

高校网络空间意识形态安全的智能识别与预警机制研究

魏雨东,王凤兵,简富梁
(电子科技大学成都学院,四川成都 611731)

[摘要]高校网络空间已成为意识形态斗争的重要阵地,生成式人工智能等新技术在赋能内容生产与舆情监测的同时,也加剧了算法偏见和隐性价值渗透风险。针对当前高校在网络意识形态安全治理中存在的技术能力不足、监测预警机制不完善等问题,本文在总体国家安全观指导下,构建高校网络空间意识形态安全智能识别与预警机制框架。通过引入人工智能技术,对校园网络思想动态进行智能识别,建立风险评估指标体系,设置分级预警阈值与响应流程,实现风险的动态监测与前瞻预警。研究从技术支撑、制度完善与协同治理等方面提出优化路径,为提升高校网络意识形态治理能力提供参考。

[关键词]高校;网络意识形态安全;智能识别;预警机制

[中图分类号] G647; G206

[文献标识码] A

[文章编号] 2096-711X(2026)18-0035-03

doi:10.3969/j.issn.2096-711X.2026.18.012

[本刊网址] <http://www.hbxb.net>

引言

当今世界正经历数字文明与智能革命的深度融合,网络空间已成为思想文化交流交锋的重要阵地。高校作为培养青年人才和传播主流意识形态的重要基地,在意识形态工作中具有不可替代的地位。然而,互联网的快速发展使高校意识形态安全面临更加复杂严峻的形势。习近平总书记指出:“互联网是我们面临的最大变量,在互联网这个战场上,我们能否顶得住、打得赢,直接关系国家政治安全。”高校网络空间的开放性和匿名性,使多元思潮和价值观在校园网络中交织碰撞,主流意识形态的网络主导权受到一定冲击。特别是生成式人工智能(AIGC)的兴起,深刻重塑了信息生产与传播范式,其自动化、规模化特征在提升内容生产效率的同时,也使部分信息呈现出“去主观意图”的中立表象,掩盖了算法背后的价值取向,增加了意识形态风险的隐蔽性。因此,新技术既可能成为巩固主流意识形态的重要工具,也可能被不良信息利用,对高校意识形态安全产生负面影响。

在此背景下,高校网络意识形态安全治理的重要性日益凸显。高校肩负着培养社会主义建设者和接班人的使命,必须牢牢掌握意识形态工作领导权,确保高校始终成为坚持党的领导的坚强阵地。然而,现实中部分高校在网络意识形态安全治理方面仍存在薄弱环节,如舆情监测与预警机制不健全、对学生网络行为和思想动态的研判不够精准等,导致在突发网络舆情事件中应对滞后、引导乏力。随着生成式人工智能的快速发展,传统依赖人工经验的治理模式已难以适应信息海量、传播快速化的网络环境,亟须引入智能化手段提升高校网络意识形态安全治理效能。基于此,本文聚焦高校网络空间意识形态安全的智能识别与预警机制,重点探讨如何运用智能技术实现风险的前瞻识别与分级预警,并构建多部门协同的治理机制,以筑牢高校网络意识形态安全防线。

一、理论基础

(一)网络意识形态安全的内涵及其高校价值

网络意识形态是社会意识在网络空间中的映射与呈现,体现了不同社会主体借助网络平台表达和传播价值观念的过程。网络意识形态安全,是指国家主导的意识形态在网络

空间中保持主流地位、不受冲击,并能够有效引领网络舆论和社会思潮发展方向的稳定状态。这一概念强调意识形态安全在网络领域的延伸与深化,其本质仍是维护国家政治安全的重要内容。

对高校而言,网络意识形态安全直接关系到“培养什么人、怎样培养人、为谁培养人”的根本问题。高校网络意识形态安全治理的核心价值,在于落实立德树人根本任务,引导大学生形成正确的思想观念和价值认同,为党和国家培养可靠的青年人才。同时,高校网络意识形态安全治理水平也是高校治理体系和治理能力现代化的重要体现。面对复杂多变的国内外环境,高校有必要将网络意识形态治理纳入整体治理框架,为维护校园稳定和正确办学方向提供制度保障。

(二)“智能识别”与“预警机制”的理论依据

在总体国家安全观视域下,意识形态安全与政治安全紧密相连,需要坚持风险防范关口前移。相关论述强调增强风险感知和研判预警能力,为高校网络意识形态治理提供了重要遵循。随着大数据与人工智能技术的发展,对网络空间实施动态监测、趋势分析与风险评估已具备现实基础。

通过构建科学指标体系,对网络意识形态态势进行分级评估,并设定预警阈值,当指标触及风险边界时及时启动响应程序,有助于将风险化解在萌芽状态。从理论上讲,该机制既契合国家网络安全战略对精准识别与快速处置的要求,也符合风险治理“预防为主”的理念,有助于推动高校治理由被动应对向主动防范转变。

(三)算法治理与生成式人工智能的意识形态影响

在人工智能时代,算法与智能生成内容重塑网络空间的意识形态生态。算法不再是单纯工具,而是承载特定价值取向的技术载体。“算法霸权”通过数据与推荐机制影响认知结构,可能削弱主流意识形态传播效果。生成式人工智能的发展在提供新工具的同时,也带来新的风险。

一方面,生成式人工智能可提升主流意识形态传播效率,如通过精准推送与智能分析增强传播效果;另一方面,其训练数据与模型规则蕴含价值取向,可能放大隐性偏见,影响受众认知,甚至削弱部分群体话语权,对主流意识形态形

收稿日期:2026-5-9

基金项目:本文系教育部高校网络思想政治工作中(四川)资助/立项课题“高校网络空间意识形态安全的智能识别与预警机制研究”(项目编号:CJWSZ25-09)的阶段性成果。

作者简介:魏雨东(1981—),男,电子科技大学成都学院副教授,主要从事数据安全、大数据技术研究。

成冲击。因此,应正视其“双刃剑”效应,在发挥技术赋能作用的同时,加强算法治理与内容规范引导。国家层面已提出以人工智能赋能网络空间治理,为相关机制构建提供了政策依据。

二、问题分析

当前高校网络空间意识形态安全风险呈现多维度、多层次特征,既受到外部环境变化影响,也反映出高校自身治理中的不足。总体来看,主要问题集中在以下方面。

(一)多元思潮冲击下主流意识形态认同弱化

网络空间已成为意识形态博弈的重要场域,多元思潮借助互联网持续影响高校师生认知。大学生思想活跃,但对复杂信息的辨识能力仍有限,海量信息与碎片化传播削弱了主流意识形态的整体叙事优势,一些非主流甚至错误思潮借机渗透,对马克思主义理论和社会主义核心价值观认同产生冲击。尤其是“去意识形态化”等思潮常以“价值中立”“理性讨论”形式出现,具有较强隐蔽性。

同时,网络群体极化现象加剧学生认知分化。在社交媒体环境下,学生易形成相对封闭的交流圈层,强化群体认同并放大情绪化倾向,若缺乏有效引导,可能由网络表达向现实行为转化,带来潜在风险。

(二)算法驱动的信息茧房效应与智能生成内容风险

算法推荐机制重塑了学生的信息获取方式,并在客观上形成“信息茧房”效应,导致学生认知视野收窄和判断偏差。商业算法所隐含的价值取向,可能对学生产生潜移默化影响,而主流意识形态相关内容则因“流量不占优”被边缘化。

从技术层面看,算法的不透明性为意识形态渗透提供了空间。与此同时,生成式人工智能的普及进一步放大风险,深度伪造等技术降低了虚假信息传播门槛,使不良信息更具迷惑性。在识别手段不足的情况下,学生易受误导,主流意识形态公信力面临挑战。

(三)高校网络意识形态安全治理能力有待提升

面对复杂网络环境,高校网络意识形态治理能力仍存在不足。首先,部分高校技术支撑相对薄弱,难以有效掌握舆论主动权;其次,舆情监测与预警机制不完善,对突发舆情反应滞后。

此外,工作队伍专业化水平有待提升,对网络传播规律和舆论演化规律把握不足;制度体系仍不健全,权责划分与协同机制不够明确,学生诉求表达渠道不畅,易形成风险隐患。

总体来看,高校网络意识形态安全风险既源于多元思潮、算法机制与生成式人工智能等外部因素叠加,也与高校自身在技术支撑与治理能力方面的不足密切相关。风险呈现隐蔽化、复杂化特征,传统治理方式难以有效应对,亟须构建智能识别与预警机制,实现风险的前置感知与协同处置。

三、机制构建:高校网络意识形态安全智能识别与预警框架

针对高校网络空间意识形态安全面临的多重风险,有必要构建融合技术手段与制度保障的智能识别与预警机制。该机制以“早发现、早研判、早处置”为基本原则,依托大数据分析和人工智能技术,对校园网络舆情和意识形态动态进行持续监测与辅助研判,并通过制度化流程实现分级预警和协同处置,形成技术支撑与人工决策相结合的闭环治理体系。

(一)多源信息监测与规范化采集

智能识别与预警机制运行的基础在于对高校网络空间信息的系统感知。高校应建立覆盖主要舆论阵地的信息监测体系,对校内官方新媒体、校园论坛、教学互动平台等内部

信息,以及校外公共平台中涉及高校的相关舆情进行持续采集和整合。通过网络爬虫、平台接口等技术手段,对热点议题、敏感信息和异常舆情变化进行动态监测,并构建校园网络舆情数据库,为后续分析研判提供数据支撑。在此过程中,应严格遵循法律法规和校园管理规范,明确数据采集边界,注重保护师生隐私,确保监测行为合法合规。

(二)意识形态内容的智能识别与风险筛查

在数据汇聚基础上,应运用人工智能技术对网络内容进行自动化分析和初步风险识别,以提升风险发现效率并辅助人工研判。可结合自然语言处理、图像识别等技术,对文本、图片和音视频内容进行多模态分析,重点识别涉及政治敏感议题、意识形态偏离和谣言特征的信息。同时,通过情感分析方法监测网络言论的情绪倾向和异常波动,并建立动态更新的特征库机制,不断优化识别规则。通过智能识别与人工复核相结合,实现对校园网络空间风险信息的分级筛查和重点关注。

(三)风险评估与分级预警机制

在完成智能识别后,高校需对潜在意识形态风险进行综合评估,并据此启动分级预警。可从议题敏感程度、传播范围和热度、舆论情绪强度以及对校园秩序和学生思想的影响等方面进行研判,并将风险划分为不同等级,明确相应的预警阈值和响应流程。高校应通过制定网络意识形态安全预警响应预案,规范预警启动条件、报告路径和处置要求,确保预警机制运行有章可循。预警信息发布应坚持及时、客观、适度原则,在争取治理主动权的同时避免不必要的恐慌和误读。

(四)协同处置与反馈改进机制

预警机制的有效性最终取决于处置环节的协同运行。高校应在党委统一领导下,建立多部门联动的处置机制,按照职责分工协同应对不同等级的舆情事件。处置完成后,应对事件进行复盘评估,总结风险成因和机制运行中存在的问题,及时优化识别指标、预警阈值和处置流程,形成“监测—识别—评估—预警—处置—反馈”的循环改进机制,不断提升治理的系统性和前瞻性。

总体来看,该智能识别与预警机制通过技术赋能与制度协同相结合,为高校防范和化解网络意识形态风险提供了可操作的机制框架,也为后续对策建议的提出奠定了基础。

四、对策建议

构建高校网络空间意识形态安全的智能识别与预警机制,需要在技术支撑、制度保障、队伍建设和内容供给等方面协同推进,形成系统完备、运行高效的治理体系。

(一)夯实技术支撑,提升智能化治理能力

高校应加快建设相对自主可控的校园网络舆情监测与分析平台,整合校内外数据资源,提升意识形态风险的辅助研判能力。同时,重视算法治理,对引入校园的商业平台算法进行必要评估和规范,对自主运营平台嵌入价值导向规则,防范技术运行中的价值偏差。持续完善网络安全基础设施建设,为智能识别与预警机制稳定运行提供技术保障。

(二)健全制度机制,强化协同治理与责任落实

在党委统一领导下,高校应压实网络意识形态安全责任,将其纳入领导班子履职考核,明确宣传、网信、学工和院系党组织等部门职责分工。完善舆情预警和应急处置制度,制定风险分级标准和响应预案,并加强校内外协同联动,与相关职能部门保持沟通协作,提升整体防控效能。

(三)加强队伍建设,提升专业化治理能力

高校应配齐建强网络意识形态工作队伍,在宣传和学生

工作等部门设置专门岗位,推动思政课教师和辅导员提升新媒体运用能力。通过专题培训、案例研讨和实战演练,增强队伍对网络舆论态势的分析研判和应急处置能力,并通过激励机制提升队伍参与网络治理的积极性和责任感。

(四) 优化内容供给,营造清朗网络文化生态

在防范风险的同时,应持续增强正面引导。高校应创新主流意识形态内容的网络表达方式,提升传播效果和感染力;坚持以社会主义核心价值观引领校园网络文化建设,对错误思潮和不良言论及时发声、正面引导。同时,畅通网络意见表达和反馈渠道,依法依规回应师生关切,将合理诉求纳入学校治理过程。

五、结论

高校网络空间意识形态安全事关意识形态工作全局,是高校稳定发展和立德树人目标实现的重要保障。面对数字时代信息传播方式深刻变革和意识形态风险形态不断演进的现实挑战,本文以智能识别与预警机制为切入点,探讨了高校网络意识形态安全治理的创新路径。研究认为,通过引入人工智能等技术手段,对网络意识形态风险进行持续监测、辅助识别和分级预警,并配套以制度化流程和协同治理机制,有助于提升高校防范和化解网络意识形态风险的前瞻性和系统性。

从理论层面看,本文丰富了技术赋能意识形态安全治理的研究视角,深化了高校网络意识形态安全治理的学理阐释;从实践层面看,所构建的智能识别与预警机制为高校开展网络意识形态风险防控提供了具有可操作性的框架;从制度层面看,有助于推动高校治理体系和治理能力现代化与国家安全战略的有效衔接。

需要指出的是,智能防控机制的有效运行离不开技术手段与人工判断的有机结合。技术工具虽能够提升风险识别效率,但最终的价值判断和引导处置仍有赖于思想政治工作者的政治敏锐性和人文关怀。展望未来,随着自主人工智能技术不断成熟和相关制度规范逐步完善,高校网络意识形态安全智能防控体系将进一步健全。在这一过程中,高校应坚持守正创新、科技赋能和协同共治,不断提升网络意识形态安全治理水平,为培养担当民族复兴大任的时代新人营造清朗有序的网络思想舆论环境。

参考文献:

- [1] 后文文,王丽霞,吴凯. 高校网络空间意识形态安全治理:价值、风险与路径[J]. 江南社会学院学报, 2025, 27(3): 61-66.
- [2] 修明圆,张新宁. 生成式人工智能“去意识形态化”的表征、实质与风险防范[J]. 河北大学学报(哲学社会科学版), 2026, 51(1): 111-118.
- [3] 刘义江,袁立宁,陈成鑫. 生成式人工智能的意识形态安全风险及其防范策略[J]. 情报杂志, 2025, 41(11): 27-32.
- [4] 梁超锋. 人工智能时代意识形态新形式:算法霸权的出场、表现与治理[J]. 成都理工大学学报(社会科学版), 2026, 34(4): 100-110.
- [5] 龙屏风,肖杰灵. 人工智能生成内容对主流意识形态安全的影响、挑战与应对[J]. 克拉玛依学刊, 2026, 16(4): 85-91.
- [6] 方璐,杨正宇. 高校网络意识形态治理能力提升路径研究[J]. 高校辅导员学刊, 2022, 14(5): 37-42.

Intelligent Identification and Early-warning Mechanisms for Ideological Security in University Cyberspace

WEI Yu-dong, WANG Feng-bing, JIAN Fu-liang

(Chengdu College of University of Electronic Science and Technology of China, Chengdu Sichuan 611731, China)

Abstract: University cyberspace has become a critical arena for ideological contestation. While emerging technologies such as generative artificial intelligence enhance content production and public opinion monitoring, they also intensify risks related to algorithmic bias and covert value infiltration. In response to current challenges in the governance of ideological security in university cyberspace—such as insufficient technical capacity and incomplete monitoring and early-warning mechanisms—this study, guided by the holistic national security outlook, proposes a framework for intelligent identification and early-warning mechanisms. By introducing artificial intelligence technologies, the framework enables intelligent recognition of ideological trends in campus networks, establishes a risk evaluation index system, and defines tiered warning thresholds and response procedures, thereby achieving dynamic monitoring and proactive early warning of potential risks. The study further proposes optimization paths from the perspectives of technological support, institutional improvement, and collaborative governance, providing a reference for enhancing ideological governance capacity in universities.

Key words: university; cyberspace ideological security; intelligent identification; early-warning mechanism

(责任编辑:桂杉杉)