DOI 编码：10.13646/j.cnki.42-1395/u.2022.02.017

基于数据分类分级的港口企业数据安全管理研究

钟璐潞，卢栋

（中国交通运输部水运科学研究所，北京 100088）

摘　要：数据作为新的生产要素，已成为国家基础性资源和战略性资源。港口是水陆交通的集结点和枢纽，在新一轮的科技革命和产业革命背景下，也迫切需要由传统要素驱动向更加注重创新驱动的方向转变。通过我国现有的数据安全法律法规、规范性文件的研究，采用科学分类分级方法，提出港口企业航运数据资产安全管理的实施路径，保证港口企业数据资产安全的同时，让数据资源流向社会、产业，实现利用数据资源赋能港口生产作业与运营管理，促进港口新业态的发展。

关键词：数据资产；数据分类分级；数据安全；安全政策

中图分类号：U691　　**文献标识码：**A　　**文章编号：**1006—7973（2022）02-0057-03

当前，我国乃至世界迎来了百年未有之大变局，新一轮科技革命和产业革命大规模快速发展，尤其在全球疫情的影响下，港口航运经济发展面临着机遇和挑战，迫切需要推动高质量发展，由传统要素驱动向更加注重创新驱动的方向转变。

2020 年 3 月，我国明确了数据是新的生产要素，是国家基础性资源和战略性资源，其安全问题影响着国家发展、安全和公众利益。同年 4 月，《关于构建更加完善的要素市场化配置体制机制的意见》明确提出的“加快培育数据要素市场”，要进一步激活数据要素潜力。而港口作为水陆交通的集结点和枢纽，积攒了大量的航运数据资产。这些数据资产，作为新型生产要素，不同于其他传统生产要素，其安全问题与国家安全以及社会经济发展密切相关。因此如何在保证港口企业数据资产安全管理的同时，扩大航运数据的流通和利用，实现数据赋能，促进港口新业态发展是亟待解决的问题。科学开展港口企业的数据分类分级管理，则是港口企业对数据进行安全管控的基础，是数据精细化管理的重要环节。

1 我国数据安全管理法规政策研究及启示

目前，我国的数据安全管理立法体系是由法律、法规、规章以及各类规范性文件共同组成的信息保护法律体系。针对我国数据安全管理现状，港口企业的数据资产安全管理应从国家和行业两个层面对现有的数据分类分级法律、行政法规、规范性文件进行梳理研究，为企业数据资产的安全管理范围、数据分类分级的步骤、方法明确法律法规依据。对数据的安全管控和资源整合、共享是大势所趋，近几年我国出台了多个相关的法规政策，以不断规范数据安全的管理和应用。相关法规制度如图 1 所示：

图 1　我国数据安全管理法规政策

具体而言，2017 年的《网络安全法》和《关键信息基础设施安全保护条例》明确了什么是重要数据以及关键信息基础设施范围，并在此基础上发布的《信息安全技术 关键信息基础设施安全检查评估指南》明确了关键信息基础设施检查评估工作的方法、流程、安全保障指标体系框架等内容；2018 年的《科学数据管理办法》，是确立大数据国家战略以来，首个国家层面出台发布的类目数据的管理办法；2019 年，在《中华人民共和国网络安全法》的基础上制定《数据安全管理办法》，进一步明确了确立数据分级分类管理以及风险评估，监测预警和应急处置等数据安全管理各项基本制度；2020 年颁布的《关于构建更加完善的要素市场化配置体制机制的意见》中指出，要“提升社会数据资源价值、加强数据资源整合和安全保护”，因此针对港口企业的数据安全管理开展的数据分类分级管理工作十分必要；2021 年，我国通过《中华人民共和国数据安全法》，确立了数据分级分类管理以及风险评估、监测预警和应急处置

等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；并建立保障政务数据安全和推动政务数据开放的制度措施。

2 港口企业数据分类分级安全管理研究

通过以上法规政策梳理，港口企业数据分类分级管理工作应按照各数据安全管理政策、指南的要求为依据，开展相应的数据分类分级安全管理工作。

2.1 数据分类分级目标

数据安全分类分级的目标是识别港口企业数据资产中的个人隐私、商业机密、关键信息基础设施信息等敏感信息及文件，并对敏感信息实施保护与控制，以符合法律法规要求，并在保证数据安全的基础上促进数据开放共享。其中，数据分类是依据自身业务特点，按照统一的数据分类方法对产生、采集、加工、使用或管理的数据进行类别划分。数据分级是以数据分类为基础，采用规范、明确的方法区分数据的重要性和敏感度差异，并确定数据防护等级。

2.2 港口企业数据资产安全管理范围

港口企业的数据资产是指港口拥有或者控制的，能够为企业带来未来经济利益的，以物理或电子的方式记录的数据资源。港口企业的数据资产管理，则是以资产管理的方法结合企业数据的特征，对数据从产生与流转，存储与整合，分析与价值发现，直至归档与消亡的全生命周期的每个环节的安全进行管理。根据我国的数据安全法律法规，对法律中提及的个人信息安全以及关键信息基础设施信息应根据《中华人民共和国电子商务法》要求的“个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。”以及《关键信息基础设施安全保护条例（（征求意见稿））》的“关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。”进行安全管理。港口企业应识别拥有的数据资产是否存在个人信息、关键信息基础设施信息以及商业机密，并从高定级、检测、评估，对数据进行分类、备份、加密认证、境内存储。其他企业数据资产信息则应在不违反我国相关法律法规的前提下，依据数据分级方法，通过统一描述影响对象、影响程度及数据级别之间的关系，对影响对象的不同程度影响进行分析，从而确定数据安全等级。

2.3 数据分类分级原则

根据《信息安全技术大数据安全管理指南》要求，港口企业数据分类分级工作应按照“职责明确、安全合规、质量保障、数据最小化、责任不随数据转移、最小授权、确保安全、可审计”8 大分类分级原则开展，并且确保数据的保密性、完整性、可用性。

2.4 港口企业数据分类分级流程及方法

根据《信息安全技术大数据安全管理指南》，港口企业开展数据安全管理的内容及流程为：明确数据安全需求、数据分类分级、明确大数据活动安全要求、评估大数据安全风险。数据分类分级则应对数据先分类，后分级，最后实施分级保护。

数据分类：港口企业的数据资产分类，可采用《GB7020–2002 信息分类和编码的基本原则与方法》中提到的线分类法、面分类法以及混合分类法三类分类方法，结合自身的数据资产特点以及安全防护需求，选择适合的分类方法进行数据分类，并形成相应的数据分类类目表，为数据分级工作提供数据资源基础。根据港口企业的业务特点，采用混合分类的方法，根据港口运营管理以及内部管理的业务大类，并结合数据性质、重要程度、管理需要、使用需要等要素，将港口企业的数据划分为运营管理相关的港口生产数据、港口服务数据、港口物流数据、航运业务数据、港口工程数据、贸易数据以及内部管理相关的人事管理数据、财务管理数据、资产管理数据、法务管理数据、安全管理数据、货运质量数据、公文管理数据、审计管理数据、综合规划数据、信息技术数据等数据一级类别，并根据需要进行进一步细分。根据数据分类层级过少不利于定级，过多不利于管理的原则，港口企业的数据类别一般可细分至三级。

数据分级：根据《数据安全法》第二十一条，在港口企业数据分类的基础上，可针对国家、公共利益、组织、个人四个维度的影响对象，结合数据安全性的三个影响要素（保密性、完整性、可用性），根据三个级别的影响程度（严重损害、一般损害、轻微损害），通过《关键信息基础设施安全保护条例》以及《数据安全法》中提到的相关定级要求（对于关键信息基础设施涉及数据，至少按三级管理；关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，

实行更加严格的管理制度。）制定定级算法，从而对影响对象的不同影响程度进行分析，按照非敏感、内部敏感、普通商密、核心商密、核心机密五个级别，将分类好的港口数据映射到各级别，从而得到港口企业数据级别定级目录，为港口企业数据定级提供科学依据。

2.5 数据开放共享机制

随着全球经济一体化，各国港口之间的合作越来越密切，港口企业所掌握的航运数据开放共享的需求也在不断增大。港口企业在数据分类分级结果的基础上，建立符合港口企业自身的数据共享机制，明确数据管理的职责分工、数据开放共享流程以及监管制度，在合法合规的条件下，让企业的数据资产发挥最大效能。

港口企业依据数据的安全等级，制定相关数据开放共享标准，一般依据机密、核心商密不共享、普通商密以及内部敏感数据有条件贡献给、非敏感级数据无条件共享的原则，按照数据申请、企业审核、数据共享实施的流程开展数据共享业务。在审核环节，针对无条件的共享数据，数据在备案后可直接共享使用；有条件共享数据，数据需通过企业相关部门审批后方可开放使用；针对不予共享的数据，原则上不允许共享，或在遵守我国数据安全管理相关法律、行政法规的前提下，采取“一事一议”原则进行商议，决议结果报送企业相关部门审核后再共享使用。

涉及到关键信息基础设施重要数据跨境共享的申请，应依据《网络安全法》第三十七条，采用重要数据境内留存制度，使用主权国家境内的服务器进行数据本地化存储，并按照《数据安全管理办法》中的规定，对申请共享的数据进行进一步的安全风险评估，并报行业主管监管部门同意或省级网信部门批准，再开展数据共享相关工作。此外，在数据安全检查和审计环节，港口企业应周期性地开展数据安全使用和管理情况检查，更新过期的数据使用信息以及相关人员的安全自查工作，确保港口企业数据资产的安全和合规应用。

3 结语

港口企业的数据分类分级管理工作是一个不断完善、优化的过程，因此港口企业需要建立相应的数据分类分级组织保障和数据分类分级管理制度，辅助数据分类分级工作的顺利开展，从而进一步提升港口企业的数据管理能力以及数据资源的深度应用能力，实现数据资源赋能港口生产作业与运营管理。

在组织保障工作方面，根据《数据安全法》中明确规定，企业应设立相关的数据安全负责机构和负责人，对重要数据安全保护责任，采取必要的安全措施，并承担相应的法律责任。因此，港口企业可成立专门的企业信息安全管理小组，明确数据安全保护的组织架构、管理职责、人员配备、数据安全的责任内容以及相关的管理角色和授权机制。安全管理小组对企业的数据分类分级工作以及数据开放共享使用情况进行监督管理，一旦发现信息泄露等问题可及时进行反馈和处理。

在制度保障方面，港口企业可依据 ISO27001 信息安全认证体系，将数据安全领域的制度文件进行级别划分，参照各级监管标准的发文要求，制定相关管理制度，明确企业数据分类分级工作的流程、管理机构、岗位职责、数据使用、维护管理办法等内容，从制度方面保障港口企业数据分类分级以及数据安全管理工作的规范开展。

参考文献：

[1] 张芬 . 大数据时代数据的分类分级管理及安全防护 [J]. 计算机产品与流通 , 2019-01.

[2] 李松涛 , 谢宗晓 . 数据分类 / 分级及其相关标准解析 [J]. 中国质量与标准导报 .2019-04.

[3] 彭诚信 . 数据安全与利用双翼驱动 [J]. 检察风云 .2020-19.

[4] 苗运卫 , 宏伟 . 三重维度解读《数据安全法（草案）》保障数据安全 [J]. 中国电信业 .2020-08.

[5] 郑鉉 , 汪灏 .《数据安全法》的体系坐标与精细表达 [J]. 西华大学学报 (哲学社会科学版);2020-05.