

检验检测机构认可业务数据分类分级研究^{*}

金 达¹, 霍珊珊¹, 张 冰², 李彦军², 刘 健¹, 郝 奇²

(1. 中国电子科技集团公司第十五研究所 信息产业信息安全测评中心, 北京 100083;

2. 中国合格评定国家认可中心, 北京 100062)

摘 要: 随着认可业务数字化、智能化进程不断推进, 认可业务数据的重要性不断增强, 数据分类分级安全保护需求日益紧迫。首先研究国外数据分类分级现状和分析我国数据分类分级战略规划, 接着分析数据分类分级方法, 然后在分析检验检测机构认可业务数据特点基础上, 提出检验检测机构认可业务数据分类分级流程和规则, 以及数据分级安全保护措施, 为实现认可业务数据分类分级安全保护提供支撑。

关键词: 认可业务数据; 数据分类分级; 数据安全; 数据保护

中图分类号: TP274

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2025.11.010

引用格式: 金达, 霍珊珊, 张冰, 等. 检验检测机构认可业务数据分类分级研究[J]. 网络安全与数据治理, 2025, 44(11): 60-64, 78.

Study on the classification and grading of accreditation service data in inspection and testing body

Jin Da¹, Huo Shanshan¹, Zhang Bing², Li Yanjun², Liu Jian¹, Hao Qi²

(1. Information Technology & Security Test and Evaluation Center, The Fifteenth Research Institute of China Electronics Technology Group Corporation, Beijing 100083, China; 2. China National Accreditation Institute of Conformity Assessment, Beijing 100062, China)

Abstract: With the continuous advancement of digitalisation and intelligence of accreditation service, the importance of accreditation service data is increasing, and the demand for data classification and grading security protection is becoming more and more urgent. Firstly, the paper studies the current status of data classification and grading in foreign countries, and analyses the strategic planning of data classification and grading in China. Next the paper analyses the data classification and grading methods. Then on the basis of analysing the characteristics of accreditation service data in inspection and testing body, the paper puts forward data classification and grading process, rules and data grading security protection measures for such body. The proposed scheme and measures are to enable the implementation of accreditation service data classification and grading security protection.

Key words: accreditation service data; data classification and grading; data security; data protection

0 引言

我国非常重视数据安全, 陆续颁布《中华人民共和国数据安全法》(以下简称《数据安全法》)、《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)等法律法规, 明确提出数据分类分级和个人信息分类管理的要求。当前国家、地方和行业发布了多个数据分类分级的标准和规范, 在宏观上对数据分类分级给出了方法指引, 具有一定的借鉴作用。但是这些标准在实践细则上还不是很完善, 缺乏类似网络安全等级保护标

准那样较为明确和可操作性的技术规范^[1], 因此在特定细分领域的的数据分类分级实践中还是存在困难, 不利于数据分类分级工作的快速推进。

中国合格评定国家认可中心负责运营的中国合格评定国家认可委员会 (China National Accreditation Service for Conformity Assessment, CNAS) 实验室/检验机构认可业务管理系统支撑全国上万家实验室、检验机构等检验检测机构认可活动, 自 2015 年 9 月上线运行以来, 截至 2020 年已积累超过 5T 的数据^[2]。随着近几年 CNAS 数字化、智能化进程加快, 检验检测机构认可业务数据 (下称检验检测认可数据) 增长明显提速, 重要程度不断提

^{*} 基金项目: 国家市场监督管理总局科技计划 (2023MK213)

升，迫切需要完成数据分类分级和安全保护。如何实现检验检测认可数据分类分级安全保护具有重要意义。本文将在研究国内外数据分类分级制度的基础上，依据CNAS检验检测认可数据特点探讨该领域数据分类分级方案，并提出相应的数据安全保护措施思路。

1 国内外数据分类分级现状

美国在数据分类分级管理方面起步很早，从2009年开始先后颁布了多个行政命令和政策文件，将数据分为国家秘密、受控非密数据^[3-4]，进行分类管理。此外，美国没有一般数据类别，在实践中以敏感数据、开放数据表述^[5]，如表1所示。对于个人数据，欧盟《通用数据保护条例》（General Data Protection Regulation, GDPR）是当前个人数据保护最具代表性的立法成果之一^[6]。GDPR提出个人数据、儿童个人数据、敏感个人数据三类数据。美国未有联邦层面的个人信息保护的整体性法律，而是各州单独立法，其中以谷歌、苹果、亚马逊等互联网企业总部所在地加州最为突出。2018年和2020年加州分别发布《加州消费者隐私保护法》和《加州隐私权与执法法案》，将个人信息分为个人信息、敏感个人信息和儿童个人信息，实行分类保护。

表1 国外数据分类分级框架

法律法规	数据分级
美国《国家安全信息分类》	国家秘密数据：最高机密、机密、秘密
美国《受控未分类信息》及受控非密信息（CUI）相关政策	受控非密数据
/	一般数据：敏感数据、开放数据
欧盟《通用数据保护条例》	敏感个人数据、儿童个人数据、个人数据

我国数据安全治理重要制度之一是数据分类分级保护，通过《保守国家秘密法》《数据安全法》《个人信息保护法》从国家层面确定数据分类分级的框架，将数据划分为三个大类：国家秘密、非密数据、个人信息，如表2所示。

表2 我国数据分类分级框架

法律法规	数据分级
《保守国家秘密法》	国家秘密数据：绝密、机密、秘密
《数据安全法》	非密数据：核心数据、重要数据、一般数据
《个人信息保护法》	敏感个人信息（含儿童个人信息）、个人信息

根据《保守国家秘密法》，国家秘密分为绝密、机密和秘密。根据《数据安全法》，不涉及国家秘密的非密数据分为核心数据、重要数据、一般数据。核心和重要数据应按照法律法规实行严格安全保护。一般数据是指除国家秘密、核心数据和重要数据之外的所有非密数据^[5]。我国个人信息与欧盟个人数据对应，虽然两者在定义上存在差异，但是两者有很大重叠，在实际应用中可等同使用^[7]。《个人信息保护法》提出个人信息和敏感个人信息分级，其中特定身份、金融账户等信息是敏感个人信息，要加强保护。

2 数据分类分级方法

2024年3月15日，国家标准化管理委员会正式发布了国家标准GB/T 43697—2024《数据安全技术 数据分类分级规则》（下称《规则》）^[8]，为全国数据分类分级工作提供统一指导。但是数据分类分级工作比较复杂，各地区、各部门、各行业还应根据自身特点制定更加细化的规则来指导实施。下面分析总结数据分类分级方法，为检验检测认可数据分类分级提供指导。

2.1 数据分类方法

数据分类是指将相同属性的数据归集为不同类别，以方便使用以及进行数据保护^[9]。根据行业、数据来源、数据开放等不同维度^[10]将相同属性数据进行归类。

数据分类要根据数据管理和使用需求^[8]出发，通常按照先行业再业务的顺序进行分类。在行业维度，数据可分为教育、金融、科技、交通等数据；在业务维度又可以根据不同业务属性进行不同分类，比如数据根据描述对象分为用户数据、业务数据、运维数据等，根据数据主体分为公共数据、组织数据、个人数据。不同行业、不同组织、不同业务场景，数据的分类方法可以不同，没有一定之规，应坚持便于数据管理和使用的原则，灵活制定分类方式将数据细化分类。

2.2 数据分级方法

按照《规则》，数据分级首先应识别数据分级要素，然后分析数据影响评估，最后综合确定数据级别^[8]。识别数据分级要素就是识别影响数据分级的要素，包括定性要素、定量要素和衍生数据分级要素，其中定性要素含领域、群体、区域、重要性等，定量要素含精度、规模、覆盖度等，衍生数据分级要素通常指深度^[8]。由于数据分级要素不同，同一类数据可以被划分为不同级别。

根据影响对象、影响程度来划分数据级别，一般分为核心数据、重要数据和一般数据，如表3所示。此外，根据《规则》，满足以下任一条件的数据也应被识别为重要数据：（1）数据直接关系国家安全、经济运行、社会

稳定、公共健康和安全的特定领域、特定群体或特定区域^[8]；(2) 数据达到一定精度、规模、深度或重要性，直接影响国家安全、经济运行、社会稳定、公共健康和安

表 3 数据级别确定规则

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据

根据《数据安全法》的规定，国家或地方主管部门应当确定部门、地区、行业的核心数据目录、重要数据目录^[8]。因此，在识别核心数据或重要数据后，数据处理者应上报国家主管部门，最终以主管部门确认的核心数据目录、重要数据目录为准。

除了核心数据、重要数据外，其他数据都属于一般数据，其涵盖数据范围较广。为了更好实现数据安全保护和开发利用之间的平衡，对一般数据进一步分级。比如按照数据一旦泄露、篡改、损毁或者非法获取、非法使用、非法共享，对经济运行、社会秩序、公共利益或者个人权益、组织权益等造成的危害程度，将一般数据从高到低依次分为 4 级、3 级、2 级和 1 级，如表 4 所示。另外，一般情况下个人信息属于一般数据，其中敏感个人信息作为重点保护对象划为 4 级，一般个人信息则 2 级以上^[8]。敏感个人信息主要包括身份信息、财产信息、生物识别信息等^[11]，可参考国家标准 GB/T 35273—2020《信息安全技术 个人信息安全规范》相关内容。

表 4 一般数据分级规则

一般数据分级	影响对象		数据示例
	经济运行、社会秩序、公共利益	个人权益、组织权益	
4 级	一般危害	特别严重危害	敏感个人信息、严格受控数据
3 级	/	严重危害	一般个人信息、受限制的内部数据
2 级	/	一般危害	一般个人信息、有条件公开数据
1 级	/	无危害	无条件公开数据

3 检验检测认可数据分类分级方案

3.1 检验检测认可数据特点分析

检验检测认可数据是 CNAS 重要程度最高的数据，存在自身特点：

(1) 数据重要程度高。CNAS 是我国国家认可机构，其认可业务涉及全国的实验室、检验机构等检验检测机构，其数据精度、规模、覆盖度呈现出全国性特征，一定程度上反映我国检验检测机构在某一特定领域的全貌，与国家安全、经济运行存在关联性，数据重要程度很高。

(2) 个人信息涉及特定群体，数据比较敏感。认可数据中的授权签字人都是我国检验检测领域的专家。这些个人信息涉及了特定群体，其精确程度明显超过互联网上的个人信息。

(3) 数据量不是很大。检验检测认可数据主要包括机构基本信息、授权签字人信息、检测能力范围等。全国检验检测机构数量在几万数量级，授权签字人在几十万左右，虽然数据存在历年数据累积情况，但是总体来看数据量不是很庞大，且个人信息存在重复现象。

3.2 检验检测认可数据分类分级流程

在遵循国家和行业领域数据分类分级要求的基础上，按照认可行业领域特点开展数据分类分级工作，具体流程如图 1 所示。

(1) 明确数据范围：对检验检测认可数据资产进行全面梳理，确定待分类分级的数据资产范围。

(2) 收集数据项，识别数据分级要素：调研收集每个数据项，并识别数据的领域、区域、重要性等定性要素，规模、覆盖度等定量要素，深度等衍生要素。

(3) 划分数据类型：根据检验检测认可数据特点，按照便于数据管理和使用的原则，划分数据类型、子类，比如采用描述对象方式进行分类。

(4) 确定数据分级：首先应根据国家主管部门确定的本行业核心数据目录和重要数据目录进行比对是否存在核心数据和重要数据；如果未收到国家主管部门确定的本行业核心数据目录和重要数据目录，则根据《规则》进行核心数据和重要数据的识别，判定形成组织的核心数据目录、重要数据目录；接着将剩余数据都确定为一般数据，并结合数据分级要素情况，对数据的影响对象和影响程度进行判定，综合确定每个数据项在一般数据中的分级。数据级别判定可采用内部评审、专家评审等方式来增加结果的合理性。

(5) 汇总上报数据分类分级结果：对数据分类分级结果进行汇总审核，形成 1 个清单和 2 个目录，即数据分类分级清单、重要数据目录和核心数据目录，并将重要

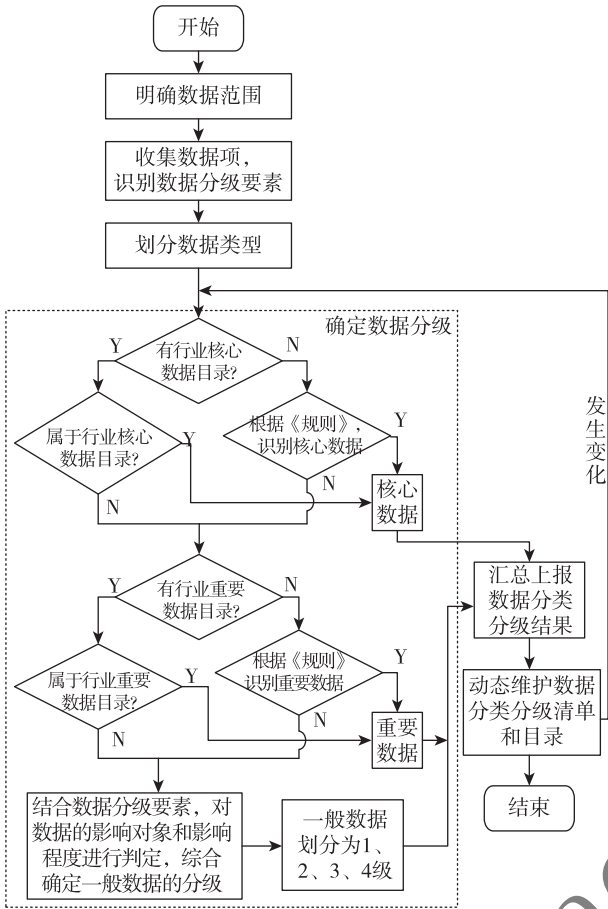


图1 数据分类分级流程

数据目录和核心数据目录上报国家主管部门进行确认。

(6) 动态维护数据分类分级清单和目录：当国家主管部门确认的核心数据目录和重要数据目录变更、数据分级要素发生变化或者数据影响对象和影响程度发生变化时，应当及时对数据进行重新分级，动态更新核心数据目录、重要数据目录和一般数据清单。比如数据规模、数据覆盖率发生显著变化，导致原数据分级不再适用；比如数据进行了脱敏或删除关键字段等匿名化处理，可以降低数据级别。

3.3 检验检测认可数据分类分级规则

结合检验检测认可数据特点，本文提出检验检测认可数据分类分级规则。

检验检测认可数据分类规则采用描述对象方式进行分类，如图2所示。

首先设计一级分类，即检验检测认可业务管理数据；在检验检测认可业务管理数据一级分类下，按照实验室、检验机构划分出二级分类；然后在二级分类下，按照基本信息、授权签字人、能力范围再划分三级分类，比如将实验室认可管理数据划分为实验室基本信息、授权签字人信息、检测能力范围。

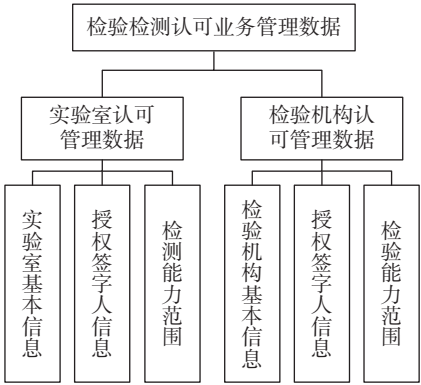


图2 检验检测认可数据分类示例图

按照数据重要程度，将检验检测认可数据划分为重要数据、一般数据，其中一般数据从高到低进一步分为4级、3级、2级和1级。表5给出检验检测认可数据的分类分级示例，为后续数据分级安全保护提供参考。

表5 检验检测认可数据分类分级示例

数据分类			数据项	数据分级
数据一级分类	数据二级分类	数据三级分类		
检验检测认可业务管理数据	实验室认可管理数据	实验室基本信息	名称	一般数据/1级
			地址	一般数据/1级
			...	...
		授权签字人信息	姓名	一般数据/2级
			证件号码	一般数据/4级
			授权领域	重要数据
		检测能力范围	手机号码	一般数据/4级
			...	...
			检测对象	重要数据
			检测项目	重要数据
	检验机构认可管理数据	检验机构基本信息	检测标准	重要数据
			...	...
			名称	一般数据/1级
			地址	一般数据/1级
			姓名	一般数据/2级
检验机构认可管理数据	授权签字人信息	证件号码	一般数据/4级	
		邮箱	一般数据/2级	
		授权领域	重要数据	
		教育/培训经历	一般数据/3级	
	检验对象	工作经历	一般数据/3级	
		...	...	
		检验对象	重要数据	
		检验项目	重要数据	
检验能力范围	检验标准	重要数据		
	...	...		

检验检测认可数据分级规则如下:

(1) CNAS 检验检测认可数据覆盖全国众多实验室和检验机构,其数据精度、规模、覆盖度呈现出全国性特征,因此在数据分级时应作为分级判定的重要依据。检测能力范围、检验能力范围、授权签字人的授权领域,是认可数据中的关键信息,可反映检验检测机构这一特定领域的全貌,与国家安全、经济运行相关,拟采用就高从严原则按重要数据进行管理。

(2) 由于 CNAS 检验检测认可数据中的个人信息规模不是很大,因此个人信息都划分为一般数据,再根据敏感程度不同划分为 3 级,其中,手机号、身份证号等敏感个人信息被划分为 4 级;教育/培训经历、工作经历涉及个人隐私,被划分为 3 级;姓名、邮箱等个人信息被划分为 2 级。

(3) 除个人信息外,实验室基本信息和检验机构基本信息包括名称、地址,是无条件公开数据,在互联网上都能查询,被划分为一般数据中的 1 级。

(4) 对于数据集的分级,以数据集所含数据项的最高级作为数据集级别。比如实验室认可管理数据包含的检测能力范围是重要数据,所以实验室认可管理数据作为数据集也应识别为重要数据。

3.4 数据分级安全保护措施

数据分类分级目的是为了对不同级别数据实施差异化保护,以实现数据安全和数据利用之间的平衡。本文从管理和技术两个方面提出安全保护措施,以期建立完善的数据分级安全保护体系。

(1) 建立完备的数据安全组织管理架构。根据《数据安全法》要求,明确网络数据安全负责人和网络数据安全管理机构,并配备数据安全岗位人员,保障数据安全要求有效落地执行。

(2) 制定完善的数据安全管理制度。开展数据安全管理制度顶层设计,建立分类分级规范、分类分级安全保护、数据安全应急响应等制度,并对全员进行宣贯培训,明确各岗位数据安全风险。

(3) 建立覆盖数据全生命周期的数据安全技术管控平台。①在数据采集阶段,通过身份认证对数据采集人员进行鉴别,确保数据来源可靠;②在数据传输阶段,采用加密、水印等技术实现数据传输安全;③在数据存储阶段,采用加密、访问控制、分级存储、容灾备份等技术实现数据分级存储和分级访问;④在数据使用和加工阶段,采用数据脱敏、隐私计算、日志审计、身份认证、访问控制等技术实现数据分级使用;⑤在数据共享阶段,采用数据防泄漏技术实施动态数据共享监控,阻止数据违规共享;⑥在数据销毁阶段,根据数据不同分

级制定逻辑擦除、低级格式化、物理销毁等不同销毁策略,实现操作方便和数据安全的统一。

(4) 建立合理有效的数据分级安全管控技术体系。

①最小化权限控制:以最小化原则实行统一身份认证和权限管理,对特权账号实行严格审批,依据不同数据分级设定对应用户角色的不同权限,对具有 4 级及以上数据访问权限的账号采用多因素身份认证;②分级访问控制:根据不同数据分级设计不同的访问控制策略,实现细粒度的分级管控,包括基于角色的访问控制、基于数据属性的访问控制等;③分级存储管理:确保不同级别数据存储在物理介质中,并依据不同数据分级设计不同存储方式,比如对 3 级及以上数据采用国密加密存储,重要数据采用容灾备份,2 级及以下数据可明文存储;④分级使用管控:采用脱敏、水印、隐私计算等技术实现不同级别数据的使用管控,比如 2 级及以下数据可采用水印技术,3 级及以上数据采用脱敏技术解决低级别用户的查看需求;⑤数据防泄漏分级监测:采用数据防泄露技术对数据分级使用情况进行实时监测,阻止数据违规使用;⑥分级销毁控制:按照数据分级提供不同的销毁方式,确保数据销毁的安全。

4 结论

数据分类分级是实现数据分级安全保护的前提条件,在实践中如何实现数据安全和数据利用之间的平衡是重大研究课题。本文首先回顾了国外和国内数据分类分级现状;然后分析数据分类分级方法;接着在分析 CNAS 检验检测认可数据特点的基础上,提出检验检测认可数据分类分级流程和分类分级规则并给出示例;最后提出数据分级安全保护措施思路,以期为数据分类分级安全保护研究提供一定参考。

参考文献

- [1] 王剑,赵瑞雪,杨晓蓉,等.数据分类分级:实践进展与经验启示[J].数据与计算发展前沿,2024,6(6):10-18.
- [2] 牛兴荣,耿雷,程燕声,等.CNAS 实验室认可能力数据分析与规范化治理研究[J].中国检验检测,2020,28(4):46-48.
- [3] 完颜邓邓,陶成熙.美国政府数据分类分级管理的实践及启示[J].情报理论与实践,2020,43(12):172-177,155.
- [4] 陈祥玲.政府数据分类分级保护的逻辑、现实困境与实践路径[J].征信,2023,41(4):36-44.
- [5] 王健,周国民,张建华,等.科学数据分类分级保护探索:框架与模式[J].农业大数据学报,2024,6(3):307-324.

(下转第 78 页)

[16] 冯洋. 公共数据授权运营的行政许可属性与制度建构方向 [J]. 电子政务, 2023 (6): 77-87.

[17] 宋烁. 公共数据授权运营中的权责分配 [J]. 法学论坛, 2024, 39 (5): 99-111.

[18] 马颜昕. 公共数据授权运营的类型构建与制度展开 [J]. 中外法学, 2023, 35 (2): 328-345.

[19] 康拉德·黑塞. 联邦德国宪法纲要 [M]. 李辉, 译. 北京: 商务印书馆, 2007.

[20] 王本刚, 马海群. 公共数据的公共价值研究——以国内外相关政策和报告为核心的解读 [J]. 情报理论与实践, 2022, 45 (10): 1-10.

[21] 梁风云. 行政公产研究导论 [J] 行政法论丛, 2003 (1): 182-218.

[22] 胡业飞, 田时雨. 政府数据开放的有偿模式辨析: 合法性根

基与执行路径选择 [J]. 中国行政管理, 2019 (1): 30-36.

[23] 李悦. 激励与规制: 公共数据授权运营的法律机构构建 [J]. 行政与法, 2023 (6): 39-50.

[24] 胡穗, 胡南. 政府数据开放: 中美比较与路径优化 [J]. 湖湘论坛, 2017, 30 (4): 118-123.

[25] 郑磊, 熊久阳. 中国地方政府开放数据研究: 技术与法律特性 [J]. 公共行政评论, 2017, 10 (1): 53-73, 206.

[26] 祝灵君, 聂进. 公共性与自利性: 一种政府分析视角的再思考 [J]. 社会科学研究, 2002 (2): 7-11.

(收稿日期: 2025-04-25)

作者简介:

李佳欣 (2000-), 女, 硕士研究生, 主要研究方向: 数字法学、行政法学。

(上接第64页)

[6] 邵晶晶, 韩晓峰. 国内外数据安全治理现状综述 [J]. 信息安全研究, 2021, 7 (10): 922-932.

[7] 田雨婕. 欧盟法视野下我国政府数据开放中个人信息保护的制度完善 [J]. 宜宾学院学报, 2025, 25 (2): 50-56, 65.

[8] 国家市场监督管理总局, 国家标准化委员会. GB/T 43697-2024 数据安全技术 数据分类分级规则 [S]. 北京: 中国标准出版社, 2024.

[9] 张琼丽, 陈翼. 数据分级分类方法及实践研究 [J]. 技术与市场, 2022, 29 (8): 150-153.

[10] 张勇. 数据安全分类分级的刑法保护 [J]. 法治研究, 2021 (3): 17-27.

[11] 国家市场监督管理总局, 国家标准化委员会. GB/T 35273

-2020 信息安全技术 个人信息安全规范 [S]. 北京: 中国标准出版社, 2020.

(收稿日期: 2025-04-30)

作者简介:

金达 (1982-), 男, 硕士, 正高级工程师, 主要研究方向: 网络安全、数据安全。

霍珊珊 (1981-), 女, 本科, 高级工程师, 主要研究方向: 网络安全、数据安全。

李彦军 (1981-), 通信作者, 男, 硕士, 高级工程师, 主要研究方向: 软件工程、认可信息化管理。E-mail: liyj@cnas.org.cn。

(上接第70页)

[19] 济南市审计局. 关于济南市2023年度市级预算执行和其他财政收支的审计工作报告 [R/OL]. (2024-08-30) [2025-03-20]. http://jinanaudit.jinan.gov.cn/art/2024/8/30/art_31371_4776205.html.

[20] 陈佳举. 法律行为理论下个人信息保护的知情同意研究 [J]. 中国政法大学学报, 2023 (2): 197-207.

[21] 中国信息通信研究院. 数字消费者权益保护白皮书 (2023) [R/OL]. (2023-10-xx) [2025-03-20]. http://www.caict.ac.cn/kxyj/qwfb/bps/202310/t20231031_464867.htm.

[22] 张素华, 刘寅. 公共数据授权运营收益分配的实践困境及制度构建 [J]. 行政管理改革, 2025 (5): 35-45.

[23] 国务院. 网络数据安全管理条例: 国令第790号 [Z]. 2024.

[24] 侯晨亮, 杨东. 平台剥削用户数据的形态、成因及规制 [J]. 中国特色社会主义研究, 2022 (Z1): 76-83.

[25] 北京市第四中级人民法院. 保护个人信息 规范数据利用

——北京互联网法院通报涉个人信息及数据相关案件审理情况 [R/OL]. (2024-10-30) [2025-03-20]. <https://bj4zy.bjcourt.gov.cn/article/detail/2025/10/id/9044402.shtml>.

[26] 徐倩倩. 个人信息保护与数据利用的冲突与平衡 [J]. 法制博览, 2024 (13): 22-24.

[27] 王龙. 政府数据安全风险治理的机理逻辑与优化策略 [J]. 科学学研究, 2024, 43 (5): 931-942.

(收稿日期: 2025-04-17)

作者简介:

武万里 (2001-), 男, 硕士研究生, 主要研究方向: 数据治理、数据安全、安全治理。

王龙 (1978-), 男, 博士, 副教授, 主要研究方向: 数据安全治理、战略管理。

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