警惕GEO滥用风险 别让AI数据“中毒”

从出行选酒店到居家挑家电,从对比数码产品到甄选日用好物,生成式AI早已融入大众日常决策的方方面面,比起手动搜索信息,人们更愿意直接“问AI要答案”。

AI给人们带来了很多便利,但AI给出的结果就一定“客观”吗?日前,中央广播电视总台第36届“3·15”晚会曝光了生成式引擎优化(Generative Engine Optimization,简称GEO)行业存在的虚假信息投放、对AI大模型进行数据“投毒”等乱象,直指部分企业滥用GEO技术制造虚假数据、干扰AI决策的行业乱象,引发社会对AI大模型“投毒”问题的广泛关注。

SEO与GEO是什么

互联网早已成为公众获取信息的主渠道,与之相伴的各类信息“优化”策略也应运而生。

在搜索引擎时代,为让自身在搜索结果中排名靠前,SEO(搜索引擎优化)成为商家网络营销的重要手段。SEO是利用搜索引擎内在规则,优化网站结构和内容,从而提升网站在搜索引擎结果中自然排名的方法,其核心目标是提高网站可见性、获取品牌效益,为企业或个人赢得更多流量和市场竞争优势。

该技术的核心原理是优化网站结构、内容和外部链接,使其更契合搜索引擎的抓取和索引规则,进而提升可见度和流量,兼具成本低、长期有效的优势,但受搜索算法更新影响较大,优化策略需随算法调整不断完善,应用范围也覆盖电子商务、企业品牌推广、内容营销等多个领域。当前的SEO研究,不仅围绕技术优化展开,还关注用户搜索行为分析、算法公平性以及人工智能对搜索排名的影响,为数字营销和信息检索提供重要支持。

GEO的概念诞生于2024年6月。印度理工学院德里分校、普林斯顿大学的学者及部分独立研究者在arXiv上发表论文,首次提出了GEO的概念、框架及相关实验设计。作为SEO技术的自然延伸,GEO通过优化内容以适配AI检索与引用,提升商业品牌在AI模型中的可见度。这项技术的初衷是帮助优质内容更好地被搜索系统或AI系统理解,助力优质内容的传播与触达。

GEO相对SEO的优势

与传统SEO相比,GEO代表搜索优化的范式跃迁。传统SEO以关键词密度、外链数量和技术指标驱动网页排名,用户需点击链接后消化信息。GEO更突出对生成式AI引擎运作逻辑的适配,例如理解AI如何抓取、解析和重组信息生成回答。

二者在技术路径上高度统一:均依赖结构化数据标记(如Schema)增强机器可读性,强化EEAT信号(专业性、权威性、可信度)建立内容可信度,并通过语义分析与多模态优化适应复杂查询场景。GEO则直接优化内容在AI生成答案中的“引用权”,用户无需跳转即可获得决策依据。这使曝光效率提升3倍至5倍,用户决策成本降低50%以上。GEO的适用场景与SEO完全重合,主要覆盖商业决策(如产品对比)、权威建设(如行业报告引用)、公共知识服务(如政策解读)三大领域。

GEO的中立性与滥用手段

GEO是为提升特定内容在生成式人工智能特定场景回答中的可见性,对内容的语义、结构、获取渠道和方式等进行针对性优化的一种综合性策略。其本身是“中立”的,平等地放大内容的“好”与“坏”。然而,部分企业为获取短期流量红利,滥用GEO污染网络数据。其滥用手段主要可分为以下三种。

一是虚假内容制造。通过伪造专家或权威机构背书、编造用户评价、捏造产品性能对比等方式批量生产虚假或夸大信息,使相关内容更容易被人工智能模型检索和引用,影响模型回答结果。

二是批量内容轰炸。通过内容农场、自动化生成工具等方式在多平台集中发布大量相似或高度重复的信息,通过多源传播刻意制造信息共识,诱导人工智能系统误判信息可信度。

三是隐性操纵优化。在网页中嵌入隐藏标签、结构化提示或针对模型偏好的特定语句,通过技术手段提升相关内容被人工智能抓取、排序和引用的概率。

GEO滥用的多重风险

GEO滥用不仅污染人工智能数据土壤,还会进一步对模型的安全性和可信性造成严重冲击,具备渗透深入、隐蔽性高、溯源治理难等特点,具体风险主要体现在以下三个方面。

其一,滥用GEO生成大量虚假数据深度污染AI数据土壤。在利益驱动下,部分企业滥用GEO在多平台投放大量看似可靠但低质虚假的数据,生成大量人工智能偏好的低质、虚假信息,造成AI数据土壤被严重污染。

其二,GEO滥用防范能力不足进一步降低AI可信度。当前,AI模型对虚假数据的识别防范能力不足,投其所好生成的虚假数据容易被大模型获取并引用,大模型可信度大幅降低,长此以往将深度影响AI产业的应用发展。

其三,GEO服务行业存在治理空白,部分服务商安全合规失守。由于GEO服务缺乏明确的治理要求和行业标准评价体系,部分GEO服务商能力不足或不负责任,一味迎合客户诉求,造成大量虚假数据被创建和散播,且难以追溯定责。

监管发力规范GEO发展

在业内人士看来,恶意投喂数据操纵AI推荐并以此牟利的行为,不仅违反了《中华人民共和国广告法》《中华人民共和国反不正当竞争法》《中华人民共和国消费者权益保护法》等法律规定,也违反了《生成式人工智能服务管理暂行办法》等部门规章要求,严重扰乱正常市场经济秩序,危害人工智能信息系统安全。

更值得警惕的是,这一灰色产业链的规模已不容小觑。据中国互联网络信息中心数据,截至2025年6月,我国生成式人工智能用户规模达5.15亿人,利用AI回答问题的用户占比高达80.9%。营销研究机构预测,2030年中国GEO行业市场规模将达到240亿元。

GEO从需求、优化、投放、传播到被用户看到,环环相扣、缺一不可,任何一段失守,整个体系都会失效。因此,GEO可信健康发展,需要GEO全链路相关方协同努力,共助AI可信发展。GEO服务商是构建可信GEO的核心主体,GEO服务企业需增强责任意识并加强可信服务能力,建立客户准入与内容审核机制,识别并拒绝违规优化需求,保留优化过程日志和内容版本记录,支持事后溯源与责任认定,采用客观、可验证的正向GEO手段实现内容优化。

针对这一乱象,监管层面已经及时亮剑。市场监管总局在1月29日发布的《2026年全国广告监管工作要点》中明确,将聚焦AI生成广告等互联网广告监管重点难点问题开展集中整治;3月3日,中国信息通信研究院人工智能研究所正式启动首轮《生成式引擎优化(GEO)可信基本要求》评测工作。通过建立行业评测标准,引导GEO行业回归合规发展轨道,为人工智能行业的健康发展筑牢防线。

董敏炜 综合报道,素材来源:央视财经、中国信息通信研究院、消费日报财经、中华网财经、北京日报、科普中国、新华网等