、百度、阿里以及科大讯飞旗下的 LLM 登记备案至了 6 月更新的境内深度合成服务算法备案清单（后续依然需要进行安全评估）。**从上述举措中，我们能感知到监管侧目前更多是从数据源去确保真实可信，即强调 AIGC 提供者自身的责任，加强事中和事后监管，在满足备案和审核的基础上降低事前的准入门槛。我们认为这充分体现了鼓励行业发展，包容审慎监管的政策基调。**

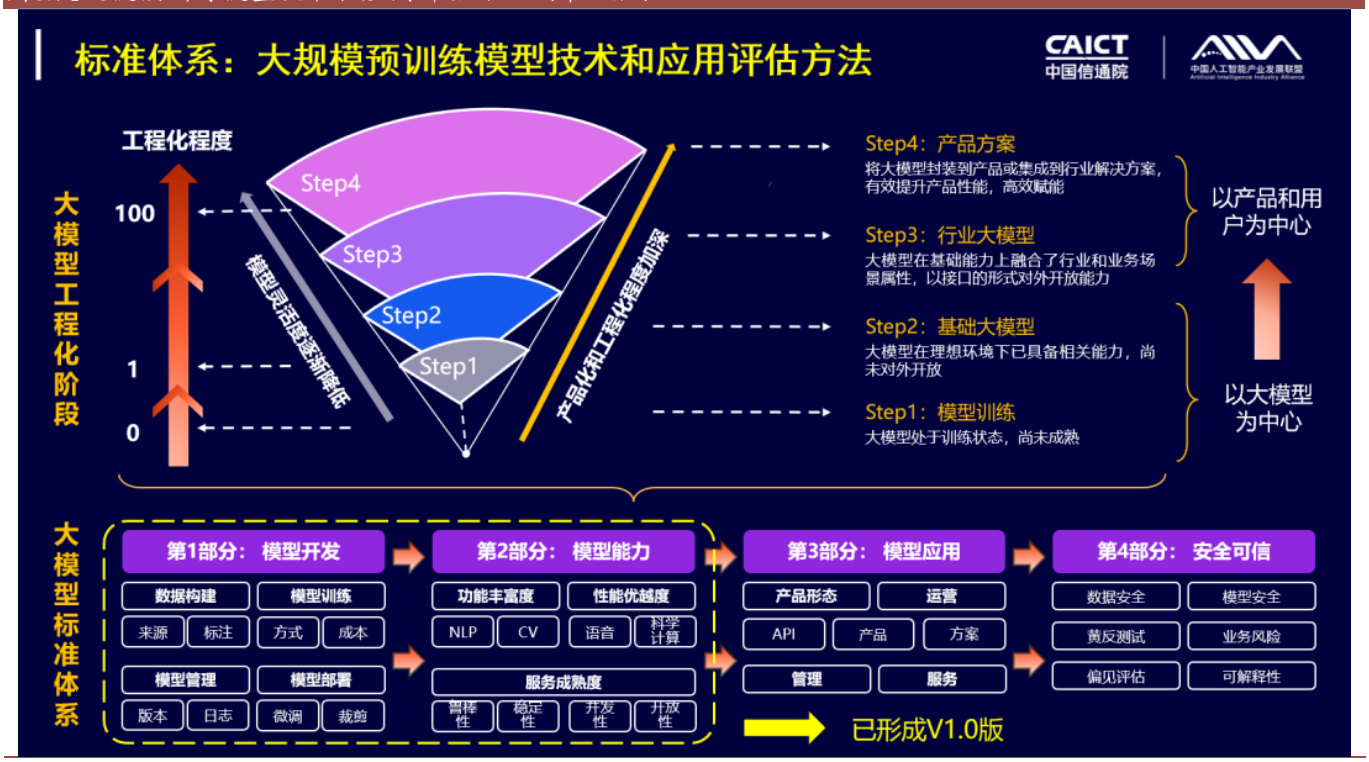
图5.境内深度合成服务算法备案清单（2023 年 6 月，与 LLM 相关部分）

算法名称	角色	主体名称	应用产品	主要用途	备案编号
智谱 ChatGLM 生成算法	服务提供者	北京智谱华章科技有限公司	ChatGLM（网站）	应用于对话生成场景，根据用户输入的文本内容，应用对话模型，生成对话文本回复。	网信算备 110108105858001230019 号
百度 PLATO 大模型算法	服务提供者	北京百度网讯科技有限公司	小侃星球（APP）	应用于对话生成场景，基于飞桨深度学习框架和对话语料训练的对话模型，生成开放域的文本回答。	网信算备 110108645502801230027 号
达摩院开放域自然对话合成算法	服务技术支持者	阿里巴巴达摩院（杭州）科技有限公司	--	应用于对话生成场景，服务于智能对话类的企业端客户，利用对话意图理解、对话内容生成等技术，通过 API 提供对话生成功能。	网信算备 330110507206401230019 号
讯飞星火认知大模型算法	服务技术支持者	科大讯飞股份有限公司	--	应用于开放域对话生成场景，利用文本、代码、prompt 数据及用户反馈数据训练 AI 大模型，服务于问答、咨询类的企业端客户，通过 API 提供文本生成服务。	网信算备 340104764864601230021 号

数据来源：网信办官网，财通证券研究所

中国信通院联合大模型产业各方构建评测体系。自 2020 年开始，信通院就已高度重视 LLM 在国内的发展，已成立覆盖大模型头部企业、互联网企业、科研院所、电信运营商、金融机构等 60 余家单位的工作组，共同研制了《大规模预训练模型技术和应用评估方法》系列标准第一版。今年以来，信通院联合业界标杆企业对大模型的工程化路径进行了进一步深入研究和探讨，按照模型化、能力化、工程化、产业化以及安全可信等需求共同编制《大规模预训练模型技术和应用评估方法》系列标准的第二版，包含模型开发、模型能力、模型运营、模型应用、安全可信五部分。**AI 大模型的安全可控在技术的持续迭代中势必将会是一个长期话题，未来涉及虚假内容，算法公平的议题将仍然对监管形成挑战。我们认为以信通院牵头的第三方评测将为行业的规范化带来良好的补充，产学研的全面融合将有助于大模型评测的加速完善。**

图6.大规模预训练模型技术和应用评估方法（第一版）



数据来源：信通院官网，财通证券研究所

2.2 美国：多主体协同，积极推进 AI 监管与现有法律体系的融合

积极推进 AI 监管与现有法律体系的融合。2022 年 10 月美国白宫发布《人工智能权利法案蓝图》，蓝图围绕安全有效的系统、防止算法歧视、保护数据隐私、通知及说明、人类参与决策制定五方面展开，为人工智能治理提供了支持框架。近期美国国会参众两院两党议员的立法小组也在推出《国家人工智能委员会法

案》(National AI Commission Act)，希望通过该法案成立一个专家委员会，研究和评估美国监管人工智能的最佳方式，近期的 6 月 22 日，美国政府成立了专门针对 AIGC 的工作小组，由商务部下属的国家标准与技术研究院（NIST）负责，处理 AICG 的机遇和挑战，帮助 NIST 制定关键指南。在人工智能法律和政策制定层面，美国白宫、国会和一系列联邦机构（包括联邦贸易委员会、消费者金融保护局和美国国家标准技术研究院等）出台了一系列与人工智能相关的举措、法律和政策。**目前，围绕人工智能治理的最紧迫问题涉及现有法律对新技术的适用性，这将涉及到重大的法律修改和技术复杂性。美国现阶段的人工智能监管的侧重点，在于更多地弄清楚现有法律如何适用于人工智能技术，而不是颁布和应用新的、专门针对人工智能的法律。**

图7.美国近年关于 AI 监管政策及事件一览

时间	发布机构	事件
2022 年 10 月	美国科学和技术政策办公室（OSTP）	《人工智能权利法案蓝图：让自动化系统为美国人民服务》。该文件由白宫科技政策办公室发布，列出了五项原则，以“指导自动化系统的设计、使用和部署，以在人工智能时代保护美国公众”。
2023 年 1 月	118 届美国国会	众议院第 66 号决议，既定目标是“确保人工智能的开发和部署以安全、合乎道德、尊重所有美国人的权利和隐私的方式进行，并确保人工智能的益处得到广泛传播，并且将风险最小化。”
2023 年 2 月	拜登政府	签署了《关于通过联邦政府进一步促进种族平等和支持服务欠缺社区的行政命令》，提出要“指示联邦机构根除在设计和使用 AI 等新技术时的偏见，并保护公众免受算法歧视。”
2023 年 2 月	118 届美国国会	《停止监视法案》（Stop Spying Bosses Act），将禁止雇主为了预测其员工行为，而在工作场所使用自动决策系统进行监视。
2023 年 4 月	FTC 与美国消费者金融保护局（CFPB）、司法部（DOJ）民权司、平等就业机会委员会（EEOC）	承诺将大力执行法律和法规，监督 AI 等技术的发展与使用。
2023 年 4 月	国家电信和信息管理局（NTIA）	发布《人工智能问责制政策征求意见稿》，征求公众对“支持发展人工智能审计、评估、认证和其他机制以建立对人工智能系统的信任”的政策的反馈。
2023 年 5 月	118 届美国国会	HR 3044，该法案将修订 1971 年的《联邦选举活动法案》，设定在政治广告中使用生成式人工智能的透明度和问责制规则。
2023 年 5 月	拜登政府	美国白宫宣布其首个遏制人工智能风险的举措，美国国家科学基金会计划拨款 1.4 亿美元用于新的人工智能研究中心。
2023 年 5 月	美国白宫科学和技术政策办公室（OSTP）	宣布将发布一份公开信息请求（RFI），呼吁所有行业的从业者提供关于雇主利用自动化工具与人工智能追踪、监控、评估和管理工人的信息。

2023 年 6 月	美国众议院	提交《国家人工智能委员会法案》，拟建立的“国家 AI 委员会”，将确保通过监管减轻人工智能带来的风险和可能造成的危害，并在建立必要、长期的 AI 法规过程中起到主导作用。
2023 年 6 月	战略与国际研究中心（CSIS）	参议院多数党领袖舒默发表名为“AI 时代的安全创新”框架，并展现他对国会该如何监管 AI 产业有哪些愿景。
2023 年 6 月	美国参议院	参议院提出一项配套法案。据《华盛顿邮报》报道，法案要求国会和白宫任命来自政府、行业、民间社会和计算机科学领域的 20 人成立一个委员会，制定人工智能监管战略
2023 年 6 月	国家标准与技术研究院（NIST）	将成立一个新的人工智能公共工作组，针对生成式 AI，例如生成代码、文本、图像、视频和音乐的 AI，处理其机遇和挑战，同时帮助 NIST 制定关键指南，指导应对生成式 AI 相关的风险。

数据来源：IAPP 官网，宾夕法尼亚州参议院网站，财新网，澎湃新闻，中华网，科学网，财通证券研究所

2.3 欧洲：欧洲议会正式通过《人工智能法案》草案，提出 AI 工具的透明度要求

欧洲议会批准《人工智能法案》，要求披露生成式 AI 训练数据版权。当地时间 6 月 14 日，经过两年左右的反复商议，欧洲《人工智能法案》（EU AI ACT）得到通过（该法案的最终版本预计要到今年晚些时候才能通过）。该法案禁止存在“不可接受风险水平”的系统（另外三个为高风险、有限风险、低或者轻微风险类型），例如在公共场合进行“实时”或“后期”的远程生物识别技术，并对 ChatGPT 等生成式人工智能工具提出了新的透明度要求。欧盟批准的法律版本提出，任何应用于就业、边境管制和教育等“高风险”用例的人工智能都必须遵守一系列安全要求，包括风险评估、确保透明度和提交日志记录。该法案不会自动将 ChatGPT 等“通用”AI 视为高风险，但对“基础模型”或经过大量数据训练的强大 AI 系统施加了透明度和风险评估要求。例如，基础模型的供应商，包括 OpenAI、谷歌和微软，将被要求声明是否使用受版权保护的材料来训练 AI。**欧盟作为数据隐私保护的全球领头羊，此次通过的《人工智能法案》是全世界第一部通过议会程序、专门针对人工智能的综合性立法。我们认为当面临同样的监管难题，各国陆续出台的政策文件能够互相成为有力的参考，帮助全世界的开发者和监管者共同打造一个健康发展的 AI 生态。**

图8.欧洲近年关于 AI 监管政策及事件一览

时间	发布机构	事件
2016 年 4 月 14 日	欧洲议会	欧洲议会通过了欧盟《通用数据保护条例》，GDPR 赋予了数据主体更多的个人数据操控权利，旨在欧盟内建立一个统一的、回应数字时代发展的高水平个人数据保护框架。由于 GDPR 对个人信息保护范围广、违规惩罚力度大、数据分类全面细致，所以也被广泛认为是欧盟历史上最严格的数据管理法规。GDPR 提供了一整套个人信息保护框架。
2021 年 4 月 21 日	欧盟委员会	2021 年 4 月 21 日，欧盟委员会公布了全球首部全面监管人工智能（“AI”）的立法草案，即《欧洲议会和理事会关于制定人工智能统一规则（人工智能法）和修正某些欧盟立法的条例的建议案》，该草案重点关注数据、技术和基础设施领域。该法案一经通过，将成为欧盟第一部监管人工智能系统的横向立法，也是全球第一个人工智能法律监管框架。
2023 年 6 月 13 日	欧洲议会	欧洲议会通过了一项名为《欧盟人工智能法案》（EU AI Act）的法律草案，AI 系统开发商必须在将该技术投入日常使用之前进行风险评估，类似于药物审批程序。

数据来源：GDPR 官网，新华社，澎湃新闻，财通证券研究所

3 投资建议

AI 大模型赋能下游应用，C 端标准化工具类产品有望率先享受产业红利，建议关注金山办公、万兴科技、同花顺、科大讯飞、福昕软件等。

算力是 AI 大模型产业化落地的必备环节，建议关注 AI 服务器相关厂商以及国产 AI 芯片厂商：浪潮信息、中科曙光、优刻得、紫光股份、海光信息、寒武纪、拓维信息、神州数码等；

生成式 AI 的诞生促使网络安全防护迎来范式转移，AI+安全建议关注：启明星辰、美亚柏科、深信服、安恒信息、奇安信、三未信安、中孚信息、中新赛克等。

4 风险提示

AI 技术迭代不及预期的风险：若 AI 技术迭代不及预期，NLP 模型优化受限，则相关产业发展进度会受到影响。

商业化落地不及预期的风险：ChatGPT 盈利模式尚处于探索阶段，后续商业化落地进展有待观察。

政策支持不及预期风险：新行业新技术的推广需要政策支持，存在政策支持不及预期风险。

全球宏观经济风险：垂直领域公司与下游经济情况相关，存在全球宏观经济风险。

信息披露

● 分析师承诺

作者具有中国证券业协会授予的证券投资咨询执业资格，并注册为证券分析师，具备专业胜任能力，保证报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解。本报告清晰地反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响，作者也不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

● 资质声明

财通证券股份有限公司具备中国证券监督管理委员会许可的证券投资咨询业务资格。

● 公司评级

买入：相对同期相关证券市场代表性指数涨幅大于 10%；
增持：相对同期相关证券市场代表性指数涨幅在 5%～10%之间；
中性：相对同期相关证券市场代表性指数涨幅在-5%～5%之间；
减持：相对同期相关证券市场代表性指数涨幅小于-5%；
无评级：由于我们无法获取必要的资料，或者公司面临无法预见结果的重大不确定性事件，或者其他原因，致使我们无法给出明确的投资评级。

● 行业评级

看好：相对表现优于同期相关证券市场代表性指数；
中性：相对表现与同期相关证券市场代表性指数持平；
看淡：相对表现弱于同期相关证券市场代表性指数。

● 免责声明

本报告仅供财通证券股份有限公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。
本报告的信息来源于已公开的资料，本公司不保证该等信息的准确性、完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的邀请或向他人作出邀请。
本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。
本公司通过信息隔离墙对可能存在利益冲突的业务部门或关联机构之间的信息流动进行控制。因此，客户应注意，在法律许可的情况下，本公司及其所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。在法律许可的情况下，本公司的员工可能担任本报告所提到的公司的董事。
本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。在任何情况下，本公司不对任何人使用本报告中的任何内容所引致的任何损失负任何责任。
本报告仅作为客户作出投资决策和公司投资顾问为客户提供投资建议的参考。客户应当独立作出投资决策，而基于本报告作出任何投资决定或就本报告要求任何解释前应咨询所在证券机构投资顾问和服务人员的意见；