ICS 35.240.01
CCS L78

T/CSAC

团　　体　　标　　准

T/CSAC 023—2025

网络安全技术 向未成年人提供生成式人工智能服务安全指引

Cybersecurity technology — Guidelines for providing generative artificial intelligence services to minors

2025－10－31 发布　　2025－12－01 实施

中国网络空间安全协会　　发 布

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。

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。

本文件由中国网络空间安全协会归口。

本文件由中国网络空间安全协会人工智能安全治理专业委员会提出。

本文件起草单位：中国网络空间安全协会、杭州网易智企科技有限公司、国家信息技术安全研究中心、公安部第三研究所、中国社会科学院大学互联网法治研究中心、中国青少年研究中心、上海人工智能创新中心、浙江省网络空间安全协会、北京师范大学、北京邮电大学、北京互联网法院、北京抖音信息服务有限公司、阿里巴巴 （中国）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、上海稀宇科技有限公司、北京金山办公软件股份有限公司、广州趣丸网络科技有限公司、科大讯飞股份有限公司、华为技术有限公司、杭州安恒信息技术股份有限公司、OPPO 广东移动通信有限公司、蚂蚁科技集团股份有限公司、杭州君同未来科技有限责任公司、北京市中伦律师事务所、北京三快在线科技有限公司(美团)、维沃移动通信有限公司（vivo）、小米科技有限责任公司、深信服科技股份有限公司、三六零数字安全科技集团、北京微梦创科网络技术有限公司、荣耀终端股份有限公司、广东小天才科技有限公司、深圳市和讯华谷信息技术有限公司、长安通信科技有限责任公司、网易有道信息技术（北京）有限公司、广州市动悦信息技术有限公司、北京猿力科技有限公司、北京师范大学出版社（集团）有限公司、成都每经新视界科技有限公司、北京米连科技有限公司、蘑菇车联信息科技有限公司、北京深言科技有限责任公司、联想（北京）有限公司、中通服咨询设计研究院有限公司、南方都市报、中国质量认证中心有限公司、北京市竞天公诚律师事务所、北京市金杜律师事务所、北京大学上海临港国际科技创新中心、广州市中网数据要素发展研究院、中讯邮电咨询设计院有限公司、北京爱诗科技有限公司、贝壳找房（北京）科技有限公司。

本文件主要起草人：郝晓伟、王健兵、夏文辉、贺敏、张震、寇振东、胡文浩、阮良、朱浩齐、苗晴晴、彭韬、沈俊成、任少锋、邓凯、陈光炎、方增泉、吴沈括、郭开元、祝阳、郝春亮、郭建领、孟令宇、李佳笑、落红卫、郝思佳、周杨，崔聪聪、曹岚、李中戈、王海宁、车喆彬、贾建斌、蔡倩楠、尹丹娜、邵萌、韩蒙、刘晓春、郭晓雷、张树玲、邹莹、张琳琳、郑晗旭、韦薇、张磊。

网络安全技术 向未成年人提供生成式人工智能服务安全指引

1 范围

本文件提出了生成式人工智能服务中关于未成年人保护的安全指引，包括安全总体原则、服务全生命周期安全管理、组织与制度保障、未成年人发展与促进，以及内容安全、数据安全、个人信息保护的安全要求。

本文件适用于生成式人工智能服务提供者开展未成年人保护相关活动，也可为相关主管部门、行业提供参考。

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 25069-2022 信息安全技术 术语

GB/T 45654-2025 网络安全技术 生成式人工智能服务安全基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 45674-2025 网络安全技术 生成式人工智能数据标注安全规范

GB/T 45652-2025 网络安全技术 生成式人工智能预训练和优化训练数据安全规范

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

生成式人工智能服务 generative artificial intelligence services

用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等内容的服务。

[GB/T 45654-2025，3.1]

3.2

服务提供者 service provider

以交互界面、可编程接口等形式提供生成式人工智能服务的组织或个人。

[GB/T 45654-2025，3.2]

3.3

面向未成年人的生成式人工智能服务 generative artificial intelligence services for minors

生成式人工智能服务对象中未成年人数量巨大或对未成年人可能产生显著影响的服务。

3.4

服务全生命周期 service full lifecycle

包括训练数据处理阶段、模型训练阶段、场景应用阶段、服务运营阶段等。

3.5

训练数据 training data

所有直接作为模型训练输入的数据，包括预训练数据和优化训练数据。

[GB/T 45654-2025，3.4]

3.6

个人信息 personal information

电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

注1：本文件根据个人信息所处阶段、存在形式不同分为以下3种保护形式：

个人训练数据保护：针对训练数据中存在的未成年人个人信息的保护，保护措施侧重对训练数据的处理；
个人可识别信息保护：针对模型可能生成或输出个人可识别信息的保护，保护措施侧重对模型输出数据的安全处理；
用户个人信息保护：针对在服务用户过程中收集使用个人信息的保护，保护措施需结合产品功能服务所需而定。

[GB/T 35273-2020， 3.1，有修改]

3.7

智能语音交互 smart speech interaction

以语音识别、语义理解、语音合成等全部或部分人工智能技术为基础，由智能软硬件组成，具备智能人机交互能力。

[GB/T 36464.1-2020，3.3，有修改]

4 安全框架

向未成年人提供生成式人工智能服务的安全框架见下图：

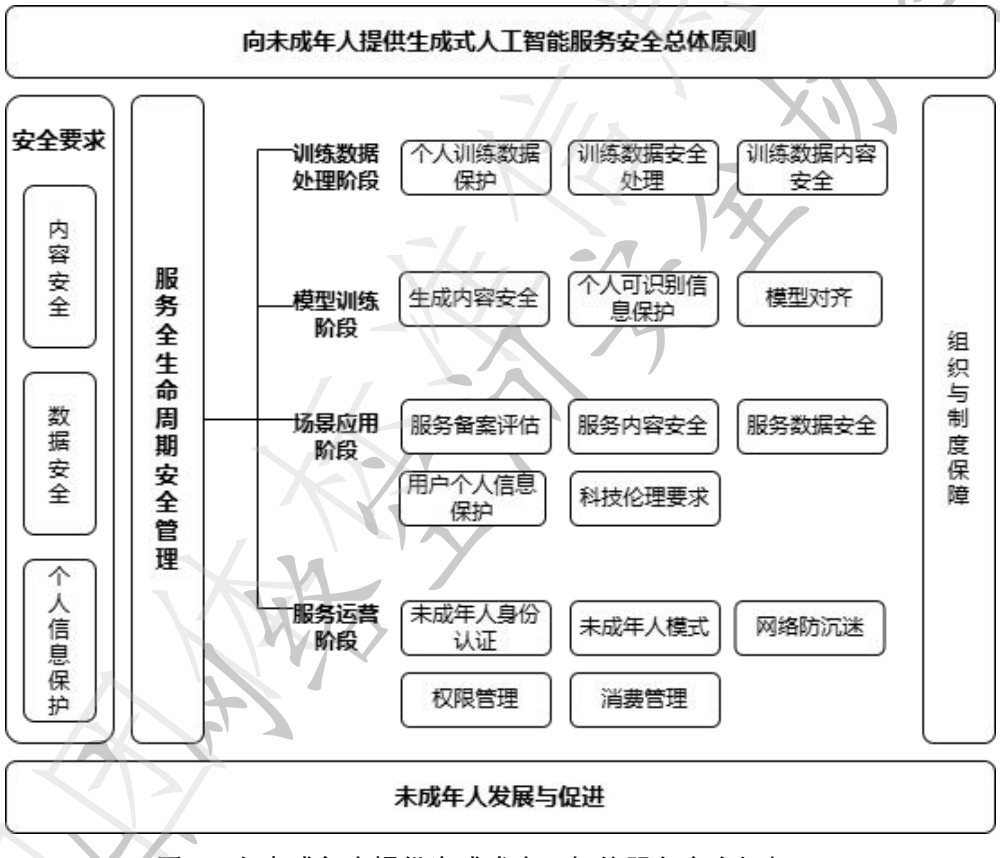

图 1 向未成年人提供生成式人工智能服务安全框架

安全要求包括：内容安全要求、数据安全要求、个人信息保护要求，详见附录 A；以及相关法律法规和部门规章参考，详见附录 B。

服务全生命周期安全管理包括：训练数据处理阶段的个人训练数据保护、训练数据安全处理、训练数据内容安全；模型训练阶段的生成内容安全、个人可识别信息保护、模型对齐；场景应用阶段的服务备案评估、服务内容安全、用户个人信息保护、服务数据安全、科技伦理要求；服务运营阶段的未成年人身份认证、未成年人模式、网络防沉迷、权限管理、消费管理。

组织与制度保障，结合服务全生命周期安全管理要求，建立未成年人保护专项工作组织和专项保障制度。

未成年人发展与促进，鼓励社会、行业、企业共同从未成年人发展权益保护、人工智能素养提升、特色化发展和智能终端协同、行业治理与协作等方面做好未成年人保护。

5 总体原则

5.1 安全原则

向未成年人提供生成式人工智能服务宜遵循以下安全原则：

a) 坚持以社会主义核心价值观为引领，适应未成年人身心健康发展和网络空间的规律和特点，实行社会共治；
b) 坚持最有利于未成年人的原则，在处理涉及未成年人的所有事务时，宜将未成年人的最佳利益作为首要考虑因素，确保未成年人的权益得到最大程度的保护和促进；
c) 遵循科技和道德伦理，以“增进人民福祉、促进公平公正、保护隐私安全、确保可控可信、强化责任担当、提升伦理素养”为原则，面向未成年人研发和提供生成式人工智能服务；
d) 坚持保护与发展并重，在“以人为本、智能向善”理念的指导下，兼顾未成年人网络保护和人工智能素养发展。

5.2 主体责任

服务提供者宜积极履行未成年人保护的主体责任：

a) 遵循保护与发展基本原则，建立常态化工作机制；
b) 明确工作规范，健全管理制度，完善服务运营规则；
c) 提升生成式人工智能技术和应用的风险识别、评估、处置能力，建立事前规划、事中管控、事后监测的一体化保护机制，防范和化解各种风险隐患。

6 服务全生命周期安全管理

6.1 训练数据处理阶段

6.1.1 个人训练数据保护

服务提供者应针对采集训练数据中的未成年人个人信息制定保护措施，包括：

a) 确保训练数据来源的合法性；
b) 使用自采数据时，不采集未成年人或其监护人已明确不可采集的数据；
c) 使用商业数据时，对交易方或合作方所提供涉未成年人个人信息的训练数据承诺材料进行审核；
d) 明确收集数据的范围和目的，严格限制收集未成年人的非必要数据，防止过度采集或与服务目的无关的数据处理；
e) 将未成年人用户输入的个人信息用于训练时，需取得用户同意，将不满十四周岁的未成年人用户输入的个人信息用于训练时，需取得其监护人的同意；
f) 以唯一识别自然人身份为目的使用包含未成年人生物特征信息的个人信息时，需获得其监护人的单独同意，或满足其他合法使用该生物特征信息的条件；
g) 可采取去标识化等技术措施保护未成年人个人信息安全。

6.1.2 训练数据安全处理

服务提供者应针对训练数据制定安全处理措施，包括：

a) 制定数据分类分级安全处理措施，采取数据脱敏、加密传输、访问控制、边界防护等技术措施保障数据安全；
b) 对安全性标注数据进行隔离安全存储。

6.1.3 训练数据内容安全

服务提供者应制定训练数据内容安全清洗过滤措施，包括：

a) 按照 GB/T 45654-2025 对全部训练数据进行清洗过滤，包括利用关键词、分类模型、人工抽检等去除数据中的违法不良信息；

b) 重点关注公开数据集、网络采集数据以及商业数据的安全性。根据 GB/T 45652-2025 原始数据集中违法不良信息含量不应超过 5%。并对计划采用的训练数据进行清洗和标注，不应采用含有违法不良信息的数据集用于训练；
c) 根据 GB/T 45674-2025 制定标注人员管理规则、数据标注规则、标注质量评价机制及管理流程；
d) 制定安全性标注规则，指导标注人员围绕训练数据及生成内容的主要安全风险进行标注，每一条标注数据至少经由一名审核人员审核通过；
e) 训练学习教育类模型的，宜重点建设具备科学性的高质量训练数据集，充分过滤其中的错误知识内容。

6.2 模型训练阶段

6.2.1 生成内容安全

服务提供者应采取有效技术措施保障模型生成内容安全，包括：
a) 制定未成年人保护评价机制，将生成内容安全性作为评价生成结果优劣的主要指标之一，建议在模型训练过程中引入保护未成年人权益的安全原则，约束模型的输出符合伦理规范、减少偏见等；
b) 通过对模型输出内容识别和过滤，改写或去除有害内容，以确保其输出内容的安全性；
c) 可制定并优化未成年人风险识别机制，充分考虑未成年人心智尚不成熟、辨别能力低、社会经验少等特点，持续挖掘针对未成年人健康成长带来的社会关系紊乱、伦理认知错误、自主意识降低等隐患，并采取有效措施在模型训练过程中降低相应风险。

6.2.2 个人可识别信息保护

服务提供者应采取有效措施防范个人信息泄漏风险，包括：
a) 重点关注模型生成并泄露如个人身份信息、财务信息、医疗信息、社交媒体活动、电子邮件、通信记录、位置数据等未成年人个人可识别信息的风险，并制定相应保护措施，如联邦学习、加密算法、差分隐私、同态加密、安全多方计算等技术措施；
b) 将训练环境与推理环境隔离，避免上述个人信息泄露和不当访问；
c) 制定应急预案，重点规划和部署涉及未成年人上述个人信息泄露事件的监测、发现与应急补救措施。

6.2.3 模型对齐

服务提供者宜持续提升模型对齐能力，保障服务的安全性和可靠性，包括：
a) 建立生成内容监测和优化机制，对提供服务过程中以及定期检测时发现的安全问题，通过针对性地监督微调、强化学习等方式优化模型；
b) 建立人类反馈学习机制，通过让人类对模型的输出进行标注和反馈，帮助模型调整其行为，使其更加符合人类的期望。

6.3 场景应用阶段

6.3.1 服务备案评估

服务提供者应按照国家法律法规和业务服务风险建立安全评估机制，包括：
a) 开展模型更新迭代的安全自评估，建立评估启动——制定评估标准——确定评估方案——评估实施——结果评价——优化整改——监督评价等评估流程；
b) 落实生成式人工智能服务备案要求。具有舆论属性或社会动员能力的、面向境内公众提供的生成式人工智能服务，在服务上线前需通过属地网信部门开展生成式人工智能服务备案，对直接调用已备案模型 API 的，需通过属地网信部门开展备案登记。上线后需在显著位置或服务详情页面标明所取得的上线编号；
c) 落实算法备案要求。在服务上线后的十个工作日内，通过“互联网信息服务算法备案系统”如实填报算法备案信息，包括主体信息、算法信息、技术服务方式、服务功能信息等，备案通过后需在产品显著位置公示算法备案号和备案算法机制原理。

6.3.2 服务内容安全

服务提供者应采取有效技术防护措施和安全管理措施，保障服务内容的安全性、可靠性和真实性，包括：

a) 具备有效识别、拦截违法和不良信息的能力，对危害未成年人身心健康的内容，应当及时采取措施阻断传播路径，并持续优化相关服务；
b) 针对输入输出内容制定安全审核机制，根据业务场景制定符合内容安全需求的审核体系，包括内容分级分类管理机制、审核标准、审核流程等；
c) 根据服务特点和内容生产规模配备相应的安全审核人员，针对涉未成年人专区内容制定专项审核策略。并对审核人员进行安全意识、专业知识等专业培训，制定相应的考核评价机制，以确保人工审核质量和效率；
d) 制定和公开管理规则、平台公约，明确用户/账户使用规范和行为管理规则，以显著方式提示使用者承担信息安全义务，引导和鼓励用户合理使用人工智能技术，分享有价值、正能量、真实可靠的内容和观点，形成积极向上的社区氛围；
e) 做好各类应用场景风险识别、评估与应对工作。关注生成式人工智能通用场景下算法不当利用导致的错误认知或信息不平等风险；生成有害内容传递错误价值观和意识形态扭曲风险；警惕特殊应用场景风险，包括但不限于娱乐场景未成年人沉迷、情感依恋等问题。结合不同场景生成内容诱导或引起未成年人效仿危险行为的风险，并采取预警、风险提示、风险阻断等合理应对措施；
f) 根据相关国家标准进行标识，明确生成合成内容的显式标识及元数据隐式标识形式；
g) 建立投诉、意见反馈渠道，对受理的问题及时处理回复，针对涉未成年人问题总结分析并制定优化策略。

6.3.3 服务数据安全

服务提供者应建立数据全生命周期安全管理规范，包括：

a) 按照相关法律法规要求开展数据分类分级管理、数据安全风险评估等工作；
b) 开展数据处理活动需加强风险监测，发现数据安全缺陷、漏洞等风险时，需采取补救措施；
c) 发生数据安全事件时，需立即采取处置措施，按照法律、行政法规的相关要求，及时告知用户并向有关主管部门报告。

6.3.4 用户个人信息保护

服务提供者在服务过程中应根据 GB/T 35273-2020 建立全方位的用户个人信息保护机制，包括：

a) 按照合法正当、公开透明的原则，公示和告知未成年人个人信息处理目的、处理方式、处理信息种类等；
b) 根据必要性原则，仅收集与提供服务目的直接相关的个人信息；
c) 涉及收集使用不满十四周岁未成年人个人信息的，获得监护人的单独同意；
d) 基于个人同意处理个人信息的，为个人提供撤回同意等服务，并采取匿名化处理、结果屏蔽等方式消除对个人信息的影响。

6.3.5 科技伦理要求

服务提供者宜从以下方面落实科技伦理要求：

a) 以显著方式提示未成年人用户依法享有的网络保护权利和遭受网络侵害的救济途径，具备生成内容标识、信息溯源、取证、及时止损等技术防护能力；
b) 关注科技伦理风险防范，鼓励在未成年人言语感知和理解、言语产出和表达、阅读习得和发展过程中，以最有利于未成年人为原则，避免给未成年人带来认知堕化、偏见歧视、情感错位与意识狭隘等影响；
c) 所开发的应用场景，根据服务定位、服务对象、服务功能、用户规模等充分评估服务中可能存在的涉未成年人科技伦理失范问题，并制定有效保护措施；
d) 监护人教育引导：向家长提供使用指南、授权设定未成年人防沉迷措施，帮助他们理解如何有效管理未成年人的在线活动，确保未成年人在使用过程中得到适当的监督和指导。

6.4 服务运营阶段

6.4.1 未成年人身份认证

服务提供者宜根据服务情况建立合理有效的未成年人身份认证机制，确保未成年人保护措施有效落实。可参照以下方式：

a) 实名认证：依据国家法律法规规定，在用户注册时进行基于手机号、身份证号等真实性身份认证，或基于其他服务触发时，收集用户的身份证件信息进行未成年人身份的识别；
b) 电子身份认证系统：应用于网络游戏服务的，可通过国家建立统一的未成年人网络游戏电子身份认证系统进行认证；
c) 主动验证：注册或登录时主动发起弹窗等提示，通过引导用户输入出生年月、选择年龄段、直接选择是否为未成年人等方式，进行未成年人身份的识别；
d) 其他智能分析识别：在符合未成年人个人信息保护基础上，鼓励提升智能识别未成年人身份的自动化技术能力。

6.4.2 未成年人模式

服务提供者宜根据服务定位和未成年人用户特点设立未成年人模式（参照附录C），包括：

a) 三方联动：移动智能终端、应用程序、应用程序分发平台之间可通过必要接口和数据共享，实现三方联动，提供未成年人模式切换、时间管理、内容管理、权限管理等功能；
b) 便捷使用：提供包括使用时段、时长、内容、功能、举报投诉等便捷化操作设置；
c) 分龄原则：根据不同年龄阶段未成年人身心发展特点和认知能力，评估服务的类型、内容与功能等要素，鼓励加大未成年人内容分龄服务能力建设，在使用时段、时长、内容和功能等方面按照国家有关规定和标准提供相应的服务；向不满八周岁的未成年人提供专用智能设备具备智能语音交互功能的，不宜使用生成式人工智能服务；
d) 强化内容安全：针对未成年人模式下的服务内容建立未成年人专项审核机制，充分评估服务功能、生成内容可能对未成年人身心健康造成的影响，并制定安全防治措施。

6.4.3 网络防沉迷

服务提供者宜根据国家法律法规、行业治理要求等制定未成年人防沉迷机制，包括：

a) 建立健全防沉迷管理机制，如优化算法推荐规则，完善算法推荐标签审核管理，制定多元化内容推荐机制，定期评估推荐效果及对应优化机制，加强沉浸式体验服务时间提示和限制等；
b) 及时修改可能造成未成年人沉迷的内容、功能和规则，并增强防绕过技术能力。

6.4.4 权限管理

在未成年人模式之外的服务，宜从包括但不限于以下方面制定未成年人使用权限管理要求：

a) 开展虚拟主播直播服务需按照网络直播服务管理要求落实保护职责；
b) 针对教育培训类等未成年人专用服务，鼓励开发有利于学习交流的创新性功能，并为监护人提供相应管理权限；
c) 充分评估未成年人使用个人智能体创建、人工智能陪伴等服务的风险，适当限制功能权限。

6.4.5 消费管理

服务提供者宜从包括但不限于以下方面制定未成年人消费管理要求：

a) 网络社交、网络游戏、网络直播、网络音视频、在线教育等场景下的生成式人工智能服务所产生的消费，建议遵从行业管理要求合理限制未成年人消费，不得向未成年人提供与其民事行为能力不符的付费服务；
b) 基于生成式人工智能服务与体验而产生的消费，鼓励服务提供者探索制定并不断完善同未成年人民事能力适配的消费限额规则；
c) 制定并不断完善涉及未成年人消费退款处理规则、流程。

7 组织与制度保障

7.1 工作组织

7.1.1 未成年人保护专项工作组

服务提供者宜设立未成年人保护专项工作组，主要职责包括：

a) 制定平台未成年人保护与发展整体工作目标；
b) 对管理制度的适用性和可操作性进行审定；
c) 对安全管理活动进行授权和审批；
d) 监督和评估保护成效并及时修正和改进；
e) 决策安全管理过程中出现的重要问题；
f) 统筹未成年人保护和社会责任落实相关专项工作等。

7.1.2 安全负责人

服务提供者宜任命未成年人保护专项工作组安全负责人，主要职责包括：

a) 统筹未成年人保护与发展工作规划和管理；
b) 审定各类管理制度、标准、规范、流程等；
c) 决策安全管理过程中出现的重要问题并合理解决；
d) 为落实未成年人保护和发展工作提供资源支持等。

7.2 制度建设

服务提供者宜制定未成年人专项保障制度，包括：

a) 服务提供者宜主动落实主体责任，建立健全未成年人保护和发展制度及工作体系。包括但不限于安全评估制度、内容审核制度、个人信息保护制度、应急处置制度等；
b) 未成年人专项制度在上述安全保护组织或专门负责人员指导下运行，并体现于整体安全管理制度之中，作为重要制度部分贯穿起草、审定、论证和发布、更新修订等主要环节。

8 未成年人发展与促进

8.1 未成年人发展权益保障

服务提供者宜从以下方面保障未成年人发展权益：

a) 研发和应用适合未成年人身心健康发展的生成式人工智能服务；
b) 开展服务合规建设，落实责任制，强化自我监督与社会监督；
c) 践行企业社会责任，参与未成年人人工智能素养培育工作；
d) 与利益相关者协同共治，多途径多层次维护未成年人发展权益。

8.2 人工智能素养提升

服务提供者宜从以下方面提升未成年人人工智能素养：

a) 生成式人工智能企业践行社会责任，在素养模型构建、培育体系设计、测评系统开发、应用数据评价中主动作为，加强未成年人人工智能素养培育工作；
b) 关注弱势群体未成年人发展，适当倾斜资源以弥合因区域和群体发展不平衡导致的智能鸿沟；
c) 开展未成年人人工智能素养普法宣传，促进未成年人形成人工智能场景下自我保护、维护自身权益的意识和水平；
d) 鼓励引入“社区互助机制”，与学校、社区合作，定期举办如“人工智能安全家长课堂”，开发“人工智能风险教育课程”等安全能力普及内容，帮助提升监护人的未成年人保护素养。

8.3 特色化发展和智能终端协同

服务提供者宜从以下方面持续探索未成年人人工智能特色化发展路径：

a) 采取参与式设计和包容性设计，根据服务定位，在适当场合下让未成年人及其监护人参与设计过程；根据不同年龄组未成年人的心智模型与需求，合理设计提示语言、用户界面、生成结果等内容。保障生成式人工智能系统适龄化特点，避免使用服务中造成过度技术依赖和盲目技术崇拜；

b） 建立未成年人适宜的训练数据库，强调自然科学、人文与社会科学等知识数据库扩充，提升算法生成的信息准确性，形成和促进良性信息交互；
c） 鼓励探索智能终端、应用程序和分发平台一体化协同机制，如未成年人模式多平台自动切换、接口和数据共享等模式创新；
d） 加强人工智能风险科普教育，帮助未成年人全面认识生成式人工智能的潜在风险，培养未成年人辨别人工智能生成内容真实性和应对风险的能力，提高其在人工智能场景下的安全意识与判断能力。

8.4 行业治理与协作

行业宜从以下方面开展治理与协作：
a） 探索行业协同自治，建立行业议事机制，针对生成式人工智能技术研发、应用设计、运营等方面的问题和难点，形成未成年人保护策略集；
b） 建立企业安全能力自评估协作机制，行业协会搭建安全评估交流、指导和服务平台，以评促改，及时排查生成式人工智能应用领域涉未成年人安全风险，提升行业安全服务水平；
c） 建设便捷有效的举报平台，通过构建网络、通讯等各种举报渠道，接受社会的技术风险与伦理规范监督，及时纠偏纠错，维护未成年人用户的健康使用环境；
d） 举办跨行业合作交流活动，推进多元主体共建共治共享，建立面向未成年人的治理合作平台，为生成式人工智能服务未成年人保护和发展提供更广泛的支持。

附 录 A
（规范性）
未成年人服务安全要求

A.1 内容安全要求

面向未成年人的生成式人工智能服务需生成有利于未成年人健康成长的内容，不得生成和传播危害未成年人身心健康的内容。包括：

a) 鼓励和支持生成弘扬社会主义核心价值观和社会主义先进文化、革命文化、中华优秀传统文化，铸牢中华民族共同体意识，培养未成年人家国情怀和良好品德，引导未成年人养成良好生活习惯和行为习惯等的信息；
b) 不得生成含有宣扬淫秽、色情、暴力、邪教、迷信、赌博、引诱自残自杀、恐怖主义、分裂主义、极端主义等危害未成年人身心健康内容的信息；
c) 不得生成对未成年人实施侮辱、诽谤、威胁或者恶意损害形象等网络欺凌内容，不得生成为组织、教唆、胁迫、引诱、欺骗、帮助未成年人实施违法犯罪提供方法、教程等的信息；
d) 不得生成影响未成年人性心理健康的内容，包括通过传播淫秽色情、低俗挑逗等信息，影响未成年人性心理、性道德和性观念扭曲等；
e) 不得生成涉未成年人网络欺诈的内容，包括利用未成年人的猎奇心理以及不成熟的认知辨别能力等，对未成年人实施诈骗，或诱导未成年人对他人进行诈骗；
f) 不得生成侵害未成年人权益的内容，包括泄露未成年人的个人信息、制造未成年人谣言等影响未成年人精神状态或现实生活的内容；
g) 生成含有可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等可能影响未成年人身心健康的信息，应当在信息展示前予以显著提示；
h) 涉及学科知识、常识等生成内容的，可采取有效措施增强其准确性、可靠性；
i) 不得生成其他危害未成年人身心健康的内容。

A.2 数据安全要求

面向未成年人的生成式人工智能服务宜履行数据安全保护义务，保障未成年人使用生成式人工智能服务的数据安全。包括：

a) 按照数据安全管理相关法律法规要求制定数据安全保障措施，包括数据分类分级管理、数据风险监测、风险评估、应急演练等机制；
b) 不得违规收集使用未成年人用户数据，在训练数据获取、提供服务与用户交互过程中，不得未经同意收集、不当使用未成年人数据；
c) 不得使用标注不规范、未经清洗或清洗效果较差的未成年人数据，防止数据投毒、模型污染导致生成有害和不良内容；
d) 不得违规开展未成年人数据处理活动，如通过诱导、欺骗、胁迫等方式处理其在平台上产生的网络数据；
e) 不得将未成年人数据置于危险环境，包括无数据系统技术防护或者技术防护能力薄弱，数据超期存储，访问授权管理不合理，数据传输、共享操作不规范等可能导致数据泄漏风险；
f) 不得违规开展数据跨境传输活动，包括训练数据集违规跨境存储、传输、提供、共享，违规向境外提供人工智能服务等；
g) 其他数据收集、存储、使用、加工、传输、提供、公开、删除等环节安全风险防范。

A.3 个人信息保护要求

面向未成年人的生成式人工智能服务需加强未成年人个人信息保护，重点关注生成式人工智能在模型训练和实际提供服务中采集或者接收的未成年人个人信息。包括：

a) 以“最小必要、目的明确、告知同意、公开透明、权责一致、确保安全、事后可查 ”为原则，设计并实施覆盖生成式人工智能个人信息处理活动全生命周期的安全保护策略，以保护个人信息；

b) 不得收集非必要个人信息，不得非法留存能够识别使用者身份的输入信息和使用记录，不得非法向他人提供使用者的输入信息和使用记录；
c) 不得强制要求未成年人或者其监护人同意非必要的个人信息处理行为，不得因为未成年人或者其监护人不同意处理未成年人非必要个人信息或者撤回同意，拒绝未成年人使用其基本功能服务；
d) 处理不满十四周岁未成年人个人信息的，服务提供者应当制定专门的个人信息处理规则，并取得未成年人的父母或者其他监护人的同意；
e) 在服务中发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，需及时提示，并采取停止传输等必要保护措施；
f) 为未成年人或者其监护人提供查阅、复制、更正、补充、删除、转移未成年人个人信息的方法，不得拒绝其合理请求或设置不合理条件进行限制；
g) 不得超范围、超频采集未成年人个人信息，不得未经授权违规使用未成年人个人信息；
h) 发生未成年人个人信息泄露、篡改、丢失时，不得隐瞒不报或漏报；
i) 不得制定晦涩难懂、关键条款模糊化的个人信息处理规则，不得以默认授权或隐式授权的方式获得信息收集权限；
j) 国家法律法规及强制性标准规定的其他未成年人个人信息保护要求。

附 录 B
（资料性）
法律法规及部门规章依据

B.1 内容安全

主要法律法规、部门规章	重点条款
《中华人民共和国网络安全法》	**第十二条** 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。 任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。 **第四十七条** 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。
《中华人民共和国未成年人保护法》	**第六十五条** 国家鼓励和支持有利于未成年人健康成长的网络内容的创作与传播，鼓励和支持专门以未成年人为服务对象、适合未成年人身心健康特点的网络技术、产品、服务的研发、生产和使用。 **第八十条** 网络服务提供者发现用户发布、传播可能影响未成年人身心健康的信息且未作显著提示的，应当作出提示或者通知用户予以提示；未作出提示的，不得传输相关信息。 网络服务提供者发现用户发布、传播含有危害未成年人身心健康内容的信息的，应当立即停止传输相关信息，采取删除、屏蔽、断开链接等处置措施，保存有关记录，并向网信、公安等部门报告。 网络服务提供者发现用户利用其网络服务对未成年人实施违法犯罪行为的，应当立即停止向该用户提供网络服务，保存有关记录，并向公安机关报告。
《未成年人网络保护条例》	**第二十二条** 任何组织和个人不得制作、复制、发布、传播含有宣扬淫秽、色情、暴力、邪教、迷信、赌博、引诱自残自杀、恐怖主义、分裂主义、极端主义等危害未成年人身心健康内容的网络信息。 任何组织和个人不得制作、复制、发布、传播或者持有有关未成年人的淫秽色情网络信息。 **第二十三条** 网络产品和服务中含有可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等可能影响未成年人身心健康的信息的，制作、复制、发布、传播该信息的组织和个人应当在信息展示前予以显著提示。 国家网信部门会同国家新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、广播电视等部门，在前款规定基础上确定可能影响未成年人身心健康的信息的具体种类、范围、判断标准和提示办法。 **第二十四条** 任何组织和个人不得在专门以未成年人为服务对象的网络产品和服务中制作、复制、发布、传播本条例第二十三条第一款规定的可能影响未成年人身心健康的信息。 网络产品和服务提供者不得在首页首屏、弹窗、热搜等处于产品或者服务醒目位置、易引起用户关注的重点环节呈现本条例第二十三条第一款规定的可能影响未成年人身心健康的信息。 网络产品和服务提供者不得通过自动化决策方式向未成年人进行商业营销。 **第二十五条** 任何组织和个人不得向未成年人发送、推送或者诱骗、强

	迫未成年人接触含有危害或者可能影响未成年人身心健康内容的网络信息。 **第二十六条** 任何组织和个人不得通过网络以文字、图片、音视频等形式，对未成年人实施侮辱、诽谤、威胁或者恶意损害形象等网络欺凌行为。 网络产品和服务提供者应当建立健全网络欺凌行为的预警预防、识别监测和处置机制，设置便利未成年人及其监护人保存遭受网络欺凌记录、行使通知权利的功能、渠道，提供便利未成年人设置屏蔽陌生用户、本人发布信息可见范围、禁止转载或者评论本人发布信息、禁止向本人发送信息等网络欺凌信息防护选项。 网络产品和服务提供者应当建立健全网络欺凌信息特征库，优化相关算法模型，采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测。 **第二十七条** 任何组织和个人不得通过网络以文字、图片、音视频等形式，组织、教唆、胁迫、引诱、欺骗、帮助未成年人实施违法犯罪行为。 **第二十八条** 以未成年人为服务对象的在线教育网络产品和服务提供者，应当按照法律、行政法规和国家有关规定，根据不同年龄阶段未成年人身心发展特点和认知能力提供相应的产品和服务。
《生成式人工智能服务管理暂行办法》	**第四条** 提供和使用生成式人工智能服务，应当遵守法律、行政法规，尊重社会公德和伦理道德，遵守以下规定： （一）坚持社会主义核心价值观，不得生成煽动颠覆国家政权、推翻社会主义制度，危害国家安全和利益、损害国家形象，煽动分裂国家、破坏国家统一和社会稳定，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，暴力、淫秽色情，以及虚假有害信息等法律、行政法规禁止的内容； （二）在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视； （三）尊重知识产权、商业道德，保守商业秘密，不得利用算法、数据、平台等优势，实施垄断和不正当竞争行为； （四）尊重他人合法权益，不得危害他人身心健康，不得侵害他人肖像权、名誉权、荣誉权、隐私权和个人信息权益； （五）基于服务类型特点，采取有效措施，提升生成式人工智能服务的透明度，提高生成内容的准确性和可靠性。
《互联网信息服务管理办法》	**第十五条** 互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息： （一）反对宪法所确定的基本原则的； （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的； （三）损害国家荣誉和利益的； （四）煽动民族仇恨、民族歧视，破坏民族团结的； （五）破坏国家宗教政策，宣扬邪教和封建迷信的； （六）散布谣言，扰乱社会秩序，破坏社会稳定的； （七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的； （八）侮辱或者诽谤他人，侵害他人合法权益的； （九）含有法律、行政法规禁止的其他内容的。 **第十六条** 互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。
《网络暴力信息治理规定》	**第七条** 网络信息服务提供者应当履行网络信息内容管理主体责任，建立完善网络暴力信息治理机制，健全用户注册、账号管理、个人信息保护、信息发布审核、监测预警、识别处置等制度。 **第十条** 任何组织和个人不得制作、复制、发布、传播涉网络暴力违法信息，应当防范和抵制制作、复制、发布、传播涉网络暴力不良信息。 任何组织和个人不得利用网络暴力事件实施蹭炒热度、推广引流等营销炒作行为，不得通过批量注册或者操纵用户账号等形式组织制作、复制、发布、传播网络暴力信息。 明知他人从事涉网络暴力信息违法犯罪活动的，任何组织和个人不得为其提供数据、技术、流量、资金等支持和协助。 **第二十四条** 网络信息服务提供者发现用户面临网络暴力信息风险的，应当及时通过显著方式提示用户，告知用户可以采取的防护措施。

	网络信息服务提供者发现网络暴力信息风险涉及以下情形的，还应当为用户提供网络暴力信息防护指导和保护救助服务，协助启动防护措施，并向网信、公安等有关部门报告： （一）网络暴力信息侵害未成年人、老年人、残疾人等用户合法权益的； （二）网络暴力信息侵犯用户个人隐私的； （三）若不及时采取措施，可能造成用户人身、财产损害等严重后果的其他情形。 **第二十七条** 网络信息服务提供者应当优先处理涉未成年人网络暴力信息的投诉、举报。发现涉及侵害未成年人用户合法权益的网络暴力信息风险的，应当按照法律法规和本规定要求及时采取措施，提供相应保护救助服务，并向有关部门报告。 网络信息服务提供者应当设置便利未成年人及其监护人行使通知删除网络暴力信息权利的功能、渠道，接到相关通知后，应当及时采取删除、屏蔽、断开链接等必要的措施，防止信息扩散。
《互联网信息服务深度合成管理规定》	**第六条** 鼓励生成式人工智能算法、框架、芯片及配套软件平台等基础技术的自主创新，平等互利开展国际交流与合作，参与生成式人工智能相关国际规则制定。 推动生成式人工智能基础设施和公共训练数据资源平台建设。促进算力资源协同共享，提升算力资源利用效能。推动公共数据分类分级有序开放，扩展高质量的公共训练数据资源。鼓励采用安全可信的芯片、软件、工具、算力和数据资源。 **第七条** 生成式人工智能服务提供者（以下称提供者）应当依法开展预训练、优化训练等训练数据处理活动，遵守以下规定： （一）使用具有合法来源的数据和基础模型； （二）涉及知识产权的，不得侵害他人依法享有的知识产权； （三）涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形； （四）采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性； （五）《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律、行政法规的其他有关规定和有关主管部门的相关监管要求。
《网络信息内容生态治理规定》	**第五条** 鼓励网络信息内容生产者制作、复制、发布含有下列内容的信息： （一）宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的； （二）宣传党的理论路线方针政策和中央重大决策部署的； （三）展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的； （四）弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的； （五）有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的； （六）有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的； （七）其他讲品味讲格调讲责任、讴歌真善美、促进团结稳定等的内容。 **第六条** 网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息： （一）反对宪法所确定的基本原则的； （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的； （三）损害国家荣誉和利益的； （四）歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的； （五）宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的； （六）煽动民族仇恨、民族歧视，破坏民族团结的； （七）破坏国家宗教政策，宣扬邪教和封建迷信的； （八）散布谣言，扰乱经济秩序和社会秩序的；

	（九）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的； （十）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的； （十一）法律、行政法规禁止的其他内容。 **第七条** 网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息： （一）使用夸张标题，内容与标题严重不符的； （二）炒作绯闻、丑闻、劣迹等的； （三）不当评述自然灾害、重大事故等灾难的； （四）带有性暗示、性挑逗等易使人产生性联想的； （五）展现血腥、惊悚、残忍等致人身心不适的； （六）煽动人群歧视、地域歧视等的； （七）宣扬低俗、庸俗、媚俗内容的； （八）可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的； （九）其他对网络生态造成不良影响的内容。 **第十二条** 网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当设置符合本规定第十条、第十一条规定要求的推荐模型，建立健全人工干预和用户自主选择机制。 **第十三条** 鼓励网络信息内容服务平台开发适合未成年人使用的模式，提供适合未成年人使用的网络产品和服务，便利未成年人获取有益身心健康的信息。 **第十四条** 网络信息内容服务平台应当加强对本平台设置的广告位和在本平台展示的广告内容的审核巡查，对发布违法广告的，应当依法予以处理。 **第十五条** 网络信息内容服务平台应当制定并公开管理规则和平台公约，完善用户协议，明确用户相关权利义务，并依法依约履行相应管理职责。 网络信息内容服务平台应当建立用户账号信用管理制度，根据用户账号的信用情况提供相应服务。 **第十六条** 网络信息内容服务平台应当在显著位置设置便捷的投诉举报入口，公布投诉举报方式，及时受理处置公众投诉举报并反馈处理结果。 **第十七条** 网络信息内容服务平台应当编制网络信息内容生态治理工作年度报告，年度报告应当包括网络信息内容生态治理工作情况、网络信息内容生态治理负责人履职情况、社会评价情况等内容。
《互联网信息服务算法推荐管理规定》	**第六条** 算法推荐服务提供者应当坚持主流价值导向，优化算法推荐服务机制，积极传播正能量，促进算法应用向上向善。 算法推荐服务提供者不得利用算法推荐服务从事危害国家安全和社会公共利益、扰乱经济秩序和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动，不得利用算法推荐服务传播法律、行政法规禁止的信息，应当采取措施防范和抵制传播不良信息。 **第七条** 算法推荐服务提供者应当落实算法安全主体责任，建立健全算法机制机理审核、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、反电信网络诈骗、安全评估监测、安全事件应急处置等管理制度和技术措施，制定并公开算法推荐服务相关规则，配备与算法推荐服务规模相适应的专业人员和技术支撑。 **第十八条** 算法推荐服务提供者向未成年人提供服务的，应当依法履行未成年人网络保护义务，并通过开发适合未成年人使用的模式、提供适合未成年人特点的服务等方式，便利未成年人获取有益身心健康的信息。 算法推荐服务提供者不得向未成年人推送可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等可能影响未成年人身心健康的信息，不得利用算法推荐服务诱导未成年人沉迷网络。

B.2 数据安全

主要法律法规、部门规章	重点条款
《中华人民共和国网络安全法》	**第二十七条** 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事

	侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。 **第四十条** 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。 **第四十一条** 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。 **第四十二条** 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 **第四十三条** 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。 **第四十四条** 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。
《中华人民共和国数据安全法》	**第二十七条** 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。 **第二十八条** 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。 **第二十九条** 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。 **第三十条** 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。 风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。
《网络数据安全管理条例》	**第十九条** 提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。 **第二十九条** 国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的网络数据进行重点保护。 网络数据处理者应当按照国家有关规定识别、申报重要数据。对确认为重要数据的，相关地区、部门应当及时向网络数据处理者告知或者公开发布。网络数据处理者应当履行网络数据安全保护责任。 国家鼓励网络数据处理者使用数据标签标识等技术和产品，提高重要数据安全管理水平。 **第三十条** 重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任： （一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案； （二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；

	（三）受理并处理网络数据安全投诉、举报。 网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。 掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。 **第四十条** 网络平台服务提供者应当通过平台规则或者合同等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。 预装应用程序的智能终端等设备生产者，适用前款规定。 第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。 国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保。 **第四十六条** 大型网络平台服务提供者不得利用网络数据、算法以及平台规则等从事下列活动： （一）通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据； （二）无正当理由限制用户访问、使用其在平台上产生的网络数据； （三）对用户实施不合理的差别待遇，损害用户合法权益； （四）法律、行政法规禁止的其他活动。

B.3 个人信息保护

主要法律法规、部门规章	重点条款
《中华人民共和国网络安全法》	**第四十一条** 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。 **第四十二条** 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 **第四十三条** 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。 **第四十四条** 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。
《中华人民共和国个人信息保护法》	**第二章 个人信息处理规则** **第一节 一般规定** **第十三条** 符合下列情形之一的，个人信息处理者方可处理个人信息： （一）取得个人的同意； （二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需； （三）为履行法定职责或者法定义务所必需； （四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需； （五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

	（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息； （七）法律、行政法规规定的其他情形。 依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。 **第十四条** 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。 **第十五条** 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。 个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。 **第十六条** 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。 **第十七条** 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项： （一）个人信息处理者的名称或者姓名和联系方式； （二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； （三）个人行使本法规定权利的方式和程序； （四）法律、行政法规规定应当告知的其他事项。 前款规定事项发生变更的，应当将变更部分告知个人。 个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。 **第十八条** 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。 紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。 **第十九条** 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。 **第二十条** 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。 个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。 **第二十一条** 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。 受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。 未经个人信息处理者同意，受托人不得转委托他人处理个人信息。 **第二十二条** 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。 **第二十三条** 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。 **第二十四条** 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。 通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

	第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。 **第二十六条** 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。 **第二十七条** 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。 **第二节 敏感个人信息的处理规则** **第二十八条** 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。 **第二十九条** 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。 **第三十条** 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。 **第三十一条** 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。 个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。 **第三十二条** 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。 **第三节 国家机关处理个人信息的特别规定** **第三十三条** 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。 **第三十四条** 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。 **第三十五条** 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。 **第三十六条** 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。 **第三十七条** 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。 **第三章 个人信息跨境提供的规则** **第三十八条** 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一： （一）依照本法第四十条的规定通过国家网信部门组织的安全评估； （二）按照国家网信部门的规定经专业机构进行个人信息保护认证； （三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务； （四）法律、行政法规或者国家网信部门规定的其他条件。 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。 个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。 **第三十九条** 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。 **第四十条** 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。

	确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。 **第四十一条** 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。 **第四十二条** 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。 **第四十三条** 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。 **第五章 个人信息处理者的义务** **第五十一条** 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； （五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。 **第五十二条** 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。 个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。 **第五十三条** 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。 **第五十四条** 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。 **第五十五条** 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录： （一）处理敏感个人信息； （二）利用个人信息进行自动化决策； （三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息； （四）向境外提供个人信息； （五）其他对个人权益有重大影响的个人信息处理活动。 **第五十六条** 个人信息保护影响评估应当包括下列内容： （一）个人信息的处理目的、处理方式等是否合法、正当、必要； （二）对个人权益的影响及安全风险； （三）所采取的保护措施是否合法、有效并与风险程度相适应。 个人信息保护影响评估报告和处理情况记录应当至少保存三年。 **第五十七条** 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项： （一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害； （二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施； （三）个人信息处理者的联系方式。 个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

	第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务： （一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督； （二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务； （三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务； （四）定期发布个人信息保护社会责任报告，接受社会监督。 **第五十九条** 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。
《中华人民共和国未成年人保护法》	**第七十二条** 信息处理者通过网络处理未成年人个人信息的，应当遵循合法、正当和必要的原则。处理不满十四周岁未成年人个人信息的，应当征得未成年人的父母或者其他监护人同意，但法律、行政法规另有规定的除外。 未成年人、父母或者其他监护人要求信息处理者更正、删除未成年人个人信息的，信息处理者应当及时采取措施予以更正、删除，但法律、行政法规另有规定的除外。 **第七十三条** 网络服务提供者发现未成年人通过网络发布私密信息的，应当及时提示，并采取必要的保护措施。
《未成年人网络保护条例》	**第四章 个人信息网络保护** **第三十一条** 网络服务提供者为未成年人提供信息发布、即时通讯等服务的，应当依法要求未成年人或者其监护人提供未成年人真实身份信息。未成年人或者其监护人不提供未成年人真实身份信息的，网络服务提供者不得为未成年人提供相关服务。 网络直播服务提供者应当建立网络直播发布者真实身份信息动态核验机制，不得向不符合法律规定情形的未成年人用户提供网络直播发布服务。 **第三十二条** 个人信息处理者应当严格遵守国家网信部门和有关部门关于网络产品和服务必要个人信息范围的规定，不得强制要求未成年人或者其监护人同意非必要的个人信息处理行为，不得因为未成年人或者其监护人不同意处理未成年人非必要个人信息或者撤回同意，拒绝未成年人使用其基本功能服务。 **第三十三条** 未成年人的监护人应当教育引导未成年人增强个人信息保护意识和能力、掌握个人信息范围、了解个人信息安全风险，指导未成年人行使其在个人信息处理活动中的查阅、复制、更正、补充、删除等权利，保护未成年人个人信息权益。 **第三十四条** 未成年人或者其监护人依法请求查阅、复制、更正、补充、删除未成年人个人信息的，个人信息处理者应当遵守以下规定： （一）提供便捷的支持未成年人或者其监护人查阅未成年人个人信息种类、数量等的方法和途径，不得对未成年人或者其监护人的合理请求进行限制； （二）提供便捷的支持未成年人或者其监护人复制、更正、补充、删除未成年人个人信息的功能，不得设置不合理条件； （三）及时受理并处理未成年人或者其监护人查阅、复制、更正、补充、删除未成年人个人信息的申请，拒绝未成年人或者其监护人行使权利的请求的，应当书面告知申请人并说明理由。 对未成年人或者其监护人依法提出的转移未成年人个人信息的请求，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。 **第三十五条** 发生或者可能发生未成年人个人信息泄露、篡改、丢失的，个人信息处理者应当立即启动个人信息安全事件应急预案，采取补救措施，及时向网信等部门报告，并按照国家有关规定将事件情况以邮件、信函、电话、信息推送等方式告知受影响的未成年人及其监护人。 个人信息处理者难以逐一告知的，应当采取合理、有效的方式及时发布相关警示信息，法律、行政法规另有规定的除外。 **第三十六条** 个人信息处理者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制未成年人个人信息知悉范围。工作人员访问未成年人个人信息的，应当经过相关负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法处理未成年人个人信息。 **第三十七条** 个人信息处理者应当自行或者委托专业机构每年对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。 **第三十八条** 网络服务提供者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示，并采取停止传输等必要保护措施，防止

	信息扩散。 网络服务提供者通过未成年人私密信息发现未成年人可能遭受侵害的，应当立即采取必要措施保存有关记录，并向公安机关报告。
《儿童个人信息网络保护规定》	**第七条** 网络运营者收集、存储、使用、转移、披露儿童个人信息的，应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。 **第八条** 网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。 **第九条** 网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意。 **第十条** 网络运营者征得同意时，应当同时提供拒绝选项，并明确告知以下事项： （一）收集、存储、使用、转移、披露儿童个人信息的目的、方式和范围； （二）儿童个人信息存储的地点、期限和到期后的处理方式； （三）儿童个人信息的安全保障措施； （四）拒绝的后果； （五）投诉、举报的渠道和方式； （六）更正、删除儿童个人信息的途径和方法； （七）其他应当告知的事项。 前款规定的告知事项发生实质性变化的，应当再次征得儿童监护人的同意。 **第十一条** 网络运营者不得收集与其提供的服务无关的儿童个人信息，不得违反法律、行政法规的规定和双方的约定收集儿童个人信息。 **第十二条** 网络运营者存储儿童个人信息，不得超过实现其收集、使用目的所必需的期限。

附 录 C
（资料性）
未成年人模式建设指南

移动智能终端、移动应用程序、移动应用程序分发平台可参照《移动互联网未成年人模式建设指南》建设未成年人模式，本文件梳理建设要点如下：

服务提供者	未成年人模式要求	内容
移动智能终端	模式入口	最简化原则： ① 入口应当在醒目位置、便捷易寻，方便用户一键切换； ② 提供开机提醒、桌面图标、系统设置等至少 3 种方式； ③ 首次开机或系统设置用户选择不需要未成年人模式，不再出现相关提醒。
	模式退出	① 家长验证同意； ② 提供密码、指纹、人脸等单一或复合验证方式。
	时长管理	差异化使用时长管理服务： ① 不满 16 周岁默认推荐使用总时长不超过 1 小时+家长豁免操作； ② 16 周岁以上不满 18 周岁默认推荐使用时长不超过 2 小时+家长豁免操作； ③ 连续使用超 30 分钟发出休息提醒； ④ 每日 22 时至次日 6 时期间默认不向未成年人提供服务+家长豁免； ⑤ 基本通信、教育等特定必要应用程序和家长自定义豁免的应用程序不受时长和时间段限制。 时间管理功能： ⑥ 整机使用时长可管理； ⑦ 整机使用时间段可管理； ⑧ 指定应用程序使用时间可管理。
	防绕过	① 退出或恢复出厂设置需家长验证并确认； ② 桌面图标位置醒目，不被卸载、冻结、隐藏、强制结束； ③ 无法修改系统日期和时间。
移动应用程序	内容分龄	① 根据年龄区间（3/8/12/16/18）分龄推荐适龄优质内容； ② 鼓励专属内容池中内容适龄推荐标注。
	内容安全	见附录 A.1
	功能限制	① 使用时段、时长、内容和功能按规定和标准提供分龄内容服务； ② 不得提供诱导沉迷的产品和服务，及时修改易沉迷部分； ③ 未成年在线教育网络产品和服务不得插入网络游戏链接、不得推送与教学无关的信息； ④ 必要措施防范外链信息内容风险； ⑤ 默认关闭陌生人私信功能，便捷防护选项。
移动应用程序分发平台	未成年人专区	① 应用程序适龄提示； ② 鼓励上架教育、益智、科普、读书、音乐、体育等有益未成年人身心健康的程序。
	应用程序管理	① 科学评估应用程序适龄范围，并在显著位置标注应用程序推荐年龄； ② 完善上架审核、日常管理、应急处置等管理措施。