

大数据技术风险与安全管理对策

——评《大数据安全:技术与管理》

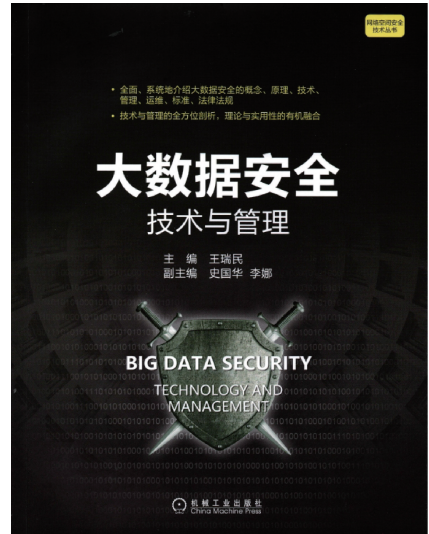
随着信息技术的迅猛发展和互联网的普及,大数据技术已经渗透到人们生活的方方面面,无论是企业运营、城市管理还是个人生活,都离不开大数据的支撑。然而,大数据技术带来的便捷,也伴随着一系列风险和挑战。因此,如何加强大数据技术的安全管理,有效应对潜在风险,值得深入研究和探讨。

我国高度重视数据安全,相继出台了《加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规以及多部涉及数据保护的部门规章,发布了国家和行业的网络个人信息保护相关标准,在国家和行业层面开展了以数据安全为重点的安全防护检查。《大数据安全:技术与管理》一书详述了大数据从创建到传输、存储、处理、交换、恢复,直至数据销毁等各个环节所涉及的安全技术与管理方法,介绍了与大数据有关的网络安全等级保护新标准内容。全书共分为9章。第1章介绍了大数据的基本概念,面临的挑战和大数据安全现状。第2章分享了大数据治理的基本概念,原则和范围,大数据架构和治理实施以及由此带来的个人隐私保护问题。第3章叙述了大数据的安全创建策略。第4章阐述了大数据的安全传输与安全存储策略。第5章介绍了大数据的安全处理措施。第6章关注了大数据的安全交换技术。第7章讲述了大数据的恢复与销毁处理策略。第8章介绍了大数据安全感知技术和安全平台的应用。第9章研究了网络安全等级保护中的大数据安全测评。

编者指出,随着大数据技术的广泛应用,数据安全问题日益凸显,已经成为制约大数据发展的关键因素。加强大数据安全管理和技术防范,对于保障数据安全和促进大数据产业的健康发展具有重要意义。保障大数据安全需要从多个方面入手,包括数据加密、访问控制、安全审计等技术手段,建立完善的数据安全管理体系。利用大数据安全感知技术,可实时监测和分析大数据的安全态势,及时发现并应对潜在的安全威胁。网络安全等级保护是国家对网络安全实施的一项重要制度,可通过测评大数据安全,评估大数据系统的安全性能,发现潜在的安全隐患,并制定相应的安全策略和管理措施。编者强调,建立完善的数据安全管理体系,包括制定数据安全管理制度、明确数据安全责任、加强数据安全培训等,这对大数据安全具有十分关键的作用。

笔者认为,数据是国家信息安全的重要组成部分,保障数据安全不仅与个人权益息息相关,也关系到国家的信息安全。随着大数据技术的迅猛发展,数据的采集、存储、处理和分析变得非常便捷。同时,也带来了多方面的风险。首先是数据安全风险。数据泄露、非法访问和篡改等事件频发,给企业和个人带来重大损失。黑客攻击、内部人员泄密等问题不断考验着数据保护机制的有效性。其次是隐私保护风险。大数据环境下,个人信息可能无意中收集并用于不正当目的,隐私泄露问题日益严重。然后是法律合规风险。随着法律法规的完善,企业在数据处理过程中必须遵守更为严格的规定,否则可能面临法律责任。最后是技术依赖风险。对大数据技术的过度依赖可能导致传统决策能力的退化,一旦技术出现故障,可能引发连锁反应。面对上述风险,笔者建议采取如下安全管理措施,以确保大数据技术的安全运行。第一,加强数据加密技术。通过采用先进的加密算法,确保数据在传输和存储过程中的安全性,防止未经授权访问和数据泄露。第二,建立完善的访问控制机制。实施严格的权限管理,确保只有授权人员才能访问敏感数据,减少内部泄密的可能性。第三,强化隐私保护措施。采用匿名化、脱敏等技术手段,保护个人隐私信息不被滥用。同时,提高公众对个人数据保护的意识,增强自我保护能力。第四,遵守法律法规要求。企业应密切关注相关法律法规的变化,及时调整数据处理流程,确保合法合规运营。第五,建立风险评估与应急响应机制。定期进行风险评估,识别潜在的安全隐患,并制定应急预案,以便在发生安全事件时能够迅速响应。第六,提升技术人员素质。加强对数据安全相关人才的培养和教育,提高他们的安全意识和技术水平,以应对日益复杂的安全挑战。

总之,在数字化时代,大数据技术的发展为社会带来了深远影响,也带来了诸多风险。必须始终保持警惕,不断完善安全防护措施,建立一个安全、可靠、高效的大数据环境。



书名:大数据安全:技术与管理

编者:王瑞民,史国华,李娜

出版社:机械工业出版社

ISBN:9787111688099

出版时间:2021年8月

定价:79元

(郑梦莉/淄博职业学院/讲师)