ICS 33.030
CCS M 21

团　体　标　准

T/TAF 209.9—2024

移动互联网应用程序（APP）合规开发管理测评规范　第9部分：算法模型

Evaluation specification for compliance development of mobile Internet application—Part 9: Algorithm model

2024-02-23 发布　　2024-02-23 实施

电信终端产业协会　发布

目　　次

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。

本文件是T/TAF 209《移动互联网应用程序（APP）合规开发管理测评规范》的第9部分。T/TAF 209已经发布了以下部分：

——第1部分：总则；
——第2部分：需求设计；
——第3部分：功能测试；
——第4部分：代码审计；
——第5部分：对外接口管理；
——第6部分：应用编程接口（API）管理；
——第7部分：更新升级管理；
——第8部分：数据使用管理；
——第9部分：算法模型；
——第10部分：人员能力；
——第11部分：能力成熟度评估。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、上海寻梦信息技术有限公司、北京微梦创科网络技术有限公司、每日互动股份有限公司、蚂蚁集团科技股份有限公司、武汉安天信息技术有限责任公司、厦门美柚股份有限公司、北京小桔科技有限公司、北京三快科技有限公司、北京快手科技有限公司、百度在线网络技术（北京）有限公司、维沃移动通信有限公司、北京抖音信息服务有限公司、华为终端有限公司。

本文件主要起草人：邓佑军、汪海、王浩仟、张静怡、朱政、徐宁、杨震、徐子涵、张鹏、任资政、邹庆、王天、方毅、叶新江、董霖、林冠辰、余丽娜、黄鹏华、张娜、王芳、吴斌、徐辉、冷杉、落红卫、王昕、郭建领、廖文娟、赵盈洁、李昳婧、靳鑫亚、潘洁、李实。

引　言

随着数字经济的快速发展，大数据、人工智能已经融入社会生产生活的各个领域，大数据杀熟、流量造假、隐私泄露、AI换脸、虚假文案、诱导沉迷等问题给网络空间带来了严峻挑战，也严重的侵害了用户的权益，其核心技术算法模型也逐步引起人们的关注。为此，国家有关部门已经出台了《互联网信息服务深度合成管理规定》《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理暂行办法》等一系列与算法相关的行政法规，明确算法的管理要求。为了更好的促进算法模型的合规运行，本文件将合规关口前移至开发阶段，提出了算法模型不同开发阶段的具体要求，并明确了各要求的测评方法。

T/TAF 209旨在对APP开发流程、功能模块、工程管理等提出合规开发管理要求，拟由11部分构成。

——第1部分：总则。目的在于给出规范移动互联网应用程序（APP）合规开发的总体原则和要求。

——第2部分：需求设计。目的在于提出规范APP需求设计环节的相关合规开发要求。

——第3部分：功能测试。目的在于规范移动互联网应用程序（APP）在合规开发阶段满足功能测试的标准要求。

——第4部分：代码审计。目的在于规范APP代码审计过程，提升代码安全管理能力。

——第5部分：对外接口管理。目的在于规范APP对外接口的合规开发和使用管理，提升合规能力。

——第6部分：应用编程接口（API）管理。目的在于规范APP在开发过程中对于API的使用，提升合规能力。

——第7部分：更新升级管理。目的在于规范APP合规开发在更新升级阶段的要求，提升APP更新升级管理能力。

——第8部分：数据使用管理。目的在于规范APP在合规开发过程中数据使用的合规管理，提升数据使用合规管理能力。

——第9部分：算法模型。目的在于规范APP合规开发在算法模型方面的要求，提升APP算法模型开发的合规管理能力。

——第10部分：人员能力。目的在于规范APP在合规开发过程中的人员能力管理。

——第11部分：能力成熟度评估。目的在于规范APP在合规开发管理过程中的能力成熟度评估。

移动互联网应用程序（APP）合规开发管理测评规范　第9部分：算法模型

1　范围

本文件规定了移动互联网应用程序（APP）中涉及与用户权益、或具有舆论属性或者社会动员能力相关的算法模型的合规开发管理要求及测评方法。

本文件适用于移动互联网应用程序开发者在开发算法模型时规范其个人信息保护、用户权益保护等方面的合规行为。也适用于监管部门、第三方评估机构等组织对算法模型的合规开发进行监督、管理和评估。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

算法　algorithm

依据给定的规则，根据数据解决特定问题的方法。可以用于确定模型参数。

3.2

模型　model

一种基于输入数据或信息生成推理或预测的计算结构，通常是算法运行得到的结果。

3.3

数据集　datasets

数据记录汇聚的数据形式。

[来源：GB/T 35295—2017]

4　缩略语

下列缩略语适用于本文件。

APP：移动互联网应用程序（Mobile Internet Application）

5　APP算法模型开发管理要求

5.1 概述

APP算法模型开发管理生命周期可分为需求、设计、编码、测试和维护五个阶段。需求阶段是明确算法模型要达到的目的;设计阶段是明确算法模型要实现的功能;编码阶段是明确功能实现的方式方法;测试阶段是确认方式方法是否能实现功能与达到目的;维护阶段是优化或改良算法模型,提升算法模型的合规性、安全性、准确性、健壮性。APP算法模型开发管理应满足以下基本原则:

a) 合法合规:应符合相关法律法规的规定,避免算法模型对应的APP服务引起社会公平、道德伦理、个人信息安全、网络安全等方面的风险;
b) 公平公正:算法模型对应的APP服务应当公平公正,不得实行不合理的差别待遇,不得利用算法模型开展不正当竞争;
c) 公开透明:以适当方式向用户公开算法模型处理活动处理用户信息的范围、目的、规则;
d) 科学合理:根据行业类型、业务场景等实际情况,科学、合理地设置相关参数条件和权重、决策规则。

5.2 需求阶段

需求阶段是通过调研和分析,理解用户和项目应用功能、性能等具体要求,最后确定算法模型应实现的功能性需求、非功能性需求和应满足的设计约束的阶段。算法模型需求阶段的具体要求如下:

a) 需求基本要求。算法模型需求提出应以企业业务需求为导向,坚持主流价值导向,不得提出法律、行政法规禁止的需求。不得提出诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的需求。不得提出从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律、行政法规禁止的需求。
b) 需求提出要求。宜明确算法模型的提出部门、目的和目标、算法模型的名称、算法类型、基础功能、基本原理、运行机制、约束条件等。
c) 应用场景要求。APP使用的算法模型应与其实际业务场景相符合;应当向用户提供算法模型的目的等以增强其可解释性。
d) 知识产权要求。企业应明确算法模型的权属关系,委托第三方开发的,应与第三方签订协议进行约定。
e) 需求评估要求。企业内部应对算法模型需求进行评估,相关评估记录宜妥善保存以便后期测评。

5.3 设计阶段

设计阶段是根据算法模型需求阶段得到的需求分析,设计出满足设计约束并能够实现任务功能性需求、非功能性需求的目标函数及相应的算法模型。算法模型设计阶段的具体要求如下:

a) 设计基本要求。算法模型设计时不得违反《互联网信息服务深度合成管理规定》《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理暂行办法》《关于进一步提升移动互联网应用服务能力的通知》等相关法律法规要求。
b) 团队要求。算法模型开发部门或第三方机构应配备与算法模型开发相适应的专业人员和技术支撑,明确算法模型的直接负责人。
c) 功能要求。应满足需求阶段相对应的功能和应用场景。
d) 制度要求。应制定算法模型配套的开发管理制度,明确该算法模型的开发管理机制,确保算法模型相关核心技术的机密性,委托第三方开发的,应与第三方签订保密协议。
e) 数据集要求。应明确算法模型的数据来源,涉及处理个人信息的,应按照法律法规要求获得用户同意或其他合法性基础,并严格控制其访问权限,具备对数据访问和操作等行为审计能力。
f) 最小必要要求。应确保算法模型所需的最小必要数据,避免过度收集不必要的个人信息。

g） 隐私保护要求。应确保算法模型能保护用户的个人隐私，防止敏感信息泄露；宜采取加密、混淆等技术手段，提供对算法模型参数的安全保护手段。

h） 防歧视要求。应确保算法模型能公平对待所有用户群体，不应存在歧视性，包括但不限于民族、信仰、国别、地域、性别、年龄、职业、健康等歧视，也包括金融借贷、大数据“杀熟”、人工智能相貌、人工智能机器人发表言论等。

i） 透明化要求。应确保算法模型能够公开其基本原理、主要运行机制、应用场景、目的意图，保护用户的知情权和选择权。

j） 其他要求。设计过程中应同步考虑算法模型的安全性、准确性和健壮性。

k） 设计评估要求。企业内部应对算法模型设计进行评估，相关评估记录宜妥善保存以便后期测评。

5.4 编码阶段

编码阶段是对算法模型设计阶段所设计的算法模型进行编程实现，包括利用数据集对算法模型开展训练、测试与验证等活动。算法模型编码阶段的具体要求如下：

a） 编码基本要求。应养成给代码加注释的良好编程习惯，提高代码的可读性和可维护性。按照设计说明书进行编程，不应编写与设计说明书无关的功能、模块、服务、后门等。

b） 代码安全要求。应采取安全编码标准进行算法模型开发，若引用到开源、第三方产品、技术或代码，应对其进行安全性评估后方可使用；应建立人工干预代码能力，如引入人工权重项，包括触发条件、干预目的、干预手段等；应建立违规内容发现能力，防范恶意行为产生数据对算法模型的威胁。

c） 密码技术要求。涉及到数据传输加密、数据完整性保护或其他密码运算的，应选用国家认可的或行业公认的密码算法和技术标准。

d） 代码存储要求。应确保源代码的安全存储，增加源代码的访问控制，不应将源代码托管保存在不可信的第三方代码托管平台中。

e） 代码审计要求。应对算法模型源代码进行审计，相关审计记录宜妥善保存以便后期测评。

5.5 测试阶段

测试阶段是对算法模型的功能和性能进行全面验证的活动。算法模型测试阶段的具体要求如下：

a） 测试基本要求。应以需求符合性为准绳，秉承公正严明的态度对提交的算法模型进行验证。

b） 测试用例基本要求。测试人员应根据需求说明书和设计说明书编写对应的测试用例和测试方法，并按照测试用例和测试方法进行测试，记录测试结果。

c） 测试用例范围要求。除算法模型基本功能和性能外，测试用例还应覆盖到最小必要、隐私保护、防歧视、安全性、准确性等范围。

d） 测试场景要求。在测试环境搭建、数据集选择等方面，应尽可能模拟真实场景数据，确保算法模型输出结果的准确性。

e） 测试工具要求。应定期对算法模型相关测试工具进行升级、优化或校准，提升结果的准确性。

f） 测试报告要求。测试完成应编写详细的算法模型测试报告，测试报告宜妥善保存以便后期测评。

5.6 维护阶段

维护阶段是指算法模型正式发布并使用后，在使用过程中不断优化和升级的一个过程。算法模型维护阶段的具体要求如下：

a） 维护基本要求。在算法模型生命周期内，应有专业维护人员或团队从事算法模型运行监测、漏洞修复、功能优化、性能优化等算法维护工作，确保算法模型正常运行。应对算法模型的部署

操作者、时间及相关结果、部署过程脚本、软硬件配置等信息内容进行记录，明确主体责任、严格责任制度。

b） 运行监测要求。应制定算法模型运行监测机制，发现违规使用或异常输出时及时处理。

c） 更新要求。算法模型更新时，应按照开发管理规范要求重新进行需求提出、需求设计、编码和测试。

d） 移交转让要求。算法模型负责人发生变化时，应做好交接工作并留存交接记录。发生转让的，应与承接方签订转让协议，并应做好算法备案变更等手续。

e） 合规评估要求。定期查看是否有处理方式变更或其他功能变更事件，在有变更时开展算法模型合规评估，确保算法模型符合相关法律法规要求。

6 APP 算法模型开发管理测试方法

APP算法模型合规开发管理的测试方法主要采用资料审查、技术验证和人员访谈对开发过程的五个环节的各项要求进行符合性评估。具体见表1。

表 1 管理规范与测评方式对应关系表

要求条款	要求名称	测评方式		
		资料审查	技术验证	人员访谈
5.2 a)	需求基本原则	○	○	√
5.2 b)	需求提出要求	√	○	●
5.2 c)	应用场景要求	√	○	●
5.2 d)	知识产权要求	●	○	●
5.2 e)	需求评估要求	√	○	○
5.3 a)	设计基本原则	○	○	√
5.3 b)	团队要求	√	○	●
5.3 c)	功能要求	√	○	●
5.3 d)	制度要求	√	○	●
5.3 e)	数据集要求	√	√	●
5.3 f)	最小必要要求	√	√	●
5.3 g)	隐私保护要求	√	√	●
5.3 h)	防歧视要求	√	√	●
5.3 i)	透明化要求	●	●	√
5.3 j)	其他要求	√	●	●
5.3 k)	设计评估要求	√	○	○
5.4 a)	编码基本原则	○	○	√
5.4 b)	代码安全要求	●	√	○
5.4 c)	密码技术要求	●	√	○
5.4 d)	代码存储要求	●	√	○
5.4 e)	代码审计要求	√	○	○
5.5 a)	测试基本原则	○	○	√
5.5 b)	测试用例基本要求	√	●	○

表 2　管理规范与测评方式对应关系表（续）

要求条款	要求名称	测评方式		
		资料审查	技术验证	人员访谈
5.5 c)	测试用例范围要求	√	●	○
5.5 d)	测试场景要求	●	√	○
5.5 e)	测试工具要求	●	√	○
5.5 f)	测试报告要求	√	○	○
5.6 a)	维护基本原则	○	○	√
5.6 b)	运行监测要求	●	√	○
5.6 c)	更新要求	●	√	○
5.6 d)	移交转让要求	●	○	●
5.6 e)	合规评估要求	√	○	○
注：“√”表示采用的测评方式；“●”表示可选的测试方式；“○”表示不适用。				

参 考 文 献

[1] GB/T 35273—2020 信息安全技术个人信息安全规范
[2] GB/T 35295—2017 信息技术 大数据 术语

电信终端产业协会团体标准

移动互联网应用程序（APP）合规开发管理测评规范 第9部分：算法模型

T/TAF 209.9—2024

*

电信终端产业协会印发

地址：北京市西城区新街口外大街28号

电话：010-82052809

电子版发行网址：www.taf.org.cn