

语言风险剖析与安全应对策略

——评《语言与安全研究(第一辑)》

在信息爆炸与网络社交蓬勃发展的当下,语言作为沟通载体正面临前所未有的风险挑战。语言风险是指在交流传播过程中,因语义模糊、情感误导、价值偏差等因素引发的误解、冲突或社会危害现象。对其进行剖析与应对关乎社会稳定、文化传承及个体权益保障。在多元话语交织的复杂语境中,识别语言风险根源、构建安全应对机制,已成为维护健康语言生态、促进理性对话的迫切需求,亦是维护社会稳定与推动社会文明进步的重要基石。

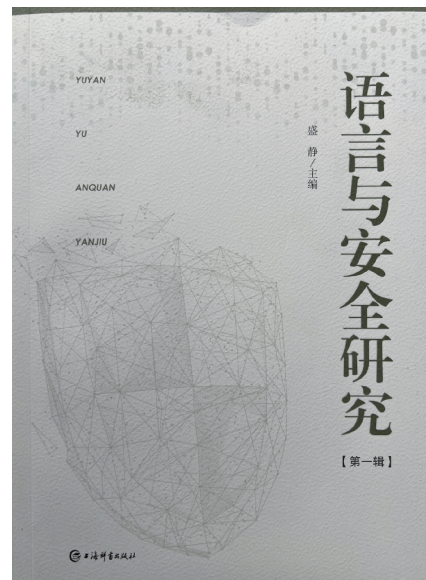
语言安全研究是守护文化根脉的关键防线,它通过剖析语言传播中的潜在风险,如信息篡改、文化误读,维护群体认同与价值传承。语言安全研究可为政策制定提供科学依据,如规范网络用语、防范语言暴力,促进社会和谐。其价值不仅在于保存语言本身,更在于通过语言安全维护人类文明的多样性与可持续发展,是文化自信的重要基石。《语言与安全研究(第一辑)》一书立足百年变局与全球治理挑战交织的时代背景,以总体国家安全观为指引,收录了国内学者关于“语言与安全”的跨学科研究成果,涵盖政治安全、军事安全、网络安全、公共卫生安全、海外利益安全等多维度议题,并设“互译互鉴”专栏,引入国际经验,通过“述评”拓展理论视野。该书以论文集形式整合语言学、安全学及文化研究理论资源,通过实证研究与理论对话,界定“语言与安全”的内涵边界,勾勒其学科框架,为语言安全学或安全语言学的学科建设奠定基础,助力国家安全研究的理论创新与实践应用,具有鲜明的时代性与学术前瞻性。

编者指出,在全球化信息交互场景中,语言作为核心载体常隐含结构性风险。以“语义模糊性”为例,其本质是语言符号的多义性与语境依赖性形成的认知裂隙,在跨文化协作、法律文本解读、数字通信等场景中易引发连锁风险。语义模糊性风险具象表现为:合同条款中的“合理时间”因缺乏量化标准导致履约纠纷;技术文档中的“适当压力”因操作员文化背景差异引发设备误操作;社交媒体中的隐喻表达被恶意解读为煽动性言论。这类风险具有潜伏性、扩散性和非线性特征——初始误解可能通过信息链式传播演变为系统性危机。应对策略需构建“三维防控体系”。在编码层,实施“显性化改造”,对关键术语建立多维度释义框架,如将“高温环境”细化为 $\geq 40^{\circ}\text{C}$ 或相对湿度 $>80\%$,并配套可视化示例,如此语言则会更加精准,从而降低因为语言范围模糊造成错误的风险概率。在传输层,采用语境增强技术,通过数字水印嵌入元数据,在跨语言转换时自动关联文化背景注释,如阿拉伯语中的“盐”在商业谈判场景自动触发“谨慎”提示,防止因此对语言习俗了解不够引发理解错误。在解码层,推行“交互验证”机制,建立双向反馈通道,如医疗处方系统要求患者复述用药说明,通过语音识别比对确认理解一致,确保不会因为理解不够准确而引发错误。

笔者认为,在数字化时代,语言数据已成为重要的战略资源,但生成过程中的安全意识缺失或无意泄露可能造成严重后果,此亦为语言风险之一。如在科研合作与文献发表过程中,核心技术参数的表述若不进行合理设计,则可能被竞争对手逆向推导核心工艺,因此,核心技术有必要进行技术性处理语言表述,既要表达正确的研究设计思路,亦要保护好核心技术工艺;在医疗研发与应用领域,患者病历出现表述疏漏导致信息流出,可能违反隐私法规;在政府文件中,一些敏感数据的表述方式亦可能被数据挖掘工具解析出机密信息分布模式,从而带来未知风险。大数据智能背景下,自然语言生成模型可能通过训练数据残留、对抗样本攻击等渠道泄露原始语料库中的敏感信息。基于上述信息泄露风险,有必要构建全流程数据防护体系。在数据采集阶段,采用差分隐私技术脱敏处理原始语料,通过添加统计噪声模糊个体特征。在模型训练环节,实施联邦学习架构实现数据不动模型动,避免集中式数据存储带来的泄露风险。对于已部署的语言生成系统,需定期进行安全审计,重点检测模型输出中的敏感信息残留,如通过会员推理攻击测试验证模型是否会泄露训练数据中的私人信息。

总之,语言安全是社会文明的防护网,面对信息洪流中的语义迷障与数据暗流,既需以学术智慧廓清理论边界,更要以实践理性构建防护之盾,让语言真正成为沟通的桥梁而非冲突的导火索,护航人类社会的共同未来。

(宗乐英/淄博职业技术大学学前教育学院/讲师)



书名:语言与安全研究(第一辑)

编者:盛静

出版社:上海辞书出版社

ISBN:9787532658510

出版时间:2021年11月

定价:70元