

信息时代高校智能化安全管理策略

——评《高等学校安全教育与管理》

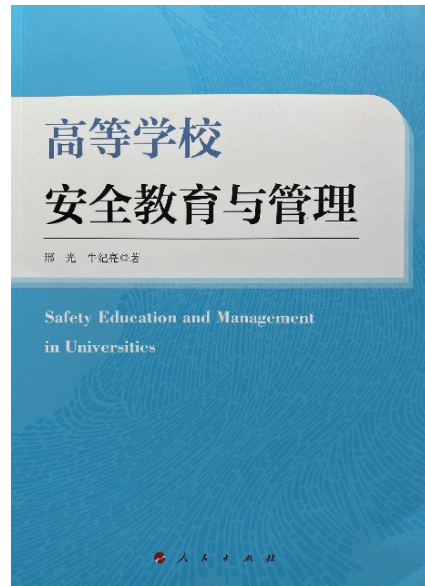
信息技术深度融入高校,物联网、大数据等为安全管理提供了新路径。智能化安全管理通过实时监控、精准预警,能将隐患化解在萌芽状态,既守护师生安全,又为教学科研筑牢稳定屏障,是新时代高校发展的必然选择。

《高等学校安全教育与管理》一书系统构建了高校安全教育与管理的理论框架与实践路径。全书以维护国家安全与高校稳定为核心,分安全教育、安全管理、应急管理3篇15章展开论述。安全教育篇聚焦大学生安全教育的功能定位、特点原则,健全涵盖国家安全与公共安全的内容体系,探索课程建设、新媒体与慕课等实现路径,并提出育人质量提升机制;安全管理篇明确管理总体要求,从政治、消防、交通、网络等多维度解析安全维护内容,强调制度建设、文化培育与技术防范的综合手段;应急管理篇围绕突发事件特点与分类,构建领导体制、预警演练、处置善后的全流程体系,强化思想政治工作与舆论引导的协同作用。

作者指出,数字化转型背景下,高校安全管理需突破传统被动防御模式,转向以数据为核心的精准化治理。数据资产梳理与分类分级是基础环节,需依据《数据安全法》《个人信息保护法》等规范,通过自动化数据发现引擎全面扫描教学、科研、学生管理等系统,识别数据类型、存储位置及权属关系,形成动态更新的数据地图。在此基础上实施三级分类管理:核心数据,如涉密科研成果、国家重点实验室数据,采用物理隔离加多人审批的最高防护;重要数据,如学生隐私信息、财务数据,实施加密存储加权限管控;一般数据,如公开课程大纲、校园通知等,可开放访问但记录操作日志,确保数据底数清晰、责任明确。动态风险评估与监测模型是治理体系的核心支撑,需整合网络流量、用户行为、系统日志、威胁情报等多源数据,应用异常检测、关联分析等机器学习算法,对数据资产、信息系统进行实时风险评分。如针对科研数据存储服务器,若检测到未加密存储或越权访问行为,系统自动触发高风险预警并推送至责任部门。全生命周期安全管控闭环是治理体系的最终保障。采集环节遵循最小化原则,仅收集必要信息,采用匿名化、差分隐私技术保护敏感信息;存储环节实施加密加多副本备份,核心数据用AES-256加密,重要数据在本地、异地、云端各存一份并定期演练恢复;处理环节落实零信任架构与最小权限原则,数据分析师仅能访问必要数据集;共享环节通过应用程序编程接口安全网关验证调用方身份、限制调用频率,嵌入不可见数据水印;销毁环节采用符合标准的工具多次覆盖,记录销毁过程并保留证明。

笔者认为,针对校园安全中人的不安全行为监管难、传统人力巡逻效率低等痛点,需构建技术+管理+协同的智能防控体系。技术层面采用“感知-传输-平台-应用”的分层架构,感知层部署蓝牙信标覆盖宿舍区、教学区等关键区域,智能穿戴设备采集心率、血压等健康数据,智能摄像头支持行为分析,实现位置、运动、体征数据的实时采集;传输层通过蓝牙网关、校园5G网络实现数据无缝分发,确保覆盖校园局部区域与全场景;平台层基于物联网大数据平台,联动位置、体征、行为数据进行24小时监测;应用层提供定位追踪、电子围栏、无感化考勤等功能,替代传统人工登记。场景应用层面聚焦3大核心需求:①异常行为智能监测,通过人工智能视频分析技术,实时识别教学楼栏杆攀爬、楼梯口追逐打闹等场景,结合广播系统自动播放安全提醒,将被动响应转为主动防范;②重点人员轨迹管控,基于电子围栏与位置回溯技术,动态展示特殊群体学生的行动轨迹,一旦进入危险区域立即触发告警;③应急协同响应,构建校警家三位一体信息共享平台,打通校园安全管理平台与公安警务系统,实时同步学生信息、安全警情、治安动态,支持远程预案启动与视频应急指挥,将应急响应时间缩短至分钟级。管理层面建立技术赋能加制度保障的协同机制。制度上明确数据所有者、管理者、使用者职责边界,制定大数据安全协议、人工智能算法伦理审查规范等制度。总之,数字化转型驱动下的高校安全管理,其核心在于治理范式的重构与多维价值的融合,构建一个更具韧性、精准与前瞻性的安全治理体系,为高等教育的现代化发展提供坚实保障。

(田泽森/四川民族学院教育科学学院/讲师)



书名:高等学校安全教育与管理

作者:邢光,牛纪亮

出版社:人民出版社

ISBN:9787010260709

出版时间:2023年12月

定价:145元