

国标《数据安全技术 数据分类分级规则》分析与解读*

单博深, 左晓栋

(中国科学技术大学 网络空间安全学院, 安徽 合肥 230026)

摘要: 2024年3月14日, 国家标准化管理委员会正式发布了国标 GB/T 43697—2024《数据安全技术 数据分类分级规则》。该标准是我国在数据治理方面的最新研究成果, 也是我国首次采用“数据安全技术”作为前缀的国标文件。该文件的发布将在国家安全、社会秩序、经济运行等多个方面产生重大影响。从国内外数据分类分级治理的相关研究背景出发, 介绍了新国标的文本内容, 对比了中美两国对数据的规制方案。本文认为, 新国标的发布, 将在提升国家数据治理水平、补齐国家安全短板、应对国际数据规则制定压力和提升我国国际形象等方面产生积极影响。最后, 对我国未来数据安全工作给出了建议与展望。

关键词: 数据分类分级; 国家标准解读; 数据治理

中图分类号: TP309.2

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2024.11.004

引用格式: 单博深, 左晓栋. 国标《数据安全技术 数据分类分级规则》分析与解读 [J]. 网络安全与数据治理, 2024, 43(11): 19-22.

Analysis and interpretation of the national standard for Data Security Technology Data Classification and Grading Rules

Shan Boshen, Zuo Xiaodong

(School of Cyberspace Security, University of Science and Technology of China, Hefei 230026, China)

Abstract: On March 14, 2024, the National Standardization Administration officially released the national standard GB/T 43697—2024 "Classification and Grading Rules for Data Security Technology Data". This standard is the latest research achievement in data governance in China, and it is also the first national standard document in China to use "data security technology" as a prefix. The release of this document will have a huge impact on multiple aspects such as national security, social order, and economic operation. Starting from the relevant research background of data classification and hierarchical governance at home and abroad, this article introduces the text content of the new national standard and compares the regulatory schemes for data between China and the United States. This article believes that the release of the new national standard will have a positive impact on improving the level of national data governance, filling the gaps in national security, responding to the pressure of international data rule, and enhancing China's international image. Finally, this article provides suggestions and prospects for future data security work in China.

Key words: data classification and grading; interpretation of national standards; data governance

0 引言

2024年3月15日, 国家标准化管理委员会正式发布了由中国电子技术标准化研究院牵头, 中国科学技术大学、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心等三十余家单位参与的国标 GB/T 43697—2024《数据安全技术 数据分类分级规则》(以下

简称“《规则》”)。《规则》是我国首次采用“数据安全技术”作为前缀的国标文件^[1], 这体现了我国对数据安全保护工作的高度重视。作为我国数据出境安全管理、数据安全审查、数据交易管理等一系列重大数据制度落地的基础, 该标准的发布将在国家安全、经济运行、社会秩序等多个领域产生重大影响。

1 相关研究

随着全球信息化的演进, 世界各国意识到许多原本不属于国家秘密的数据, 在新兴技术的加持下能够对国

*基金项目: “十四五网络空间治理”国家重点研发项目 (2022YFB3103200)

家安全、经济运行、社会秩序及组织、个人利益产生巨大影响。但世界各国对这类数据认识模糊，更未形成科学的应对体系，难以应对其带来的安全挑战。目前，中美两国在相关领域的探索研究走在世界前列。

1.1 美国相关研究

2008年，美国国家标准技术研究院（NIST）根据《联邦信息安全管理法案》的要求制定了SP 800-60《将各类信息与信息系统映射到安全类的指南》。该指南不仅对信息进行分类，还从信息机密性、完整性、可用性等角度为信息标注影响级。2010年，时任美国总统奥巴马签署了第13556号总统行政令《非密受控信息》，该行政令旨在加强对非密受控数据（CUI）的保护。此后数十年间，美国联邦政府多次在国家安全战略文件中强调CUI安全保障问题。在政府部门层面，美国国防部发布了《国防部联邦采购条例》，该条例定义了隐藏国防信息（CDI）与受控技术信息（CTI），以加强国防部内部数据的安全防护。

除了提高自身数据安全防护水平，美国对外数据政策逐年趋紧。近年来，美国以“数据安全”为由对TikTok展开审查，要求美国外国投资委员会（CFIUS）与TikTok讨论确定的“受保护信息”必须存储于甲骨文公司位于德克萨斯州的云服务器，且中国员工不得接触该数据。2024年2月29日美国总统拜登签署了第14117号总统行政令《防止受关注国家获取美国大量个人敏感数据与政府数据》。该行政令要求多个部门协力合作阻止敏感个人数据被大规模转移至受关注国家，并通过授权司法部门制定规则或条例，保护美国敏感个人数据不被受关注国家利用。

1.2 我国相关研究

2016年《网络安全法》第二十一条首次提出了“重要数据”与“数据分类”的概念，要求“采取数据分类、重要数据备份加密等措施，防止网络数据泄露或篡改”^[2]。2021年《数据安全法》第二十一条明确提出“国家建立数据分类分级保护制度，对数据实行分类分级保护”^[3]。同年，《关键信息基础设施安全保护条例》要求关键信息基础设施运营者在发生重大数据泄露等重大网络安全事件时，应及时向国家网信部门、国务院公安部门报告^[4]。

除国家法律政策外，2017年《信息安全技术 数据出境安全评估指南》向社会公开征求意见，该文件首次对重要数据的界定做出探索。2019年，全国信息安全标准化委员会设立《重要数据识别指南》国家标准研究项目。2020年《信息安全技术 重要数据识别指南》在前述项目研究成果的基础上正式立项，后经全国信安标委协调于

2023年与另一标准制定项目合并，最终作为《规定》正式发布。2022年，“十四五”国家重点研发计划“重要数据分类、识别与安全评估技术”项目正式立项，该项目旨在改变重要数据长期失于保护的局，补齐国家安全短板，筑牢我国数据安全防线。

2 国标内容分析

《规则》共包含正文七章、附录十件，要求按照科学使用、边界清晰、就高从严、点面结合、动态更新的原则实现数据分类分级，并给出了数据分类规则、数据分级规则以及数据分类分级实施的参考流程。

2.1 数据分类

数据分类的目的是便于数据监督与管理。由于数据来源不同且应用环境时常变化，难以为数据划分静态类别，《规则》仅给出了数据分类的通用框架，拟采用动态的分类方式加强对数据的管理。在归纳了数据的主要行业领域与数据业务属性的基础上，《规则》提出采用“明确范围—业务分类—属性分类—确定数据分类”层层递进的理念，针对特定场景帮助数据处理者构建灵活的数据分类方案。

2.2 数据分级

数据分级的目的是满足数据保护的需要。数据分级有利于对具有价值的对象实施与其价值相匹配的安全保护措施。《规则》按照“数据在经济社会发展中的重要程度”与“数据一旦遭到泄露、篡改、损毁或非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度”两个维度，将数据划分为核心数据、重要数据、一般数据三个级别，并提出“确定分级对象—分级要素识别—数据影响分析—综合确定等级”的分级步骤与数据等级的判定标准。

在分级要素识别方面，《规则》确定了三类共计八项影响数据等级判定的要素，即：定性分级要素（包含领域、群体、区域与重要性）、定量分级要素（包含精度、规模、覆盖度）与衍生数据分级要素（包含深度）。

在数据影响分析方面，《规则》从“数据影响对象”与“数据影响程度”两个维度判断数据可能造成危害与影响。影响对象包括国家安全、经济运行、社会秩序、公共利益、组织权益与个人权益六类，影响程度包括特别严重危害、严重危害、一般危害三类。

《规则》将对国家安全造成特别严重危害或严重危害，对经济运行、社会秩序或公共利益造成特别严重危害的数据识别为核心数据；将对国家安全造成一般危害，对经济运行、社会秩序或公共利益造成严重危害的数据

识别为重要数据；将其他数据识别为一般数据。

当分级对象为数据集时，应首先确定数据集各数据项的数据级别，按照就高从严的原则将所有数据项中最高数据级别作为数据集的整体级别。衍生数据与跨行业领域数据的数据级别可以在判定原始数据级别的基础上，考虑融合加工对数据分级要素的影响，按照就高从严的原则确定。

2.3 分类分级流程

《规则》适用对象包括行业、领域主管（监管）部门与数据处理者。行业、领域主管（监管）部门应参照《规则》制定行业标准规范，指导数据处理者准确识别数据等级，编制报送重要数据和核心数据目录。数据处理者应按照国家、行业领域数据分类分级要求，承担数据分类分级责任，进行数据资产梳理、内部数据规则制定、完成重要数据与核心数据目录编制，并及时动态更新本单位重要数据与核心数据目录。

3 影响分析

数据是国家安全体系的重要组成部分。在人工智能、大数据、云计算等新兴技术的加持下，数据对国家安全衍生出前所未有的潜在影响。一方面，《规则》发布能够协助企业、单位设计相适宜的保护策略，提高企业自身数据保护水平；另一方面，《规则》发布能够提高主管部门的监管能力，防止重要数据、核心数据的泄露与跨境传输，补齐长期以来存在的治理短板，进一步筑牢国家安全防线。

3.1 《规则》发布是我国数据治理领域的重大突破

重要数据是我国在世界范围内首次提出的全新概念，开创了我国数据治理学术研究的新方向和新方案。《规则》不仅明确给出了重要数据、核心数据的定义与判定标准，提出了数据分类分级的参考步骤，还给出了针对结构更复杂数据集的分类定级方法，附录更是对数据分类分级过程中可能出现的特殊情况作出详细说明，体现了我国对重要数据、核心数据基本属性与治理客观规律的认识深刻，是我国数据安全治理工作的巨大突破^[5]。

3.2 《规则》发布为我国数据安全制度具体落实奠定基础

数据等级的精准识别是我国数据安全制度落地实施的基础^[6]。除数据分类分级制度以外，我国还建立了数据出境管理、数据安全审查、数据交易管理等六项数据安全制度，共同构成我国数据治理的基本框架。其中，重要数据与核心数据是重点，《规则》的正式发布明确了重要数据、核心数据的定义与判定准则，为落实《网络安全审查办法》《促进和规范数据跨境流动规定》等政策文件监管要求的落地实施提供了抓手。

3.3 《规则》发布将进一步巩固国家安全防线

数据已经成为国际竞争的前沿阵地。一方面，西方发达国家依靠科技优势推动建立符合自身利益的国际规则；另一方面，欧美等国常常以“去风险”“安全考虑”等为由，排斥、打压中国网络数据产品，不遗余力地造谣、抹黑中国的国际形象。《规则》发布不仅旗帜鲜明地表达了我国进行数据治理与保护数据安全的决心，同时表明我国数据保护只针对可能影响国家安全、社会秩序、经济运行的重要数据与核心数据，并不包括国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等正常活动中的数据。

近年来，欧美等国家凭借自身在数字经济技术上的优势，极力鼓吹全球数据跨境自由流动，通过制定规则、谈判合作形成“数字同盟圈”，并试图引领、主导甚至重塑世界数字经济格局走向，对其他国家的数字主权产生威胁。《规则》的发布，有利于我国政府部门、企事业单位、科研院所进行准确的数据分类分级，确保数据安全合规流通。同时，《规则》发布为世界数据治理提出了新的思路和治理手段。

4 未来建议

一是在《规则》的基础上，各地区、各部门应加快开展本部门、本地区的数据分类分级保护工作。《数据安全法》第二十一条对重要数据保护工作提出要求，即“各地区、部门以确定本地区、本部门及相关领域的重要数据具体目录，对列入目录的数据进行重点保护”。目前国家并没有对地区、部门的数据分类分级方案做额外限制，但地区、部门数据分类分级方案的制定应当以边界清晰、综合考虑绩效费效为基本原则，科学合理地编制重要数据目录。同时应当紧随外界环境变化，及时更新重要数据目录，避免出现数据保护措施滞后于数据等级变化的不利情况。

二是加强政府与企业之间在重要数据、核心数据保护方面的合作。数据安全保护不仅仅是政府的责任，同样是广大企业维护国家安全的义务。当前，政府与企业都面临着数据保护的巨大挑战，又在数据保护方面各自具有不同的优势。其中，政府掌握了大量的政务数据，能够在各级政府间快速共享安全风险信息，统筹协调各类资源，提供应急响应能力；企业则掌握了海量的用户数据、业务数据、经营管理数据与系统运维数据，并在数据安全技术、大规模数据管理等方面具有丰富的经验储备。应促进政府企业优势互补，加快健全政府与企业间安全事件信息共享的工作机制，建立科学合理的安全检测技术，制定足备合理的应急响应预案，同时以技术

委员会的形式邀请企业专家参与数据安全保障工作顶层制度的设计,优势互补,以提升我国数据安全保障水平。

三是在数据类别、等级识别的基础上,加快数据安全保护行动指南等文件的出台。尽管《规则》的出台解决了数据类别划分、等级识别等基础问题,但不同等级数据安全保护的具体措施尚缺乏统一标准。当前,国内市场上不同厂家安全产品保护能力相互重叠,降低了产品采购方预算投入的收益,造成了社会财富的浪费。美国 NIST 在 2022 年 10 月和 2024 年 3 月分别发布了《网络安全绩效目标》与《网络安全框架》2.0^[7-8],为美国网络安全保护提供了统一的参考框架,并将网络安全产品的绩效费效比作为考虑重点,该方法降低了网络安全保护的成本,值得我国学习借鉴。因此,应综合研究数据安全保护产品的实践案例,明确不同产品安全功能与应用场景,在数据等级识别的基础上,加快制定数据处理安全要求与数据安全保护指南等文件,在规范数据处理者数据处理行为的同时,为企业数据安全保护工作提供指导。

四是积极开展国际合作,扩大我国在世界数据治理领域及国际规则制定领域的话语权。面对网络空间发展不平衡、规则不健全、秩序不合理的现状,习近平总书记于 2020 年杭州 G20 领导人第十五次峰会提出了《全球互联网倡议》,希望“共同构建和平、安全、开放、合作、有序的网络空间”。我国应当与各国加强合作,依托我国数据治理理论与先进成果,扩大我国在世界数据治理领域乃至国际规则制定领域的话语权,为建立安全、公正、平等、合理的网络空间秩序作出新贡献。

参考文献

- [1] 陈磊,彭理云,单博深,等.重要数据安全国家标准的设计思路[J].网络安全与数据治理,2023,42(11):53-57.
- [2] 徐玉梅,王欣宇.我国重要数据安全法律规制的现实路径——基于国家安全视角[J].学术交流,2022(5):37-48,191.
- [3] 陈兵,郭光坤.数据分类分级制度的定位与定则——以《数据安全法》为中心的展开[J].中国特色社会主义研究,2022(3):50-60.
- [4] 张勇.数据安全分类分级的刑法保护[J].法治研究,2021(3):17-27.
- [5] 商希雪,韩海庭.数据分类分级治理规范的体系化建构[J].电子政务,2022(10):75-87.
- [6] 袁康,鄢浩宇.数据分类分级保护的逻辑厘定与制度构建——以重要数据识别和管控为中心[J].中国科技论坛,2022(7):167-177.
- [7] 单博深,左晓栋.美国《跨部门安全绩效目标》新政策解读[J].工业信息安全,2022(10):13-18.
- [8] 陈磊,单博深,左晓栋.美国《网络安全框架》2.0概念文件研究[J].中国信息安全,2023(8):88-92.

(收稿日期:2024-04-24)

作者简介:

单博深(2000-),男,博士研究生,主要研究方向:数据安全治理、网络空间安全。

左晓栋(1975-),男,博士,教授,主要研究方向:数据安全治理、网络空间安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com