Deloitte.
Insights

掌控全局：使用个人及企业数据训练生成式人工智能

避免使用公共数据训练模型引致风险，越来越多的公司预计将使用企业数据训练生成式人工智能，以提高生产率、优化成本，并获得深度见解。

2023年，生成式人工智能崛起。它一度登上头条新闻，促进初创企业数量爆发式增长，并有望推动全球最大公司重塑战略路线图。人工智能系统首次表现出对话能力、创造力，甚至看似拥有情感，并能呈现出非凡的图像，为复杂的问题咨询提供深入而全面的答案（即使不完全准确）。短短几个月内，大型语言模型（LLM）和视觉扩散模型的能力引发了国际争论，探讨其对全球经济和地缘政治的潜在影响。[1]

生成式人工智能的最初浪潮主要面向消费者，并使用公共数据进行训练，但随着个人数据（包含更多专有数据和领域数据）加入训练，生成式人工智能将迎来一轮更深层次的发展浪潮。积累多年数据的公司如今有机会利用生成式人工智能释放更多数据价值。如能有效释放数据价值，则有助于解决公司目前在使用公共数据训练生成式人工智能模型时面临的部分挑战，但公司或需进行深思熟虑的投资和决策。

2023年企业生成式人工智能支出约160亿美元，德勤预计2024年将再增长30%。[2]尽管企业对生成式人工智能的热情高涨，但大多仍选择谨慎行事，试图挖掘生成式人工智能对企业的具体价值，并确定有效部署、扩展和运行人工智能的成本。[3]

尽管如此，生成式人工智能市场仍在不断扩大，越来越多的企业将支出预算分配给生成式人工智能。2024年，企业大部分生成式人工智能支出预计将支付给领先的云服务提供商，用于训练模型、为用户查询提供计算服务，以及支付给数据科学家，助力连接企业数据与基础模型。然而，2024年，随着大型企业和政府实体力求引入并控制更多生成式人工智能功能，更多的内部数据中心图形处理单元（GPU）市场或出现增长，这与此前数字化转型的生命周期不谋而合，即从云计算到混合云，再到数据中心。阻碍GPU市场增长的主要因素可能是人才获取——从某种程度上来说，也可能是GPU[4]的获取——但企业亦可能面临GPU用例不明和数据质量问题。

公共数据训练模型的利与弊

未来一年，生成式人工智能的能力和成本将接受更合理的评估，恐削弱其强劲势头。用户和用例有望协助阐明生成式人工智能的优势所在，以及其不合时宜或不可信赖之处。云服务提供商正在应对早期公共数据训练模型存在的事实错误、“幻觉”（模型编造一些听似事实的东西[5]）、版权及合理使用等问题，同时这也进一步激励更多企业使用个人数据训练生成式人工智能。[6]

生成式人工智能模型亟需接受大量数据训练，因此第一批公共数据训练模型主要使用公共互联网上大量可用的公共数据进行训练。[7]因此，公共数据训练模型包含了互联网存在的许多偏见、矛盾、不准确性和不确定性。但在某种程度上，这些模型也因此能够交流一系列深度话题，并表现出令人惊讶的创造性、诗歌能力甚至貌似情绪化的行为。为此，需推进训练模型稳健发展、避免有害输出，并提高生成式人工智能回复的准确性和可取程度。

使用社交网络帖子等公共数据训练出来的生成式人工智能模型，在被追问事实时可能会捏造事实。[8]由于该等模型具有权威性，许多用户在未对结果进行适当核实的情况下相信其断言。热门的大型语言模型并不追求事实准确性，而是追求统计准确性。它们非常擅长推测一般人即将进行的会话内容。这一能力再加上模型的“温度”（模型反应中允许存在的随机性）[9]，可导致模型产生幻觉并生成虚假信息，例如，某位律师引用生成式人工智能模型生成的虚假案件摘要提交“判例”。[10]不过，这种能力也激发了模型的创造力，例如利用视觉扩散模型为视频游戏生成新颖的角色设计。[11]

此外，使用公共数据训练的生成式人工智能模型亦违反了有关版权及著作权合理使用的法律，越来越多的创作者因发现模型输出的内容源于自有作品而提起诉讼。[12]扩散模型使用公共数据集来训练图像生成，而公共数据集又涉及版权作品，扩散模型尤为容易招惹麻烦。[13]为此，部分云服务提供商协助网站屏蔽其内容，避免数据被抓取用于模型训练，因此公共数据训练模型寻求训练数据集的难度或将加大。[14]尽管版权法因市场而异，但对现有艺术作品过度衍生或者没有足够人类输入内容的人工智能衍生作品不受版权保护。[15]然而，艺术家和版权持有人很难从包含数十亿不同输入值的训练数据集中证明其衍生性。[16]此外，企业可能会担心如果将其数据添加到公共数据训练模型中，企业将失去数据控制权。当训练数据集所使用的数据被用户无意或通过对抗性提示工程发现时，就会导致数据泄漏。[17]基于上述原因，许多企业对于是否采用使用公共数据训练出来的生成式人工智能还犹豫不决。[18]

领先的生成式人工智能提供商也面临着上述挑战，并承受着发展其业务模式的压力。[19]由于上述原因，他们面临着法律诉讼和监管问题，同时还要斥资来训练和调整生成式人工智能模型，以生成数以百万计的用户日常提示词。[20]大规模训练模型和推理所需的计算成本高昂，因此超大规模数据中心需既有能力提供算力，亦能承担主要的成本和责任。

从面向消费者应用到服务于企业

由于生成式人工智能的基本能力令人信服，但使用公共数据进行训练又或招致不必要的风险，因此越来越多的公司希望开发自己的生成式人工智能模型，使用自有数据进行训练。[21]如此一来，公司可以避免版权及著作使用问题，同时还能定制解决方案，以产生期望行为和值得信赖的结果。

对于大量传媒和娱乐公司而言，生成式人工智能已对内容创作造成颠覆性影响，因为任何人都能生成文本、音频和图像。然而，作者和艺术家纷纷提起诉讼，因为未经同意或未付报酬擅自抓取其作品在公共网络中训练生成式人工智能的常用工具。[22]为避免此类版权使用问题，Adobe Systems[23]和Getty Images[24]均推出了解决方案，可使用经授权的视觉内容（即多年运营过程中积累的照片和数字图像）训练生成式人工智能模型。这些工具生成的新图像明确属于其内容库的许可和再利用协议范围，有助于规避版权问题，同时为创作者提供多种变现方式。

不过，公司仍需遵守相关数据类型（如个人身份数据或医疗信息）的领先实践和法规。将私人数据和公共数据合并的公司可能也面临类似挑战，既要有效整合这些数据，又要遵守数据隐私和版权法。然而，这些都是会话学习系统，虽处于早期发展阶段，但在发现和放大数据价值方面已初露发展潜力。

如果数据如许多人所说是“新石油”，大型语言模型和扩散模型则可能提供更高性能的引擎，助数据一臂之力。许多公司已沉淀大量数据，生成式人工智能可助其实现数据的可操作性。生成式人工智能为公司提供更好的数据视角，将会话和可视化界面与海量数据计算能力结合起来，这样的能力远超出了人类的推理。展望2024年，生成式人工智能不仅将影响更多公司的运营和产品线，还将助力公司的首席高管和董事会发挥作用。

小结

越来越多的公司希望借助生成式人工智能来提高生产率、优化成本。公司亦可凭借生成式人工智能能力，分享复杂的洞察、发现错误和欺诈、降低决策风险、寻求优化、预测机遇，甚至增强创新，从而释放更多数据价值。部分公司已着手开发特定领域的解决方案，未来一年内或初见成效。[25]事实上，越来越多的公司开始释放生成式人工智能的竞争优势，因此可能存在潜在风险。不过，开发和运营成本、价值链不同环节的部署位置，以及如何设置防护栏并确保结果准确可信等方面有待商榷。

企业使用个人数据训练生成式人工智能模型可避免出现一些缺陷，但仍需确保其可信度和准确性。将训练数据集限定于特定领域，可缩小生成式人工智能的回复范围。强化学习[26]和人类反馈[27]有助于引导生成式人工智能模型朝着有利于人类偏好的方向发展，但熟知自身数据的企业应带头开发奖励模型、优化政策。[28]这些举措有助于解决人工智能幻觉和偏见问题，但亦存在自身的局限性。[29]通过优化特定结果，模型的新颖性和创造性会逐步降低。[30]如果处理得当，反馈可以增强这些特定领域的专业知识和超人推理能力。[31]

企业计划开发自身模型时应考虑成本问题。模型的开发可能相对容易，尤其随着新的开源模型进入市场。特定公司应根据用例试图了解模型所需的规模、有效训练模型所需的数据量，以及启动和运行模型所需的算力。公司的数据集质量参差不齐，应对这些数据加以调整并汇集到数据库中。[32]随后对数据进行整理。由于企业熟知其自身数据，因此企业是准确标记训练数据集的最合适人选。

生成式人工智能模型拥有数十亿个参数，需要使用超大规模数据集进行训练。因此算力需求极高。[33]公司可能需要与超大规模云服务提供商合作，并计划支付服务周期费用，或者购买自身的硬件，但购买和运营成本高昂。[34] 训练可能是最昂贵的环节，但训练有素的模型能够响应查询。如果查询工作负载大，推理成本也会上升。这意味着企业应慎重考虑开发、部署和运行模型所需的人才、算力和时间成本，并与预期的投资回报率进行比较。如企业拥有明确目标和目标实现路线图，可保持项目正常运行，同时及早发现收益或损失。

生成式人工智能模型训练所需的算力和专业知识亦推动公司考虑部署和合作者的问题。与现有的云服务提供商合作乃明智之举。随着公司规模扩大，或者公司如果拥有专有或敏感数据，可能会选择部署混合数据中心或内部数据中心。如此一来，公司就应像对待任何其他关键服务一样，考虑到数据中心的冗余和安全问题。更重要的原因在于，受到攻击的系统可能会泄露有关公司数据的深度情报，或者对抗攻击导致可信赖的人工智能被利益相关者操纵。

在大多数情况下，生态系统方法可以通过分配投资、专业知识和风险而获益。然而，每家公司都应考虑如何以最佳方式实现其目标。根据成本、绩效、安全性、数据类型和战略目标的独特需求，公司应采取不同途径、“恰当”的方法。这是一个发展迅速、资金雄厚的领域，其用例、机遇和影响力才刚刚开始显现。

人工智能进入首席高管层和董事会

展望未来，如果企业拥有自己的智能学习系统，将意味着什么？人工智能原生组织是什么样的？它在多大程度上与业务战略保持一致，而非以人为本？会话式大型语言模型可以从您的数据或竞争对手的模式中发现你无法发现的东西，这有何影响？公司可能很快就会拥有多个代理开展众多工作流程，不仅负责运营，还负责规划和决策。

随着这些系统建立起价值和信任，可进一步提升决策层次，并有望成为首席高管或董事会的对话声音。[35]这种可能性通常被认为是科幻情节，但在2024年，似乎近在咫尺、值得期待。

归根结底，企业领导者将承担实验和精心策划的职责，确定生成式人工智能对公司利润的助益。生成式人工智能的能力能否真正实现差异化的财务业绩和竞争优势？如果能，该竞争优势能持续多久？生成式人工智能会成为企业业绩新的必备能力吗？退一步说，有哪些信号表明生成式人工智能是渐进式变革还是革命性变革？

作者

Chris Arkenberg
United States

Bariş Sarer
United States

Gillian Crossan
United States

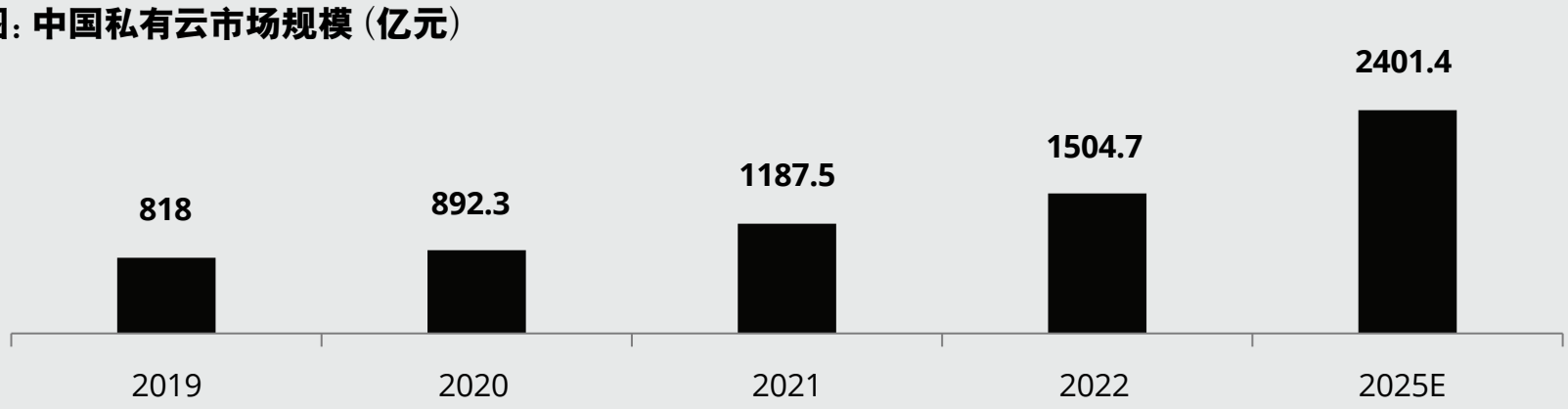
Rohan Gupta
United States

大模型私有化加速部署，行业经验将是成功关键

随着人工智能的快速发展，大模型正快速的扩展到各种应用场景。在自然语言处理、计算机视觉等领域，大模型已经取得了重大突破，为各行各业的智能转型提供了强有力的支持；然而，大模型也面临一些挑战，尤其是数据安全和隐私问题。对企业来说，私有数据具有极高价值，因此，采用私有化AI部署的需求潜力巨大。企业倾向于采用私有化方式部署大模型，以解决数据安全和隐私问题。通过私有化部署，企业可以将其数据用于大模型训练，从而确保数据的安全和隐私。未来中国大模型私有化市场将呈现以下主要趋势：

1. **私有云成AI大模型算力主流**。在进行大规模、连续的AI训练时，私有云比公有云具有更高的效率和更低的成本等优势；因此，现在有越来越多的企业开始倾向于使用私有云。此外，由于AI训练需要处理大量高度敏感的内部数据，私有云具有高度安全性，使其成为更适合的解决方案。

图：中国私有云市场规模（亿元）



数据来源：CCID

2. **私有化AI部署将更广泛的在各行业中铺开**。大模型的企业用户行业分布比较广泛，目前来看，能源以及金融行业私有化大模型部署的占比较高。一方面，这些行业的的数据基础设施较为完备；此外，业内大型企业数量较多，能够支撑私有化部署资金。随着AI应用普及，预计未来私有化AI会在更多行业中展开，包括零售、医疗保健、制造业、公共服务领域等。

3. **新型数据技术（如：向量数据库）以契合私有大模型数据量大而多样的需求**。过去AI模型训练的数据量较小、数据类型较单一的场景下；而如今训练数据量已经发生量级变化，且行业、企业所拥有数据各有不同；在此背景下，向量数据库等新技术的应用将变的更广泛，未来将成为智能化数据调度平台的中枢。例如，腾讯云已经全面升级向量数据库多项核心性能，最高支持千亿级向量规模和500万QPS峰值能力。

4. **国内私有大模型技术的发展使得未来选择更为丰富**。不同于国外大部分企业可能会直接选择OpenAI，国内大模型的选择会更为多样。虽然国内大模型虽起步较晚，但随着国内大模型技术的加速发展，以及训练量的累积，国内头部大模型厂家已经缩小与国外大模型的差距。2023年，国内已有11家大模型通过了《生成式AI服务管理暂行办法》备案，首批国产大模型将获批上线，这将进一步推动大模型私有化部署的商业模式发展。

5. **行业经验将成为大模型私有化解决方案厂商的核心能力**。除了通用大模型开发以外，国内企业也开始在其通用大模型的基础上，基于各行业的行业特征，帮助行业客户定制、训练私有大模型。由于各行业的数据体量、数据类型、业务模式各有不同，未来AI大模型厂家将更专注行业专业数据和行业经验的积累，未来大模式的竞争主要聚焦在场景应用，而私有化、垂直化、企业化、个人化的专有大模型、深度定制的解决方案将成为企业的发展重点。

作者

钟昀泰
中国

尾注

1. David Solomon, Eric Schmidt, “The future of generative AI,” Goldman Sachs, September 13, 2023.

2. Michael Shirer, “IDC Forecasts Spending on GenAI Solutions Will Reach $143 Billion in 2027 with a Five-Year Compound Annual Growth Rate of 73.3%,” IDC, October 16, 2023.

3. Katyanna Quach, “Despite the hype, generative AI is not a significant chunk of enterprise cloud spend,” The Register, September 12, 2023.

4. Lucas Mearian, “Chip industry strains to meet AI-fueled demands — will smaller LLMs help?,” Computerworld, September 28, 2023.

5. Janakiram MSV, “How to reduce the hallucinations from large language models,” The New Stack, June 9, 2023.

6. Tiana Garbett et al, “Generative AI and Copyright – Some Recent Denials and Unanswered Questions,” The National Law Review, October 4, 2023.

7. Sharon Goldman, “Generative AI’s secret sauce – data scraping – comes under attack,” VentureBeat, July 6, 2023.

8. Sascha Heyer, “Generative AI – understand and mitigate hallucinations in LLMs,” Google Cloud Community, Medium.com, June 13, 2023.

9. Sascha Heyer, “Generative AI – mastering the language model parameters for better output,” Google Cloud Community, Medium.com, June 12, 2023.

10. Benjamin Weiser, Nate Shweber, “The ChatGPT lawyer explains himself,” The New York Times, June 8, 2023.

11. Shannon Liao, “A.I. May Help Design Your Favorite Video Game Character,” The New York Times, May 22, 2023.

12. “From ChatGPT to Getty v. Stability AI: a running list of key AI-lawsuits,” The Fashion Law, October 19, 2023.

13. James Vincent, “Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement,” The Verge, February 6, 2023.

14. Danielle Romain, “An update on web publisher controls,” The Keyword, Google, September 28, 2023.

15. Christopher Hutton, “Generative AI set for era-defining clash with copyright law,” Washington Examiner, April 20, 2023.

16. Blake Brittain, “US judge finds flaws in artist’s lawsuit against AI companies,” Reuters, June 19, 2023.

17. Jaydeep Borkar, “What can we learn from Data Leakage and Unlearning for Law?,” Cornell University, July 19, 2023.

18. Carl Franzen, “More than 70% of companies are experimenting with generative AI, but few are willing to commit more spending,” VentureBeat, July 25, 2023.

19. “Why Gen AI adoption among businesses will look radically different in 2024,” Code and Theory, Medium.com, September 13, 2023.

20. Will Oremus, “AI chatbots lose money every time you use them. That is a problem.,” the Washington Post, June 5, 2023.

21. “AI is setting off a great scramble for data,” The Economist, August 13, 2023.

22. Christopher J. Valente et al, “Recent trends in generative artificial intelligence litigation in the United States,” K & L Gates, September 5, 2023.

23. Ashley Still, “Reimagining our video and audio tools with Adobe Firefly,” Adobe Blog, April 17, 2023.

24. “Getty Images launches commercially safe generative AI offering,” Getty Images Newsroom, September 25, 2023.

25. Jamiel Sheikh, “Bloomberg uses its vast data to create new finance AI,” Forbes, April 5, 2023.

26. Cameron Hashemi-Pour, “What is reinforcement learning?,” TechTarget.

27. Jan Leike et al, “Learning through human feedback,” Google DeepMind, June 12, 2017.

28. Dimitriy Konyrev, “Reinforcement learning with human feedback (RLHF) for LLMs,” SuperAnnotate, April 27, 2023.

29. Ben Dickson, “The challenges of reinforcement learning from human feedback (RLHF),” TechTalks, September 4, 2023.

30. Jithin James, “The Impact of Temperature in LLMs: Balancing Determinism and Creativity,” Medium.

31. Jan Leike, “Learning through human feedback,” Google DeepMind, June 12, 2017.

32. Tom Davenport and Maryam Alavi, “How to Train Generative AI Using Your Company’s Data,” Harvard Business Review, July 6, 2023.

33. Sid Sheth, “Generative AI drives an explosion in compute: The looming need for sustainable AI,” SiliconAngle, February 5, 2023.

34. Guido Appenzeller et al, “Navigating the high cost of AI compute,” Andreessen Horowitz, April 27, 2023.

35. Stanley McChrystal, “AI has entered the situation room,” Foreign Policy, June 19, 2023.

致谢

Cover image by: **Manya Kuzemchenko**