

# 数智化管理中信息安全法治风险评估研究

李盼飞<sup>1</sup> 倪辉<sup>2</sup>

1. 中国船舶集团有限公司第七一三研究所, 中国·河南 郑州 450000

2. 河南省农业农村厅, 中国·河南 郑州 450000

**摘要:** 随着数智化管理在各领域的广泛应用, 信息安全与法治风险问题日益凸显。本文围绕数智化管理环境下的信息安全法治风险进行评估, 通过构建综合评估模型, 识别并量化风险因素, 提出包括法律法规完善、技术保护措施增强、管理体制创新及政府监管强化等对策建议。研究采用多角度分析法, 结合实际案例, 发现隐私泄露、数据滥用及管理不善是主要风险点。本文旨在为政府和企业等社会主体的决策提供理论和实践支持, 推动信息安全法治建设。

**关键词:** 数智化管理; 信息安全; 法治风险评估; 隐私泄露; 风险控制策略

## Research on Risk Assessment of Information Security Rule of Law in Digital Management

Li Panfei<sup>1</sup>, Ni Hui<sup>2</sup>

1. China Shipbuilding Industry Corporation's 713 Research Institute, China Henan Zhengzhou 450000

2. Department of Agriculture and Rural Affairs of Henan Province, China Henan Zhengzhou 450000

**Abstract:** With the widespread application of digital management in various fields, the issues of information security and legal risks are becoming increasingly prominent. This article evaluates the legal risks of information security in the context of digital management. By constructing a comprehensive evaluation model, risk factors are identified and quantified, and countermeasures and suggestions are proposed, including improving laws and regulations, enhancing technical protection measures, innovating management systems, and strengthening government supervision. The study adopts a multi angle analysis method, combined with practical cases, and finds that privacy leakage, data abuse, and poor management are the main risk points. This article aims to provide theoretical and practical support for the decision-making of social entities such as the government and enterprises, and promote the construction of information security rule of law.

**Keywords:** Digital management; Information security; Rule of law risk assessment; Privacy leakage; Risk control strategy

## 0 引言

伴随信息技术的快速进步, 数智化管理已变成提高管理效率与决策精确度的关键手段。它依靠数字技术与智能技术的深入整合, 改造了常规管理模式, 为各行业产生了空前的革新与发展机遇。这一进程同样产生了繁杂的信息安全和法治风险。信息安全不单关乎数据保护, 还牵涉公民权益、企业运行、社会平稳乃至国家安全。如果出现信息安全事件, 例如个人隐私、商业秘密或核心技术泄露等, 会给个人和社会带来重大的损失。在此种情形下, 对数智化管理中的信息安全风险开展彻底评定, 并将风险防控纳入法治化管理体系, 进一步加强政府监管, 似乎格外关键。

## 1 数智化管理概述及信息安全的重要性

### 1.1 数智化管理的定义与应用领域

数智化管理为数字技术与智能技术深入结合的当代管

理模式, 其核心在于运用大数据、人工智能、物联网等技术, 达成对管理对象的彻底察觉、详尽研究和改进管理, 进一步提高各社会主体的管理质量和效率。以某城市为例, 借助建设智慧交通系统, 达成了对交通流量的即时监控和智慧安排, 高效减轻了城市拥堵问题; 智慧医疗系统的使用, 使患者能够通过线上平台预约挂号、查询检查报告, 增强了就医的便利性。以某企业为例, 构建数智化管理与研发平台, 深化数据治理体系建设, 识别和论证产品与人工智能、大数据等技术的融合应用场景, 孵化与推广智能产品原型和解决方案, 通过智能化升级提升产品性能、功能附加值与市场竞争力为业务融合创新提供核心能力支撑。

### 1.2 信息安全的核心要素

信息安全的核心要素包含机密性、完整性和可用性。机密性保障信息只向授权人员公开, 阻止没有授权的接触

和外泄,比如个人的隐私信息等都必须严密的守护。完整性保障信息的精确性和可信性,阻止数据遭篡改和毁坏,比如在金融交易中,数据的完整性极其关键,如果交易数据遭篡改,会引发重大的经济损失。可用性保障信息系统的正规运行,使用户可以在需要时获取信息和服务,比如政府公共服务网站一定要确保系统的可用性,避免干扰公众取得服务。

同时,身份验证和授权的具体方式、数据备份和复原的实际作用、预防不法入侵的监视和防御的具体手段,全都属于信息安全管理的关键部分。身份验证和授权的方式能够保证满足条件的用户才能使用系统资源,挡住外来的危害侵入系统内部。数据备份和复原的作用可以帮助系统发生问题或数据遗失时找回丢失的信息资源。

### 1.3 法治在信息安全管理中的作用

法治对于信息安全管理发挥着关键性的标准和限制作用。政府部门颁布关于信息安全的相关法律条文,清楚地规定了数据处理和隐私保护的具体标准,这样的法律体系为从事信息安全相关工作的各方主体提供了数智化管理行为的明晰指导意见,可有效降低法律纠纷发生的概率。我国颁布了一系列法律条文,对网络运营者和数据处理者的权利义务作出了明确规定,为信息安全领域提供了坚实的法律保护措施。政府部门对信息安全的监管显得十分必要,政府部门可过颁布和实施相关法律条款,仔细监察数智化管理活动的细节,确保各方都能遵循法律要求的内容,保护广大公民的权益以及整个社会的稳定局面。

## 2 数智化管理中存在的法治风险

### 2.1 隐私泄露的风险

隐私泄露是数智化管理中的突出法治风险,信息广泛应用使个人信息被大量采集处理,泄露事件频发。例如数据采集时,部分机构存在过度收集信息、未落实数据分级分类保护、向境外传输未通过安全评估,甚至是未经授权强制采集用户信息的情况,将会导致个人信息被滥用,存在违反《网络安全法》《数据安全法》等法规规定。政府应充分发挥主导作用,制定严格数据采集规范,明确目的、范围与方式,要求数据传输加密并加强监管,规定数据存储机构采取加密存储、访问控制等安全措施。

### 2.2 数据滥用的风险

若干数据滥用针对信息安全法治挑战明显,损害个人隐私、社会秩序和公共利益。一些机构采集到的用户信息如果被不法分子获取,用来违法的营销、准确的诈骗,将

严重干扰社会秩序,近年使用泄露数据发生的电信诈骗案就是典型的案例。政府应制订严厉数据使用规范,禁止未批准数据挖掘和二次利用。强化数据交易监管,促进数据共享合法化,设立共享平台并且严厉审查掌控,创造全社会保护信息安全氛围。

### 2.3 管理不善导致的法律风险

治理不当在数智化管理中经常引发信息安全的法律问题。由于管理流程的不完备、形式化和职责划分不清晰,进而引起法律责任追究无明确依据,导致用户难以维权。某政府部门由于未设立完备的信息安全管理制度,工作人员能够随便查阅和获取敏感数据,造成数据泄露事件出现,该部门因而负责相应的法律责任<sup>[1]</sup>。权利告知的形式化、申诉渠道的单一化、管理方技术方服务方等主体责任边界不清晰,都将会在事件发生后的处置上引发推诿扯皮的风险。政府应发布指导性文件,制定信息安全管理制度基本框架和内容要求,规定数智化管理活动参与者构建完备的信息安全管理制度,清楚各方责任,保障信息安全管理的高效落实。

## 3 风险评估方法和控制策略

### 3.1 风险因素的识别和量化

数字化管理内,信息安全法治风险的识别与度量是风险评定的核心。风险识别可采用多角度剖析法,全面整理数据隐私等隐性问题的法律责任以明确核心风险,例如自技术、管理、法律角度逐一剖析,运用融合的方式度量系统漏洞、人员管理不当、法律法规不健全等各项风险。定性剖析依靠专家访谈、法律文献探究等,评定风险隐性作用与概率,如请信息安全专家评定风险因素。定量评定依靠统计模型,度量风险概率和作用程度,为整体风险给予数据基础,如构建风险评定模型评分确认风险级别。

### 3.2 风险控制的策略建议

以高效处理信息安全法治风险,政府需要自多方面增强监管,改进法律法规,针对数智化管理在持续出现的新型信息安全问题,及早修改改进,保证它有约束力和指导性,例如以新兴技术隐私保护新型问题制订专业条款。设立跨部门监管机制,因为信息安全牵涉多方面的部门,单个监管困难全面涵盖,因此需要设置专业协调机构,协调各部门工作,达成信息共享和协同监管。促进技术创新应用,发布政策支援科研机构与企业进行信息安全技术研发,奖赏普及研发成果,提高信息安全保护水平。增强国际合作,主动加入国际信息安全合作,和国际组织及其他国家

进行交流合作项目,共享经验技术,协同处理跨国挑战,改进全球治理体系<sup>[2]</sup>。

### 3.3 技术与管理措施融合

技术和管理融合对于数智化管理风险控制极度关键。政府应当促进,普及高端技术,借助财政补贴、税收优惠等,激发各方应用数据加密、多因素认证、入侵检测等技术增强数据保护力。设立严谨管理制度,规定数据处理机构设立数据访问控制与定时可靠审计机制,政府制订标准规范,惩戒不遵循机构,前者制约访问权限防止泄漏,后者定时检验评价去除隐患。强化人员培训,安排信息可靠培训活动,给机构供应服务,规定机构定时内在培训,增进员工信息可靠意识与技能,减小人工事件。设立应急响应机制,指引机构改进该机制,包括事件报告、处置、复原计划等,政府评价监察其有效性,减低信息安全事件损失。

## 4 法治构建与信息安全的未来发展

### 4.1 法律法规的完善需求

随着数智化管理的快速发展,现有的信息安全法律法规面临诸多挑战。现有的法律法规可能无法完全适应新技术带来的信息安全问题,例如,人工智能、区块链等新兴技术的应用,给信息安全带来了新的挑战和风险。政府应加快立法进程,完善信息安全法律法规体系,明确各方在数智化管理中的权利和义务,为信息安全提供坚实的法律保障。同时,政府应密切关注技术发展趋势,及时调整和完善法律法规,以适应数智化管理的新要求。例如,针对人工智能技术可能带来的隐私泄露、算法歧视等问题,政府应制定相应的法律法规进行规范。政府还可以建立法律法规的动态调整机制,根据技术发展和实际需求及时修订法律。

### 4.2 技术发展对法治的挑战与机遇

技术不断发展,影响到信息安全领域的法律管理,体现出既有挑战也有机会的双重效果。新兴技术,比如人工智能、大数据、区块链,发展速度非常快,明显增加了信息处理和分析的复杂程度,导致现有法律体系很难完全适应这些多样的技术变化。人工智能算法做决策时,过程往往不够公开透明,很难通过传统的法律规则来有效加以限制。大数据被大量使用后,个人信息的收集和使用变得非常方便,但同时也加大了隐私信息被泄露的可能性。政府部门应该充分利用技术发展带来的各种有利条件,借助先进的科技方法来提升法律体系的建设水平。结合大数据分析和人工智能技术,可以更好地加强法律监督和合规管理

的实际能力,提升信息安全法律保护的精确程度和快速响应的执行效率,确保面对问题时处理更加高效。政府能够运用大数据分析技术对网络上的信息安全事件实施即时监控和分析,迅速察觉和解决违规行为。运用人工智能技术研发智能合规系统,协助数据处理机构自行遵循信息安全法律法规。政府应当强化对新兴技术的研究和评估,拟定相关的法律规范,指导技术良好发展。

### 4.3 系统化风险管理的实践路径

系统化风险管理的实践路径需要从法律法规、技术支持和管理策略三个方面加以整合与实施。政府应发挥主导作用,推动各方共同参与系统化风险管理。具体措施包括:制定政策引导,通过制定相关政策,引导数据处理机构加强信息安全风险管理,推动系统化风险管理的实施。例如,政府可以出台政策,鼓励机构建立信息安全风险管理体系,对建立完善体系的机构给予奖励。提供资金支持,设立专项基金,支持数据处理机构开展信息安全风险管理研究和应用,推动技术创新和管理创新<sup>[3]</sup>。例如,政府可以通过专项基金支持机构开展信息安全技术研发、风险评估工具开发等项目。搭建合作平台,建立政府、数据处理机构和相关组织之间的合作平台,促进信息共享和经验交流,共同应对信息安全法治风险。例如,政府可以组织召开信息安全研讨会、交流会等活动,为各方提供交流合作的平台。

## 5 结语

本文针对数智化管理环境下的信息安全法治风险进行了系统的评估与分析,特别是从政府监管的角度提出了有效的风险控制与管理策略。通过构建一个综合的评估模型并采用多角度分析法,本文成功识别并量化了各种风险因素,尤其是隐私泄露、数据滥用及管理不善这三大主要风险点。这些成果不仅丰富了信息安全风险评估的理论基础,而且为政府决策提供了有力的支撑。未来研究可以进一步探讨政府在不同行业和领域中的特定法治风险及监管策略,推动相关法律法规的完善与实施,促进社会的和谐稳定发展。同时,随着新技术的发展和应用,新的风险因素不断涌现,对风险管理策略的持续更新也是未来研究的重要方向。政府应不断适应数智化管理的发展变化,加强信息安全的法治建设和监管力度,为数智化管理的健康发展保驾护航。

### 参考文献:

- [1] 吴小燕,石德金. 财务数智化背景下“黑字破产”风险管理[J]. 中国农业会计, 2022,(03):71-72.
- [2] 钟毅. 基于风险控制理论的信息安全管理策略思

考——评《信息安全管理与风险评估(第2版)》[J]. 安全与环境学报, 2022,22(03):1693-1694.

[3] 曹秋仙. 数智融合解构隧道安全风险[J]. 科技资讯, 2023,21(13):165-168.

作者简介: 李盼飞(1990.08-), 男, 汉族, 河南汝州, 硕士研究生, 高级经济师, 研究方向: 企业法人治理、法治建设、内控合规、审计、风险管控等方面。