

ICS 点击此处添加 ICS 号

CCS 点击此处添加 CCS 号

T/CADPA

中国音像与数字出版协会团体标准

T/CADPA XXXX—XXXX

出版业生成式人工智能技术应用指南

Application guidelines of generative artificial intelligence technology in publishing industry

（征求意见稿）

（本草案完成时间：2023-11-14）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国音像与数字出版协会 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 基本原则	1
4.1 导向性	1
4.2 合规性	1
4.3 隐私性	1
4.4 安全性	1
4.5 透明性	1
4.6 公平性	2
4.7 准确性	2
4.8 先进性	2
4.9 适用性	2
4.10 价值性	2
5 主要应用场景	2
5.1 信息采集	2
5.2 辅助创作	2
5.3 辅助审核	2
5.4 智能编加和校对	2
5.5 宣传推广	2
5.6 辅助决策	2
5.7 知识服务	2
5.8 其他场景	3
6 管理机制	3
6.1 出版机构	3
6.2 服务提供者	3
7 知识产权	3
8 安全保障	3
8.1 语料安全	3
8.2 模型安全	3
8.3 数据安全	3
8.4 网络安全	3
8.5 系统安全	3
参 考 文 献	4

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国音像与数字出版协会出版融合工作委员会提出。

本文件由中国音像与数字出版协会归口。

本文件起草单位：北京印刷学院、化学工业出版社有限公司、机械工业出版社有限公司、人民邮电出版社有限公司

本文件主要起草人：XXX

出版业生成式人工智能技术应用指南

1 范围

本文件规定了出版业应用生成式人工智能技术的基本原则、主要应用场景和相应的保障措施。本文件适用于出版机构应用生成式人工智能技术提供的服务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273—2020 信息安全技术 个人信息安全规范

CY/T 96—2013 电子书内容术语

3 术语和定义

CY/T 96界定的以及下列术语和定义适用于本文件。

3.1

生成式人工智能技术 generative artificial intelligence technology

基于算法、模型和大规模语料自动生成文本、图片、声音、视频、代码等内容的自然语言处理技术。

3.2

出版机构 publishing institution

从事出版活动的专业机构。

[来源：CY/T 96—2013，定义4.1.4]

3.3

服务提供者 service provider

以交互界面、可编程接口等形式面向我国境内公众提供生成式人工智能服务的组织或个人。

4 基本原则

4.1 导向性

确保利用人工智能技术生成的内容导向正确，符合国家相关法律法规和伦理准则，尊重社会价值观和道德标准，以促进生成式人工智能技术应用向上向善。

4.2 合规性

用于生成式人工智能技术训练的数据来源合法，尊重知识产权。同时相关服务提供者不滥用市场优势地位，遵守反垄断法规，维护公平竞争环境，促进创新和多样性。

4.3 隐私性

出版机构和服务提供者按照GB/T 35273等国家有关规定要求，在数据收集、存储、使用和共享过程中做好个人隐私的保护。

4.4 安全性

出版机构和服务提供者在数据收集、存储、使用、加工、传输、提供、公开的过程中应提供相关措施确保数据安全和自主可控。同时服务提供者应提供安全、稳定、持续的服务，以保障出版机构和其他用户的正常使用。

4.5 透明性

在应用生成式人工智能技术的过程中，包括出版机构、服务提供者在内的所有参与者都应了解并明确披露人工智能内容生成的使用情况，包括底层数据集、数据来源和数据处理方法等。

4.6 公平性

在训练数据选择、算法设计、模型生成和优化、使用过程中仔细评估和审查潜在的数据和内容偏差来源，同时减少人工智能生成内容在文化或者语言上的不公平现象。

4.7 准确性

对利用人工智能技术进行预训练、优化训练的数据来源应准确、描述应客观和数据应多样，避免虚假信息和误导性的内容传播。

4.8 先进性

出版机构选择具有先进的人工智能生成内容技术和算法模型的服务提供者，即该服务提供者所具有的算法核心指标（例如参数规模）和权威评测得分在行业内达到领先水平。

4.9 适用性

服务提供者提供的人工智能生成内容技术和相应工具应满足出版机构对内容资源管理和应用的需求。

4.10 价值性

出版机构对外提供人工智能生成的内容具有一定的思想性、艺术性、知识性、逻辑性和科学性。

5 主要应用场景

5.1 信息采集

根据市场需求或选题策划，利用生成式人工智能技术在信息搜索、信息整合等方面的能力选取合适的内容用于出版。

5.2 辅助创作

利用生成式人工智能技术工具帮助编辑和作者生成创意写作的草稿内容。

5.3 辅助审核

利用生成式人工智能技术工具，对出版内容是否符合国家有关出版管理的要求进行初步审查，特别是对意识形态、法律法规、敏感内容、版权等方面进行排查，并提供相应的审读报告和标识，供人工审核确认。

5.4 智能编加和校对

利用生成式人工智能技术工具，进行初步的语言学编辑、加工，以及字词错误校对、用语规范性校对、体例格式校对等。排版、版式设计等形式的加工工作也可借助生成式人工智能工具完成。

5.5 宣传推广

利用人工智能技术生成的内容开展新媒体运营、出版内容的推广或者出版机构的品牌营销活动，提升出版机构的品牌影响力以及出版内容的触达率、阅读率和影响力。

5.6 辅助决策

利用生成式人工智能技术具有的数据分析能力，可识别行业发展趋势和模式，指导制定出版计划和战略，以辅助出版决策。

5.7 知识服务

利用生成式人工智能技术，以信息采集、组织分析为基础，根据用户需求和信息环境，提供能够有效支撑知识应用和创新的出版内容服务，且能够注明必要的引用来源和参考文献。

5.8 其他场景

出版机构可利用生成式人工智能技术进行出版物封面、插画等内容的辅助设计，出版物内容的辅助翻译、语义分析，数据搜集、整理与分析等工作。

6 管理机制

6.1 出版机构

出版机构在应用生成式人工智能技术和相关工具的过程中应遵循《出版管理条例》《网络出版服务管理规定》和本机构的出版业务流程管理规范等，加强内容筛选、审核和人员培训工作，做好相关内容安全和质量安全管理。

6.2 服务提供者

服务提供者需建立相应的算法机制机理审核、科技伦理审查、用户注册、信息发布审核、数据安全和个人信息保护、安全事件应急处置等方面的管理制度，配备与其服务规模相适应的专业人员和技术支撑。

7 知识产权

出版机构和服务提供者需对人工智能生成内容的使用情况进行充分、正确的披露和声明，未经权利人和相关利益方的具体和明确许可，其不得以任何方式或者授权他人以任何形式将有关作品内容用于生成式人工智能技术的训练。

8 安全保障

8.1 语料安全

出版机构和服务提供者应建立相关的语料来源黑名单，加强对各来源语料的安全评估和标注人员的培训考核，确保用于生成式人工智能技术预训练的语料安全。

8.2 模型安全

服务提供者使用的生成式人工智能技术基础模型，应经国家主管部门备案；对提供的服务使用人群以及使用第三方基础模型情况进行公开；加强对使用者输入信息的安全分析和生成内容准确性方面的评估，以保证服务提供者的模型安全。

8.3 数据安全

在应用生成式人工智能技术时，应按国家有关规定对数据的处理、传输、访问使用有效的加密和控制手段，保障数据安全、保护个人隐私。

8.4 网络安全

按照国家有关规定，配置相应的防火墙、网络监控工具、身份验证措施、接口安全、入侵检测等网络安全措施。

8.5 系统安全

在提供生成式人工智能技术服务时，服务提供者需遵循国家有关规定具有安全的系统架构设计、操作系统和硬件安全保障和应用程序等，以保证系统安全平稳运行。

参 考 文 献

- [1] 中华人民共和国数据安全法（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）
- [2] 中华人民共和国网络安全法（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）
- [3] 网络信息内容生态治理规定（2019年12月15日国家互联网信息办公室令第5号公布）
- [4] 互联网信息服务深度合成管理规定（2022年11月3日国家互联网信息办公室2022年第21次室务会议审议通过）
- [5] 互联网信息服务算法推荐管理规定（2022年3月1日起实行）
- [6] 生成式人工智能服务管理暂行办法（2023年7月10日国家互联网信息办公室 中华人民共和国国家发展和改革委员会 中华人民共和国教育部 中华人民共和国科学技术部 中华人民共和国工业和信息化部 中华人民共和国公安部 国家广播电视总局令第15号公布）
-