数字化时代的法律建设与安全治理

——评《数字化转型时代网络安全环境治理:以上海为例》

数字技术深度重塑社会形态,数据流动突破物理边界,算法决策渗透生活场景,传统法律规制面临“技术黑箱”与“规则真空”的双重挑战。法律建设需从静态规范转向动态适配,既要回应数据主权、算法伦理等新兴议题,又需重构网络空间权利义务体系。安全治理需超越技术防控,构建法律、技术、伦理协同的治理框架,以平衡数字创新活力与社会秩序稳定,为数字文明提供规则根基与安全屏障。

书名:数字化转型时代网络安全环境治理:以上海为例
编者:王寒梅、惠志斌
出版社:学林出版社
ISBN:9787548618607
出版时间:2022年9月
定价:88元

笔者在开展辽宁省教育厅高等学校基本科研项目(LJ112410144027)研究过程中,认真阅读了《数字化转型时代网络安全环境治理:以上海为例》一书,编者立足全球数字化变革背景,以上海市为典型样本,系统探讨城市数字化转型进程中的网络安全治理问题。全书第一章从政策、技术、产业三维度解析上海数字化转型现状与趋势;第二章基于多维监测数据,揭示木马僵尸网络、网页篡改、移动恶意程序等网络安全态势特征;第三章聚焦5G、区块链、人工智能等新技术应用场景及数字政务、智能网联汽车等重点行业的安全威胁,结合数据泄露、高级持续性威胁攻击等典型案例,剖析数字化转型中的风险传导机制;第四章梳理了国内外数据安全治理政策体系与监管模式;第五章通过应用软件违规治理、虚拟货币挖矿整治、黑色产业链打击等实践,总结网络安全事件监测与处置的上海经验;第六章结合重大活动保障案例,提炼网络安全能力建设路径;第七章围绕态势感知系统、互联网协议第六版流量监测等技术领域展开专项研究。第八章提出城市级网络安全环境治理创新模式,并展望战略发展方向。附录收录网络资源数据与行业标准,为理论研究与实践操作提供数据支撑。

编者指出,在数字化浪潮中,法律体系的适应性重构已成为国家治理现代化的核心命题。网络空间的虚拟性、跨域性与技术迭代性对传统法律框架提出结构性挑战,要求立法活动在权利保护与技术发展之间构建动态平衡机制。以数据主权为核心的法律建构正在重塑国际数字秩序,欧盟《通用数据保护条例》与我国《数据安全法》的出台,标志着数据流动规则从“技术中立”转向“主权优先”的范式转型。这种转型不仅涉及个人隐私与商业利益的博弈,更关乎国家数字竞争力的战略布局。法律体系的数字化适配需遵循“技术-法律”协同进化原则。在人工智能治理领域,算法歧视、深度伪造等技术风险要求立法突破“结果导向”的传统模式,建立覆盖算法设计、数据采集、结果应用的全程规制体系。跨境数字治理的法律协调面临双重困境:技术标准差异导致执法协作低效,地缘政治博弈加剧规则碎片化。国际社会在电子证据取证、网络犯罪管辖等领域形成的《布达佩斯公约》等软法机制,虽提供基础框架,但难以适应区块链、量子计算等新技术带来的证据形态变革。未来立法需在坚持国家数据主权的前提下,探索建立多边数字治理联盟,通过技术标准互认与法律规则对接,构建兼具权威性与灵活性的全球数字法治网络。

笔者认为,数字化安全治理已进入“技术-制度-文化”三维共治的新阶段。在技术维度,区块链的不可篡改特性为数据溯源提供可信解决方案,但分布式架构也带来新的攻击面。我国“东数西算”工程中采用的同态加密技术,在保障数据流通安全的同时,有效平衡了隐私保护与价值挖掘的需求。这种技术赋能需与制度创新同步推进,建立涵盖技术标准、认证体系、应急响应的完整治理链条。治理机制的创新体现在“平台-政府-用户”三元共治模式的形成。头部平台企业凭借技术优势成为事实上的“数字守门人”,但其商业利益与公共安全的冲突要求建立问责机制。我国《网络安全法》确立的关键信息基础设施保护制度,通过强制认证与定期演练,将平台安全责任纳入法治轨道。安全治理的韧性构建需突破传统“防御-响应”的线性思维,基于威胁情报共享的动态防御体系,通过人工智能分析实现攻击模式的实时识别,将被动处置转向主动预判。

综上,数字化时代的法律建设与安全治理,需以动态协同思维破解技术迭代与规则滞后的矛盾。通过法律规制的技术适配、治理机制的多元共治及数字素养的全民提升,构建“制度-技术-文化”三位一体的防护体系,为人类社会数字化转型提供可持续的治理方案。

(李至顺/东北大学外国语学院;李函锦/东北大学外国语学院/副教授)