人工智能示范法 4.0

中国社会科学院“人工智能安全治理研究”实验室孵化专项资助项目成果

2026 年 5 月 31 日

首席专家

李洪雷 中国社会科学院法学研究所国际法研究所联合党委书记、研究员

起草组组长：

周　辉　中国社会科学院法学研究所网络与信息法研究室副主任（主持工作）

李延枫　中国社会科学院信息情报研究院第八编研室主任、编审

起草组专家（按姓氏拼音排序）：

曹艳林　中国医学科学院医学信息研究所医疗卫生法制室主任、研究员

陈天昊　清华大学公共管理学院长聘副教授

狄行思　广州大学法学院讲师、广州大学粤港澳大湾区法制研究中心特聘研究员

冯子轩　西南政法大学数字法治政府研究院执行院长、教授

傅宏宇　阿里研究院人工智能治理中心主任

郭江兰　中国人民公安大学法学院讲师

韩　键　广州小鹏汽车科技有限公司法务总监

何　波　中国互联网协会互联网法治工作委员会副秘书长

何晶晶　中国社会科学院法学研究所科技与法研究中心主任、国际法所副研究员

呼娜英　中国信通院人工智能研究所安全治理部副主任

金　晶　中国政法大学民商经济法学院教授

金　耀　宁波大学法学院副教授

李　霞　中国社会科学院法学研究所宪法与行政法研究室主任、研究员

李晶晶　暨南大学学报编辑部副主编、副编审，《暨南学报》副主编

李学尧　上海交通大学凯原法学院长聘教授、法律与认知智能实验室主任

林北征　广州互联网法院二级法官

刘灿华　中国社会科学院法学研究所助理研究员

齐英程　吉林大学法学院副教授、吉林大学司法数据应用中心研究员

苏　宇　中国人民公安大学法学院教授、数据法学研究院院长

苏和生　中国社会科学院法学研究所助理研究员

孙牧原　中国信息通信研究院政策与经济研究所工程师

孙南翔　中国社会科学院国际法研究所国际经济法研究室副主任（主持工作）、副研究员

谭观福　中国社会科学院国际法研究所副编审

唐林垚　中国社会科学院法学研究所副研究员

王　俊　21 世纪经济报道商业秩序工作室负责人

王　磊　北京理工大学智能科技法律研究中心研究员

王　伟　同济大学法学院助理教授、上海市人工智能社会治理协同创新中心研究员

王　翔　ISO 行政、商业、产业中流程和数据标准化技术委员会委员

王　玥　西安交通大学法学院教授

王智飞　人力资源和社会保障部信息中心正高级工程师

王新锐　北京市律师协会数字经济与人工智能领域专业委员会副主任

吴　涵　中国互联网协会法治工作委员会副秘书长

萧　鑫　中国社会科学院法学研究所副研究员、中国社会科学院法学研究所私法研究中心副秘书长

肖尤丹　中国科学院科技战略咨询研究院研究员

谢惠加　华南理工大学法学院（知识产权学院）副院长、教授

徐玖玖　中国社会科学院法学研究所助理研究员

闫文光　中国人民公安大学警体战训学院讲师

杨　帆　厦门大学法学院副教授、网络空间国际法研究中心副主任

姚志伟　广东财经大学法学院教授、人工智能法研究中心主任

袁　康　武汉大学法学院教授、武汉大学网络治理研究院副院长

袁　玥　美团南部大区高级法务总监

张　敏　西北工业大学马克思主义学院教授、陕西省法学会人工智能与大数据法学研究会会长

张　嵩　昆仑数智科技有限责任公司高级工程师

张　欣　对外经济贸易大学法学院副院长、教授

张心宇　北京理工大学数智化风险法律防控工信部重点实验室研究员

张　龑　中国人民大学法学院教授

张吉豫　中国人民大学法学院教授、未来法治研究院执行院长

赵景琛　广东财经大学法学院院长

朱　悦　同济大学法学院助理教授、上海市人工智能社会治理协同创新中心研究员

朱玲凤　美团数据和隐私保护法务负责人

朱凌云　杭州市市场监督管理局网络交易监督管理处干部

专家组其他成员（按姓氏拼音排序）：

蔡星月　北京航空航天大学法学院副教授

戴　昕　北京大学法学院副院长、长聘副教授、数字法治研究中心副主任

洪延青　北京理工大学法学院教授、网络空间国际治理研究基地主任

胡萧力　厦门大学法学院副教授

金明子　延边大学法学院讲师

李广德　中国人民大学法学院副教授、法律科技与社会治理实验室执行副主任、研究员

刘　晗　清华大学法学院教授、副院长，清华大学国际争端解决研究院院长

刘　权　中央财经大学数字经济与法治研究中心执行主任、法学院副院长、教授

马　兰　奇安信科技集团首席法律顾问

苏苗罕　同济大学法学院副教授，上海市人工智能社会治理协同创新中心研究员

汪庆华　北京师范大学法学院数字法学研究中心主任、教授

王　静　北京师范大学法学院宪法与行政法学教研中心主任、副教授

王　竹　四川大学法学院教授、四川智慧社会智能治理重点实验室主任

王禄生　东南大学社会科学处处长、法学院教授

王燕玲　华南师范大学法学院教授，博士生导师；广东省人工智能法律应用重点实验室主任；小包公.法律 AI 创始人

吴　凡　联想集团法务执行总监（中国区法律合规负责人）

谢鸿飞　中国社会科学院法学研究所研究员

徐　钢　同济大学法学院副院长、副教授，上海市人工智能社会治理协同创新中心秘书长

姚　佳　中国社会科学院法学研究所编审、《环球法律评论》编辑部主任

张　亮　宁波大学法学院教授

张　红　北京师范大学法学院教授、中国法学会行政法学研究会副秘书长

张韬略　同济大学法学院教授，上海市人工智能社会治理协同创新中心研究员

张效羽　中央党校（国家行政学院）政治和法律教研部宪法与行政法教研室主任、教授

赵淑钰　中国信通院互联网法律研究中心主任工程师

朱宝丽　山东建筑大学法学院院长

起草组秘书：

魏日升　中国社会科学院大学法学院硕士研究生

龚展业　中国社会科学院大学法学院硕士研究生

前言

《人工智能示范法 4.0》（以下简称“示范法”）是由中国社会科学院“人工智能安全治理研究”实验室孵化专项资助项目组在广泛调研、国际比较和产业交流基础上形成的学术性立法参考文献，旨在为全球范围内人工智能立法提供制度思路、规范模型和对话基础。

示范法不代表任何国家机关的正式立场，具有开放性、迭代性和理想性。其所设计的主管机关设置、负面清单、人工智能特区等制度，是探索性理论设想，供立法者与学术界讨论参考。

读者在理解示范法时，可将其视为推动法治共识形成的过程性成果，而非最终的政策建议。

示范法的起草和讨论，除了得到中国社会科学院文化法制研究中心、中国社会科学院法学研究所网络与信息法研究室、中国社会科学院大学法学院的坚实保障外，还得到了以下单位的大力支持（以下按单位名称首字拼音排序）：

北京理工大学网络空间国际治理研究基地

北京理工大学智能科技法律研究中心

北京师范大学法学院数字法学研究中心

北京师范大学法学院宪法与行政法学教研中心

电子科技大学人文社科高等研究院

东南大学法学院

“法学学术前沿”微信公众号

广东财经大学法学院

广东财经大学人工智能法研究中心

广州市法学会粤港澳大湾区互联网法治研究中心

华南理工大学法学院（知识产权学院）

吉林大学司法数据应用研究中心

暨南大学学报编辑部

密码法治实践创新基地

“那一片数据星辰”微信公众号

南方财经全媒体集团

清华大学国际争端解决研究院

清华大学科技发展与治理研究中心

陕西省法学会人工智能与大数据法学研究会

上海交通大学凯原法学院、法律与认知智能实验室

四川智慧社会智能治理重点实验室

同济大学法学院、上海市人工智能社会治理协同创新中心

武汉大学网络治理研究院

西交苏州信息安全法学所

西南政法大学数字法治政府研究院

延边大学法学院

中国互联网协会互联网法治工作委员会

中国人工智能产业发展联盟安全治理委员会

中国人民公安大学数据法学研究院

中国信息通信研究院人工智能研究所

中国医学科学院医学信息研究所医疗卫生法制室

中央财经大学法学院

中央财经大学数字经济与法治研究中心

目　录

第一章 总则

第一条（立法依据）为了促进人工智能发展，规范人工智能的研发、提供和使用活动，维护国家主权、安全与发展利益，保护个人、组织的合法权益，根据宪法，制定本法。

第二条（适用范围）在中华人民共和国境内从事人工智能的研发、提供和使用活动及其监管，适用本法。

在中华人民共和国境外从事人工智能的研发、提供和使用活动，影响或者可能影响中华人民共和国国家安全、公共利益或者个人、组织合法权益的，适用本法。

第三条（治理原则）国家统筹发展和安全，坚持促进创新和依法治理相结合，实施包容审慎监管。

第四条（以人为本原则）从事人工智能研发、提供和使用活动应当以人为本、智能向善，确保人类能够监督和控制人工智能，始终以增进人类福祉为最终目标。

第五条（安全原则）从事人工智能研发、提供和使用活动，应当采取必要措施保障所研发、提供和使用的人工智能及相关网络与数据的安全。

第六条（公开透明可解释原则）从事人工智能提供活动应当遵循公开原则，对所提供的人工智能生成内容予以适当标注。

从事人工智能研发、提供活动应当遵循透明、可解释原则，采取必要措施对所研发、提供的人工智能的目的、原理和效果予以说明。

第七条（可问责原则）从事人工智能研发、提供和使用活动，应当分别对其研发、提供和使用活动负责。

第八条（公平平等原则）从事人工智能研发、提供和使用活动应当遵循公平原

则，采取有效措施避免对个人、组织实行不合理的差别待遇。

从事人工智能研发、提供和使用活动应当充分考虑未成年人、老年人、残疾人等群体的需求。

第九条（绿色原则）国家鼓励在人工智能研发、提供和使用活动中应用节能减排技术，促进绿色智慧的数字生态文明建设。

第十条（促进发展创新原则）国家支持人工智能基础设施建设，推动公共算力、公共数据和其他相关公共资源开放共享，鼓励个人、组织依法开放共享算力、数据和其他相关资源。

国家鼓励人工智能研发和应用，依法保护人工智能领域知识产权，支持利用人工智能生成物进行的科学研究和文化创作活动。国家完善人工智能知识产权申请审查标准，建立人工智能训练数据法定许可和合理使用制度，基于公平合理原则明确人工智能生成物的权利归属、权益保护和收益分配机制。

第十一条（伦理原则）开展人工智能研发、提供和使用活动应当将伦理要求贯穿全过程，促进人工智能的负责任创新与善意使用。

第十二条（国际合作）国家积极开展人工智能领域的国际交流与合作，推进与其他国家和地区的对话与互认，参与人工智能相关国际规则和标准的制定和实施，推进形成具有广泛共识的国际人工智能治理框架和标准规范。

国家完善人工智能领域的人才、技术引进和技术合作制度。

第十三条（主管机关）国家人工智能主管机关在中央人工智能领导机构领导下，主管全国的人工智能发展和管理工作。其他有关部门和军队有关部门依照本法和有关法律、行政法规的规定，密切配合、加强协调，依法做好有关工作。

省、自治区、直辖市，省、自治区的人民政府所在地的市，经济特区所在地的市和国务院已经批准的较大的市人工智能主管机关和其他相关部门，按照国家有关规定，在本辖区范围内负责人工智能发展和管理工作。

第十四条（协同共治）国家建立和完善政府管理、企业履责、行业自治、社会监督、用户自律的人工智能治理机制，促进多元主体协同共治。

第十五条（合法正当）从事人工智能研发、提供和使用活动应当合法正当，遵守以下规定：

（一）坚持社会主义核心价值观，弘扬全人类共同价值，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）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；

（三）依法保护消费者、劳动者权益，尊重他人合法权益，依法履行未成年人、老年人、残疾人等群体的保护义务，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；不得利用人工智能实施情感操控、设置情感陷阱或者诱导自伤自残、过度消费、违法犯罪等危险行为。

第二章 人工智能支持与促进

第十六条（人工智能发展规划）国家制定和实施人工智能发展规划，坚持人工智能研发攻关、产品应用和产业培育共同推进，全面支撑科技、经济、社会发展和国家安全。

省级以上人民政府应当将人工智能发展纳入本级国民经济和社会发展规划，并

根据需要制定人工智能发展规划。

第十七条（政策和决策适配性评估）国家建立人工智能政策适配性评估机制，对拟出台或者已实施的政策、决策、制度，开展与人工智能发展和安全形势的适配性评估。经评估认为可能显著影响人工智能发展或者安全的，应当及时调整、废止或者修改完善。

第十八条（算力基础设施建设）国家建立人工智能公共算力资源供给制度，推动公共算力资源平台建设与利用，加强算力科学调度，为人工智能技术与产业发展提供公共算力支持。

鼓励和支持高等院校、科研机构、企业和其他组织建设人工智能算力基础设施，开展算力资源市场化交易，引导各行业合理有序使用算力资源，提升算力基础设施利用效能。

第十九条（算法和模型创新）国家支持人工智能算法创新，鼓励建设、运营开源开发平台、开源社区和开源项目等，鼓励设立开源人工智能基金会，推进开源软件项目安全合规应用。

对人工智能技术的攻关研究和应用创新有突出贡献的组织和个人，国家依法予以表彰奖励。

人工智能研发者采用符合国家标准的去标识化技术处理个人信息，用于模型训练，取得认证后，不需取得个人同意。

第二十条（数据要素供给）国家建立健全数据要素市场化配置机制，完善数据标准体系和质量管理体系，加快建设人工智能语料库，建设高质量数据集，扩大面向人工智能应用的数据供给范围。

建立健全数据要素供给激励机制，支持相关主体将数据与行业知识深度融合开

发数据产品，为人工智能算法设计、模型训练、产品验证和场景应用提供全方位数据支撑。

第二十一条（可信数据）国家支持建立权威、安全的信息数据库，对不同类型数据的可信度建立标签体系。

第二十二条（模型开发平台的支持、引导）国家引导和支持模型开发平台的建设和运行，鼓励其为人工智能研发者、提供者提供算力调度、数据管理、模型训练、测试验证、部署发布、安全测评和合规工具等基础服务。

模型开发平台提供者应当根据其实际功能和控制能力，建立必要的数据安全、模型安全、访问控制、日志留存、漏洞管理和违法违规内容处置机制；法律、行政法规另有规定的，从其规定。

第二十三条（人工智能基础研究促进）国家将人工智能基础研究纳入科技发展规划，支持基础理论与交叉学科研究。国家建立稳定的基础研究多元投入机制，支持符合条件的高等学校、科研机构及企业承担研究任务。

国家建立面向基础研究的公共算力优先保障机制。利用财政性质资金开发的人工智能基础模型、核心算法及研究工具，除涉及国家安全、商业秘密等依法不公开的情形外，应当向科研机构、高等学校等从事非营利性研究的组织开放共享。

第二十四条（基础模型训练利用作品法定许可）国家建立基础模型训练利用作品法定许可制度，完善法定许可费用标准和分配机制。

除著作权人声明不许利用其作品进行模型训练的外，符合国家规定条件的基础模型研发者，可以根据法定许可制度规定，在模型训练过程中使用已发表的作品。

第二十五条（开源基础模型训练著作权合理使用）开源基础模型研发者利用作品进行模型训练，除著作权人声明不许利用其作品进行模型训练的，可以不经著作

权人授权，在模型训练过程中使用合法获取的作品，不需向著作权人支付报酬。

鼓励开源基础模型研发者以适当方式向著作权人提供相应补偿，促进作品的传播和利用。

第二十六条（人工智能搜索服务的作品合理使用）生成式人工智能在服务中提取网页等公开内容并整合输出，标明来源，且不影响作品正常使用、不损害著作权人合法权益的，适用《中华人民共和国著作权法》合理使用规定。

第二十七条（产业发展与应用创新）鼓励政府和企事业单位使用人工智能关键技术，促进技术集成与商业模式创新，推动重点领域智能产品创新，积极培育人工智能新兴业态，打造具有国际竞争力的人工智能产业集群。

国家推动人工智能与各行业融合创新，在重点行业和领域开展人工智能应用试点示范，推进人工智能规模化应用，引导形成人机协同、跨界融合、共创分享的智能经济和智能社会新形态。

第二十八条（智能体生态构建）国家推动构建安全、有序、开放的智能体生态。

第二十九条（促进中小企业创新）国家鼓励中小企业开展人工智能研发、提供活动，重点支持中小企业在基础模型及其具体应用领域的技术创新、产品研发和应用拓展。

第三十条（国家机关先行先试）鼓励政府机关、事业单位及其他依法具有管理公共事务职能的组织，在政务服务、公共管理等领域依法开展人工智能技术应用先行先试，优先采购和使用安全可靠的人工智能产品和服务。

第三十一条（人工智能特区及授权立法）国家在符合条件的地区设立人工智能特区，推动人工智能创新发展先行先试，促进人工智能产学研用结合，构建有利于人工智能发展的社会生态。

人工智能特区所在地的市级人民代表大会及其常务委员会可以根据本法，结合特区内人工智能创新发展实践需要，遵循宪法规定以及法律和行政法规基本原则，就人工智能研发、提供、使用活动制定法规，在人工智能特区范围内实施。

人工智能特区法规可根据授权对法律、行政法规、地方性法规作变通规定。

人工智能特区法规应当报送全国人民代表大会常务委员会和国务院备案；对法律或者行政法规、部门规章的规定作变通规定的，应当说明变通的情况和理由。

第三十二条（自贸试验区豁免）经国务院批准，自贸试验区（自由贸易港）对符合条件的人工智能研发、提供活动建立税收优惠机制，灵活调整知识产权保护、网络数据安全管理和贸易管制等措施，促进国际技术交流、跨境数据共享及国际科研合作。

第三十三条（财政和采购支持）中央财政应当在本级预算中设立人工智能科目，安排人工智能发展专项资金。

县级以上地方各级人民政府应当根据实际情况，在本级财政预算中安排人工智能发展专项资金。

鼓励各级人民政府和国有企事业单位采购符合国家标准的开源人工智能产品、服务。

第三十四条（税收抵免优惠）人工智能研发者、提供者研发或购置用于安全治理等专用设备的投资额，可以按不低于30%的比例实行税额抵免。

国家针对开源人工智能研发制定专门的税收优惠办法。符合国家人工智能主管机关确定标准的开源人工智能研发主体，可以依法享受研发费用加计扣除等税收优惠。

第三十五条（测评体系）国家支持和引导科研院校、企事业单位参与人工智能模型测评体系建设，发展公平、可靠、成本合理的测评基准，形成具有国际竞争力和影响力的测评方案。

第三十六条（人工智能国际标准制定）国家鼓励提升人工智能标准国际化水平，支持有关单位和个人依法参与人工智能国际标准制定，推动中国人工智能领域标准与国际标准的对接、转化、互认和协同适用。

第三十七条（专业人才培养）国家支持高等院校完善人工智能领域学科布局和人才培养机制。

鼓励高等学校、科研机构和企业等开展面向人工智能领域重大科学前沿问题的基础理论研究和关键共性技术研发。

国家支持建立有利于促进人工智能发展的项目管理创新机制，创新人才评定机制、科技成果转化激励机制等。

第三十八条（人工智能技术与产品出口鼓励措施）国家鼓励和支持符合安全合规要求的研发者向全球推广人工智能技术产品,对纳入目录的非敏感人工智能技术和产品出口，简化出口管制审批流程。

第三十九条（人工智能涉外法治协调机制）国家建立人工智能涉外法治协调、风险预警和争议应对支持机制，支持人工智能涉外合规服务平台建设，依法开展跨境监管协作和执法合作。

第三章 人工智能管理制度

第四十条（分类管理制度）国家建立人工智能负面清单制度，对负面清单内的产品、服务实施许可管理;对负面清单外的产品、服务,确有需要的,实施备案管理。

国家人工智能主管机关根据人工智能在经济社会发展中的重要程度，以及一旦遭到攻击、篡改、破坏或者非法获取、非法利用，对国家安全、公共利益、社会稳定、环境保护，或者个人、组织合法权益、经济秩序造成的危害程度，牵头制定并定期更新人工智能产品、服务负面清单。

第四十一条（负面清单管理制度）开展人工智能负面清单内的研发、提供活动，应当在开展前取得国家人工智能主管机关的许可。

禁止未经许可或者超越许可范围开展负面清单内人工智能研发、提供活动。

第四十二条（负面清单许可条件）申请负面清单内人工智能研发、提供许可，应当具备下列条件：

（一）在中华人民共和国境内依法设立的法人；

（二）主要负责人是中华人民共和国公民；

（三）有与风险相适应的具备质量保障、安全保障、人类监督、合规管理等专业知识的一定数量的专职人员；

（四）有健全的人工智能质量管理体系、网络数据安全管理制度、伦理审查制度；

（五）有符合法律法规和相关国家标准的安全可控的人工智能技术保障措施；

（六）有与风险相适应的人工智能应急处置机制；

（七）有与人工智能研发、提供相适应的场所、设施和资金；

（八）法律、行政法规规定的其他条件。

利用智能体提供负面清单内人工智能产品、服务，可能实质影响原许可范围或者风险水平的，应当依法申请许可、变更许可或者重新申请许可。

第四十三条（负面清单许可的申请）人工智能研发者、提供者申请负面清单内人工智能产品研发、提供许可，应当提交以下材料：

（一）申请书；

（二）法人资格、场所、设施、资金等证明；

（三）主要负责人为中华人民共和国公民的证明；

（四）质量保障、安全保障、人类监督、合规管理专职人员的资质情况；

（五）人工智能质量管理体系、网络数据安全制度、伦理审查制度、风险管理制度及执行情况；

（六）符合规定的人工智能安全评估报告；

（七）法律、法规规定的其他材料。

第四十四条（负面清单许可的审批）国家人工智能主管机关受理负面清单内人工智能研发、提供许可申请后，自受理之日起十个工作日内进行初步审查。

经初步审查，发现人工智能的研发者和提供者提交的申请材料不符合要求的，国家人工智能主管机关可以要求其补充或者更正。人工智能研发者、提供者无正当理由不补充或者更正的，该申请即被视为撤回申请。

初步审查材料齐全的，国家人工智能主管机关应当自受理申请之日起四十五个工作日内作出许可或者不予许可的决定。予以许可的，向申请人颁发人工智能研发、提供许可证；不予许可的，应当书面通知申请人并说明理由。

期满不能作出决定的，经国家人工智能主管机关负责人批准，可以延长十个工作日，并应当将延长期限的理由告知申请人。

第四十五条（负面清单许可的再次申请、变更、注销）负面清单内人工智能研

发、提供许可证应当载明使用许可的期限和范围。

超出许可范围，或者因技术改进、使用场景变更、用户群体调整等导致人工智能的风险发生显著变化而与原许可条件不符的，负面清单内人工智能研发者、提供者应当再次申请研发、提供许可。

未导致风险显著变化或者超出原许可范围的，应当依法办理许可变更手续；具体变更事项、程序和期限由国家人工智能主管机关规定。

使用许可期限届满前六个月，负面清单内人工智能研发者、提供者可以申请更新研发、提供许可。

负面清单内人工智能研发者、提供者停止许可内人工智能研发、提供的，应当在停止之日起三个月内，向国家人工智能主管机关申请注销研发、提供许可。

第四十六条（许可证公开）负面清单内人工智能研发者、提供者应当在所提供的人工智能产品、服务的显著位置，注明许可证编号，并提供便捷的许可范围、许可期限的查询方式。

第四十七条（投诉、举报、释疑机制）个人和组织发现违法从事负面清单内人工智能研发、提供活动的，有权向国家人工智能主管机关投诉、举报，国家人工智能主管机关应当及时核实、处理。

个人和组织对负面清单内人工智能研发、提供活动有疑义的，有权请求国家人工智能主管机关予以说明，国家人工智能主管机关应当及时答复、处理。

第四十八条（其他许可、备案）根据法律、行政法规规定，应用人工智能应当取得行政许可或者办理备案的，人工智能提供者、使用者应当依法取得许可或者办理备案。

第四章 人工智能研发者、提供者、使用者义务

第一节 一般规定

第四十九条（安全管理义务）人工智能研发者应当履行以下义务：

（一）在将人工智能投入使用或者投放市场前以及在提供产品、服务期间定期开展安全评估，安全评估报告保存期限不少于五年；

（二）建立健全数据安全、系统安全保障机制，加强人工智能防御系统，防范外部攻击和内部泄露；

（三）及时发布最佳安全实践，持续维护和优化用于模型训练的语料库安全；

（四）建立重要数据和核心数据处理全流程追溯机制,妥善保管相关技术文档；

（五）采取有效措施，提升模型生成内容的准确性、可靠性；

（六）告知使用者人工智能的安全责任、风险隐患，并以显著方式引导使用者安全、正确地使用人工智能。

人工智能提供者应当根据具体情形参照执行第一款规定。

人工智能使用者应当依法、安全、诚信使用人工智能产品与服务，履行合理注意义务，采取必要措施防范安全风险，不得利用人工智能实施危害国家安全、公共利益及他人合法权益的行为。

禁止提供、传播、推广规避标识、去除标识或者逃避内容治理措施的技术、工具、服务或者方法。

第五十条（关键系统加密敏捷性与长周期安全）为关键信息基础设施提供的人工智能产品或者服务生命周期预期五年以上的，应当具备符合国家规定的长周期密码安全能力。

第五十一条（安全漏洞管理义务）鼓励相关组织和个人向人工智能研发者、提供者通报其产品、服务存在的安全漏洞。

人工智能研发者、提供者应当按照相关规定履行安全漏洞管理义务，及时发布并修补安全漏洞，指导支持使用者采取防范措施。

第五十二条（审计义务）人工智能研发者、提供者应当按照国家有关规定及国家人工智能主管机关的要求进行审计，核验输入数据、算法模型、输出数据等的合规性，对人工智能产品、服务活动遵守法律、行政法规的情况进行审查和评价。

第五十三条（补救和通知义务）人工智能研发者、提供者应当加强基础设施安全、算法模型安全、数据安全风险监测，发现安全缺陷、漏洞以及逻辑缺陷等风险时，应当立即采取补救措施。

人工智能研发者发现所研发的人工智能发生安全事件时，应当立即采取处置措施，并通知人工智能提供者，人工智能提供者按照本条第三款规定履行通知义务。人工智能提供者发现所提供的人工智能发生安全事件时，应当立即采取处置措施，按照本条第三款规定履行通知义务，并及时通知人工智能研发者。

人工智能提供者发现或者被通知发生安全事件，应当按照国家有关规定及时告知使用者并向主管机关报告以下事项：

（一）安全事件的发生过程、影响范围；

（二）人工智能提供者已采取的补救措施和使用者可以采取的减轻危害的措施；

（三）人工智能提供者的联系方式。

人工智能提供者采取措施可以有效避免对使用者造成实质损害的，可以不通知使用者；国家人工智能主管机关认为可能造成危害的，有权要求其通知受影响的使

用者。

人工智能研发者在发现安全事件或者收到提供者通知发生安全事件后应当立即进行评估。如果评估发现研发阶段存在问题风险的，应当立即通知其他人工智能提供者，在问题风险解决前，人工智能研发者应当暂停或者下架人工智能产品、服务。其他人工智能提供者收到通知的，应当立即采取处置措施，管控产品、服务风险。

第五十四条（公开透明性义务）人工智能提供者提供与自然人互动的人工智能服务，应当提前以清晰、易于理解的方式，告知自然人其正在与人工智能产品、服务进行交互；自然人从使用场景中可以明显判断的除外。

提供智能体服务的人工智能提供者应当根据国家有关规定、服务协议，记录与用户权益相关的智能体活动，为用户的合理查询提供便利。

提供深度合成服务的人工智能提供者应当根据国家有关规定，对合成内容进行合理标识，向公众提示深度合成情况。涉及算法推荐服务的，应当公示算法推荐服务相关规则，优化和提升透明度。

人工智能提供者应当在产品投入市场前或者提供服务前，以适当的方式告知使用者以下信息：

（一）产品、服务的基本原理、目的意图和主要运行机制；

（二）产品、服务的许可或者备案公示信息；

（三）使用者享有的权利和救济渠道；

（四）法律、行政法规规定的其他信息。

人工智能研发者应当配合提供者履行上述义务。

第五十五条（可解释性义务）人工智能产品、服务对个人权益有重大影响的，

人工智能使用者有权要求提供者对产品、服务决策的过程、方式等作出解释，有权对不合理的解释进行投诉。

人工智能提供者应当综合考虑产品、服务的场景、性质和行业技术发展水平等因素，对使用者的要求及时作出反馈。

人工智能研发者应当配合提供者履行上述义务。

第五十六条（公平性义务）人工智能研发者应当在训练数据处理和标注、算法模型设计研发和验证测试过程中，采取相应的必要措施，有效防范偏见和歧视。

人工智能提供者应当在提供产品、服务过程中，加强对输入数据、输出数据和服务运行情况的管理，并采取相应的必要措施，有效防范偏见和歧视。

第五十七条（风险管理）人工智能提供者应当综合考虑产品、服务的场景、性质、受众和行业技术发展水平等因素，建立健全并实施全生命周期风险管理制度。在产品、服务投入使用前以及使用过程中，人工智能提供者应当对人工智能的风险进行识别，采取必要管控措施，并保留风险识别和采取措施的记录不少于两年。

人工智能研发者应当对设计、数据收集训练、模型选择、测试验证等研发过程，建立并运行风险管理制度，对人工智能的风险进行识别，采取必要管控措施。人工智能研发者应当在保障商业秘密的前提下，配合提供安全评估报告、风险识别和管控措施记录，支持人工智能提供者履行人工智能服务的风险管理义务。

第五十八条（风险阻断与应急熔断机制）人工智能的研发者与提供者应当将安全防范要求贯穿设计、开发及运行的全流程，采取有效措施，防止系统局部故障、漏洞或者遭受攻击引发大范围的安全失控。

研发者与提供者应当建立人工智能应急熔断机制。发现系统存在严重安全隐患、处于失控状态或者可能引发级联风险时，应当立即主动采取暂停研发、停止更新、

限制功能、终止运行或者销毁系统等风险阻断措施，并向国家人工智能主管机关报告。

针对可能严重危害国家安全、社会公共利益或者引发重大系统性风险的人工智能，国家人工智能主管机关有权责令相关主体采取停止研发、终止服务、下架或者销毁系统等处置措施；必要时，可依法采取切断网络连接、限制数据传输等措施。

第五十九条（人工智能伦理审查义务）符合国家规定条件的人工智能研发者、提供者应当根据国家规定设立人工智能伦理审查委员会，开展人工智能伦理审查工作。

伦理审查应当重点评估人工智能活动是否符合增进人类福祉、促进公平公正、保障可控可信、提升透明可解释、确保责任可追溯以及隐私保护等方面的伦理要求。

国家鼓励设立第三方伦理审查机构，依照国家有关规定，为未设立伦理审查委员会的中小企业提供人工智能伦理审查服务。

第六十条（科研伦理）利用人工智能辅助科学研究的人员，应当在研究过程中保持学术自主性，恪守学术道德，对人工智能生成的内容进行必要的核实与判断，承担相应学术责任。

面向科研场景提供人工智能工具的主体，应当为使用者进行内容核验提供必要的技术支持和可追溯工具，并以显著方式提示使用者的核实义务。

第六十一条（国家机关提供、研发义务）国家机关及其他依法具有管理公共事务职能的组织，在政务服务、公共管理等领域研发、提供人工智能的，应当遵守本法规定的人工智能研发者、提供者的义务，尤其应当保障用于公共事务管理中的人工智能产品、服务的安全性、透明性、公平性。

第六十二条（授权代表）本法第二条第二款规定的中华人民共和国境外的人工

智能研发者、提供者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理人工智能相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送国家人工智能主管机关。

第六十三条（衍生模型特别规定）利用已有基础模型进行输出训练或者微调等技术处理形成的衍生模型，具备与原基础模型实质等同的通用能力，或者在特定领域、特定用途上显著扩展能力并可能产生相应风险的，应当参照基础模型履行相关义务。

第二节 人工智能研发者义务

第六十四条（负面清单内人工智能研发者增强义务）负面清单内人工智能研发者应当履行以下义务：

（一）制定并保存符合本法要求的技术文件；

（二）在研发过程中，制定并运行符合本法要求的质量管理体系；

（三）配合提供者履行相关义务；

（四）法律、行政法规规定的其他义务。

第六十五条（基础模型研发者特殊义务）基础模型研发者应当遵守以下规定：

（一）按照国家规定建立健全安全风险管理制度，加强风险监测，及时有效预防、处置对国家安全、公共利益或者个人、组织合法权益、经济秩序造成的风险；

（二）按照国家规定建立健全基础模型的模型管理和数据管理制度；

（三）遵循公开、公平、公正的原则，制定基础模型的使用规则，明确使用基础模型的研发者、提供者应当履行的义务，不得滥用市场支配地位；

（四）确保安全风险管理所必需的算力资源投入；

（五）协助其他研发者、提供者履行本法规定的相关义务；

（六）对严重违反本法规定的研发者、提供者，应当采取停止提供服务等必要措施；

（七）成立主要由外部成员组成的独立机构对基础模型的研发情况进行监督；每年发布社会责任报告，接受社会监督。

第三节　人工智能提供者义务

第六十六条（备案义务）人工智能提供者提供的产品、服务不在负面清单内，但注册用户数超过100万的，应当在满足条件之日起十个工作日内，向国家人工智能主管机关备案以下信息：

（一）人工智能提供者的姓名或者名称、联系方式；

（二）人工智能产品、服务的商标或者名称、提供形式、应用领域、算法类型、安全自评估报告；

（三）备案拟公示内容；

（四）法律、行政法规规定的其他信息。

注册用户数超过1万、不足100万的，应当在满足条件之日起十个工作日内，向省级人工智能主管机关备案前款信息。

备案信息发生变更的，应当在变更之日起十个工作日内办理变更手续。

完成备案的人工智能提供者应当在其对外提供服务的网站、应用程序等的显著位置注明其备案编号。

第六十七条（备案流程）主管机关收到备案材料后，材料齐全的，应当在三十个工作日内予以备案，发放备案编号并进行公示；材料不齐全的，应当在十个工作

日内通知备案人补充材料。

第六十八条（管理制度）人工智能提供者应当采取下列措施确保人工智能符合法律、行政法规的规定：

（一）制定内部数据安全、风险控制、质量管理等制度和相应的操作规程；

（二）保存提供人工智能产品、服务自动生成的日志；

（三）定期对从业人员进行教育和培训；

（四）采取保障鲁棒性、抗攻击性等合规技术措施；

（五）至少每两年进行一次人工智能审计；

（六）法律、行政法规规定的其他措施。

第六十九条（终止机制）人工智能提供者终止提供产品、服务的，应当采取以下妥善安排措施：

（一）提前三十个工作日公示终止方案、使用者权利等；

（二）自终止之日起三十个工作日内，删除使用者的个人信息；根据国家有关规定，对人工智能产品、服务提供过程中产生的数据、训练数据、算法模型作出必要处理；

（三）法律、行政法规规定的其他措施。

第七十条（许可注销）负面清单内的人工智能提供者终止提供产品、服务的，应当提前三十个工作日通知主管机关，说明有关情况，并在终止提供产品、服务后将许可证交回原许可机关。

不在负面清单内的人工智能提供者应当在终止服务之日起二十个工作日内办理

注销备案手续。

第七十一条（负面清单内的人工智能提供者增强义务）负面清单内的人工智能提供者，还应当履行如下义务：

（一）按照本法要求进行安全评估，确保安全、稳健；

（二）制定并保存符合本法要求的技术文件，以证明所提供的人工智能符合本法对负面清单内人工智能的要求；

（三）建立并运行符合本法要求的全生命周期质量管理体系；

（四）在人工智能产品、服务自主运行过程中，确保人类可以随时采取介入、接管等措施；

（五）法律、行政法规规定的其他义务。

第七十二条（终端权限安全保障）人工智能终端设备提供者应当确保终端设备产品质量,终端设备人工智能服务提供者应当保障终端设备人工智能服务的安全性、透明性。

终端设备人工智能服务涉及跨应用权限调用的，应当遵循最小必要原则，实施动态授权机制。用户授权范围应当限定于具体场景功能需求，防止通过泛化授权方式获取非必要权限。

第七十三条（智能体管理要求）智能体服务提供者应当提供撤销授权、退出运行等功能，保障使用者对智能体的运行实施合理控制。

提供智能体服务的人工智能提供者不得利用数据、算法、系统入口、接口控制及技术权限优势实施不正当竞争行为。

第七十四条（人工智能生成内容标识义务）人工智能提供者应当依照国家规定，

对人工智能生成合成内容进行标识，并采取必要措施，防止标识被删除、篡改、伪造或者隐匿。

人工智能提供者应当向使用者明确说明生成合成内容标识的方式及相关管理要求，并提示使用者合规使用。人工智能提供者发现使用者存在破坏标识行为的，应当及时采取限制使用、暂停服务等必要处置措施，并留存相关记录。

第四节　人工智能使用者义务

第七十五条（合法使用义务）人工智能使用者应当确保其向系统输入的数据、指令的合法性，不得故意输入侵犯他人合法权益或者包含歧视性、仇恨性内容的违法信息，不得故意提供误导性信息以诱导人工智能生成有害结果，不得向不符合保密要求的人工智能输入国家秘密、工作秘密和敏感信息。

人工智能使用者不得利用人工智能服务实施危害国家安全、侵入他人系统、窃取他人数据等违法犯罪行为。

第七十六条（公开传播时的标识义务）在使用人工智能生成内容并将其用于公开传播时，人工智能使用者应当按照国家有关规定添加、保留或者展示显式标识和隐式标识，不得删除、篡改、隐匿、伪造或者规避生成合成内容标识。

第七十七条（特定领域审慎使用义务）将人工智能用于可能影响公共利益或者他人重大权益的场景时，人工智能使用者应当进行必要的事实核验、来源审查、人工复核、风险提示。

人工智能使用者不得将未经核验的人工智能生成内容作为事实性、专业性或者决策性结论直接发布、传播或者提供给他人使用。

第七十八条（禁止恶意传播与污染义务）人工智能使用者不得通过批量生成、自动化发布、操纵账号、虚构流量、伪造来源、污染数据、误导模型等方式，扰乱网络传播秩序、制造虚假舆论、污染信息生态、影响人工智能系统正常运行。

第七十九条（劳动者权益保护义务）用人单位使用人工智能对职工岗位、工作内容、劳动条件、绩效评价、职业发展、劳动合同的履行产生重大影响的，应当经过集体协商，并采取告知、培训、安置等权益保护措施。

用人单位不得仅以人工智能技术替代为由，在未采取培训、安置、协商等必要措施的情况下单方变更或者解除劳动合同。

用人单位使用人工智能侵犯职工劳动权益的，工会可以依法要求企业、事业单位、社会组织予以改正并承担责任。

第八十条（国家机关使用人工智能的管理要求）国家机关使用人工智能，应当坚持确保安全、统筹集约的原则，实施集中统一的安全管理和体系化技术防护措施。

国家机关使用人工智能作出或者辅助作出影响公民、法人或者其他组织合法权益的认定、决定、裁决等活动的，除依法确定为国家秘密外，应当依当事人、相对人或者利害关系人申请公开使用人工智能的基本情况。

第五章 人工智能综合治理机制

第八十一条（国家人工智能主管机关职责）国家人工智能主管机关依法履行以下人工智能监管职责：

（一）每年3月31日前向国务院报送人工智能发展和治理情况专项报告；

（二）开展人工智能伦理、安全教育与宣传，指导、监督人工智能研发、提供和使用活动；

（三）制定人工智能监管规则、指引，组织制定人工智能伦理、安全、管理等方面的标准；

（四）建立统一的人工智能监管服务平台，推动申请材料共享、审查与评估结果互认、跨部门联合审查与协同监管；

（五）推进人工智能治理社会化服务体系建设，指导、支持专业机构开展人工智能安全及伦理监测、评估、审计、认证等服务；

（六）指导、支持开源人工智能创新共同体建设与开展活动，引导、协调创新共同体定期发布和更新开源人工智能项目最佳实践指南等；

（七）建立人工智能伦理及风险监测预警机制，组织人工智能领域伦理及风险信息的获取、分析、研判、预警工作；

（八）建立人工智能伦理及安全事件应急处置机制；

（九）接受、处理与人工智能技术及产品研发、提供和使用有关的投诉、举报；

（十）调查、处理人工智能研发、提供和使用中的违法活动和可能导致严重后果的违背伦理行为；

（十一）法律、行政法规规定的其他职责。

第八十二条（人工智能伦理专家委员会）国家人工智能主管机关成立国家人工智能伦理专家委员会，地方人工智能主管机关成立本级人工智能伦理专家委员会。

国家人工智能伦理专家委员会负责对人工智能研发、提供和使用中的重大伦理问题进行研究，为国家人工智能主管机关提供咨询意见，指导全国范围内的伦理审查相关工作。

地方人工智能伦理专家委员会负责对本行政区域人工智能研发、提供和使用活

动中的伦理问题进行研究，为本级地方人工智能主管机关提供咨询意见，指导本行政区域人工智能研发者、提供者和使用者人工智能伦理审查委员会的工作。

第八十三条（安全审查制度）从事人工智能研发、提供、使用活动，影响或者可能影响国家安全的，应当按照国家有关规定通过安全审查。

依法作出的安全审查决定为最终决定。

第八十四条（人工智能出口安全审查与豁免）国家有关部门制定并动态调整人工智能技术产品禁止类、限制类出口管理目录。对符合国家规定的用于民生改善、灾害防治、公共卫生、应急等公益领域的人工智能产品，可豁免部分出口许可审查程序。

第八十五条（前置程序期限）人工智能研发者、提供者、使用者依照本法及国家有关规定，就人工智能新技术新应用申报安全审查、办理备案或者申请行政许可的，国家人工智能主管机关应当在规定的工作期限内及时处理、作出答复。

第八十六条（约谈）国家人工智能主管机关和地方各级人工智能主管机关在履行职责中，发现人工智能研发、提供、使用活动存在较大风险或者发生安全事件的，可以按照规定的权限和程序对该人工智能研发者、提供者进行约谈，要求其采取下列措施：

（一）按照要求进行整改，消除隐患；

（二）对其研发、提供活动作出适当的解释，说明人工智能产品、服务的开发、管理和运行的责任，为保障公平性、安全性和稳定性采取的措施，以及对利益相关方的影响等；

（三）委托专业机构对其人工智能研发、提供、使用活动进行合规审计。

人工智能研发者、提供者承诺限期整改合规，且能够有效避免人工智能研发、提供或者使用活动造成危害的，可以不暂停相关活动。国家人工智能主管机关认为可能造成危害的，可以责令暂停相关活动。

第八十七条（创新监管）国家人工智能主管机关就因违法行为轻微等情形依法决定不予行政处罚的，应当通过批评教育、指导约谈、组织会商研讨等措施督促、引导当事人依法合规开展人工智能产业研发、提供和使用活动。

国家人工智能主管机关可以针对开源人工智能研发者制订专门的合规指引，推动开源人工智能创新发展。

第八十八条（人工智能产业链）国家引导人工智能产业链供应链合理有序布局，提升产业链供应链安全可控水平。国家人工智能主管机关会同相关部门建立健全人工智能产业链供应链安全风险预警、应急管理制度。

第八十九条（监管试验）国家人工智能主管机关建立人工智能监管试验机制，就以下事项制定具体规定、指引：

（一）参与监管试验的条件以及遴选程序；

（二）监管试验的运行机制；

（三）监管试验的风险监测与防控措施以及处置机制；

（四）参与监管试验的人工智能研发者、提供者、使用者的义务、责任减免机制。

第九十条（内部举报人保护机制）人工智能研发者、提供者、使用者应当建立健全内部举报制度和举报人保护制度，明确举报处理程序和保护要求。

举报范围包括但不限于人工智能研发、提供、使用过程中存在的下列情形：

（一）可能造成重大人身伤害或者财产损失的安全隐患；

（二）违反法律规定的风险防控义务和安全要求；

（三）故意隐瞒或者歪曲重要技术缺陷或者安全评估结果；

（四）其他影响或者可能影响国家安全、公共安全的情形。

内部举报人向所在单位举报或者向有关主管部门、司法机关举报的，人工智能研发者、提供者、使用者所属机构不得对举报人实施降职、调岗、解聘等任何形式的打击报复。

因内部举报人举报，人工智能研发者、提供者、使用者企业或者机构及时发现并消除安全隐患、防止或者减轻危害后果的，应当作为从轻或者减轻研发者、提供者、使用者行政处罚的情形。内部举报人曾参与相关违法行为，但主动举报并积极配合调查的，可以依法从轻、减轻或者免除对其的处罚。

国家保护内部举报人的个人信息、隐私和安全。国家人工智能主管机关应当设立举报渠道，及时受理、处理举报，并对举报人的个人信息、举报内容严格保密。任何组织或者个人不得泄露内部举报人的身份和个人信息，不得威胁、恐吓内部举报人或者对其采取打击报复措施。

第九十一条（国家机关责任人）国家机关及其他依法具有管理公共事务职能的组织应当指定人工智能负责人，负责对人工智能有关活动以及采取的安全保护措施等进行监督。

第九十二条（执法机制）国家人工智能主管机关应当加强专门队伍和专业技术建设，提升监管从业人员的专业能力，开展相关技术培训，不断提升人工智能监管能力和水平。

国家人工智能主管机关应当依法确定本系统行政执法程序，建立行政执法监督制度。

第九十三条（技术治理）国家支持企业、科研机构、高等院校等研究开发有关人工智能监测预警、安全评估、应急处置等技术，鼓励在人工智能领域应用监管科技、合规科技。

第九十四条（域外效力）境外的机构、组织和个人从事侵害中华人民共和国国家安全、公共利益和公民、组织合法权益的人工智能的研发、提供或者使用活动的，依法追究法律责任；造成严重后果的，国家人工智能主管机关可以依法采取限制或者禁止其在中华人民共和国境内研发、提供或者使用人工智能等措施，并予以公告。

第九十五条（采取反制）外国国家、地区、组织、个人违反国际法和国际关系基本准则，以各种借口或者依据其本国法律对中国人工智能技术、机构和行业等进行遏制打压，对我国公民、组织采取歧视性禁止、限制或者其他类似措施，有关部门依法采取相应处理措施。

第六章 法律责任

第九十六条（一般违法责任）违反本法规定开展研发、提供、使用活动，或者对内部举报人进行打击报复的，由国家人工智能主管机关责令改正，给予警告，没收违法所得，并可以责令暂停或者终止相关业务；拒不改正的，处十万元以上一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上、十万元以下罚款。

有前款规定的违法行为，情节严重的，由国家人工智能主管机关责令改正，没收违法所得，并处一百万元以上、一千万元以下或者上一年度营业额百分之四以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管机关吊销相关业务许

可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第九十七条（负面清单许可的撤销）人工智能研发者、提供者在研发、提供活动中违反本法规定，发生重大安全事件、一年内发生三次以上安全事件或者受到三次以上行政处罚的，国家人工智能主管机关可以中止许可并责令限期改正；期限届满未改正，或者中止许可后再次发生安全事件或者受到行政处罚的，国家人工智能主管机关可以撤销许可。

第九十八条（行政罚款的裁量方式）本法规定的罚款可以作为责令整改等措施的补充，国家人工智能主管机关决定行政罚款金额时，遵循合法原则、过罚相当原则、公平公正原则、处罚和教育相结合原则、综合裁量原则，应当充分考虑以下因素：

（一）违法行为及后果的性质、严重性和持续时间、受影响的范围和损害程度；

（二）违法行为是故意还是过失；

（三）对违法行为是否采取了补救措施并减轻可能造成的损失；

（四）是否依照本法规定通知国家人工智能主管机关；

（五）是否依照本法规定采取了合理有效的组织和技术措施管理人工智能的风险；

（六）是否遵守了人工智能和安全等相关标准或者获得了相关认证；

（七）此前的违法行为；

（八）内部举报人举报行为对损害结果的影响；

（九）其他法律法规规定的加重或者减轻处罚的因素。

第九十九条（备案违规责任）人工智能提供者应当备案而未备案的，由国家人工智能主管机关给予警告；经警告后仍未及时备案的，处一万元以上十万元以下罚款。

人工智能提供者通过隐瞒有关情况、提供虚假材料等不正当手段取得备案的，由国家人工智能主管机关予以撤销备案，给予警告、通报批评；情节严重的，并处十万元以上一百万元以下罚款。

人工智能提供者终止服务未办理注销备案手续，或者发生严重违法情形受到责令关闭网站、吊销相关业务许可证或者吊销营业执照等行政处罚的，由国家人工智能主管机关依职权注销备案。

第一百条（人工智能侵权归责原则）研发者因训练数据或者算法设计不当、安全测试不符合标准、明知存在重大隐患而未采取必要安全措施等，侵害他人合法权益造成损害的，应当承担侵权损害赔偿责任。

提供者侵害他人合法权益造成损害，不能证明自己没有过错的，应当承担侵权损害赔偿责任。

使用人工智能侵害他人合法权益造成损害的,应当依法承担侵权损害赔偿责任。

研发者、提供者、使用者能够证明损害系因被侵权人故意规避安全措施所致，且履行必要的技术防范义务的，可减轻或者免除侵权损害赔偿责任。

研发者、提供者、使用者的侵权行为危及他人人身、财产安全的，被侵权人有权请求侵权人承担停止侵害、排除妨碍、消除危险等侵权责任。

第一百零一条（损害赔偿计算）人工智能侵权损害赔偿按照被侵权人的实际损失确定；实际损失难以确定的，按照侵权人因侵权所获得的利益确定；被侵权人的

损失或者侵权人获得的利益难以确定的，由人民法院根据侵权行为的具体情节确定赔偿数额。

人工智能研发者、提供者、使用者对内部举报人进行打击报复，违反规定解除劳动合同或者采取其他不利措施的，应当按照实际损失的二倍以上十倍以下向举报人支付赔偿金，且不低于上一年度劳动报酬。

第一百零二条（生成式人工智能提供者的安全港）利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，侵犯他人民事权益造成损害，提供者同时采取以下措施的，不承担侵权损害赔偿责任：

（一）制定民事权益保护规则，建立有效的投诉机制，供权利人维护其合法权益；

（二）以用户协议等方式提示使用者不得侵犯他人民事权益；

（三）收到权利人的有效侵权通知后，采取必要措施停止生成侵权内容，并依法依约对利用其服务侵犯他人合法权益的使用者采取警示、限制功能、暂停或者终止向其提供服务等处置措施；

（四）对人工智能生成内容依法进行标识。

因提供者故意或者重大过失导致侵权的，不适用前款免责规定。

第一百零三条（生成式人工智能使用者责任）使用者利用人工智能生成并传播侵权内容造成损害，存在过错的，应当承担侵权损害赔偿责任。提供者知道或者应当知道使用者利用其服务侵犯他人民事权益而未采取第一百零二条规定的必要措施的，与使用者承担连带责任。法律另有规定的，从其规定。

第一百零四条（开源人工智能的法律责任减免）以免费且开源的方式提供人工

智能研发所需的部分技术组件，同时以清晰的方式公开说明其功能及安全风险的，对因第三方独立使用行为导致的损害不承担侵权损害赔偿责任。

免费且开源提供人工智能的个人、组织能够证明已经建立符合国家标准的人工智能合规治理体系，并已采取相应有效安全治理措施的，可以减轻或者免除侵权损害赔偿责任。

第一百零五条（法律救济）公民、法人或者其他组织对人工智能主管机关作出的行政行为不服的，可以依法申请行政复议或者向人民法院提起行政诉讼。

第一百零六条（公益诉讼）人工智能提供者违反本法规定提供产品或者服务，侵害公共利益的，人民检察院、法律规定的消费者组织和由国家人工智能主管机关确定的组织可以依法向人民法院提起诉讼。

第一百零七条（治安管理处罚和刑事责任的衔接）违反本法规定，构成违反治安管理行为的，依法给予治安处罚；构成犯罪的，依法追究刑事责任。

第一百零八条（不予处罚）人工智能研发者、提供者、使用者违法行为轻微并及时改正，没有造成危害后果的，不予行政处罚。初次违法且危害后果轻微并及时改正的，可以不予行政处罚。

第一百零九条（国家机关不履职的责任）国家机关开展人工智能研发、提供、使用活动，不履行本法规定的义务的，由其上级机关或者国家人工智能主管机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

国家机关工作人员履行本法规定的义务存在玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

依法不构成行政执法过错的情形，不追究有关工作人员的行政执法责任。

第七章 附则

第一百一十条（军事人工智能）中国人民解放军、中国人民武装警察部队的人工智能的研发、提供和使用活动，由中央军事委员会依照本法规定的原则另行规定。

第一百一十一条（人工智能科研豁免与科研安全港）专门为科学研究与技术开发目的，在限定范围内使用人工智能的，不适用本法一般性监管的规定；但法律、行政法规对国家安全、公共安全、个人信息与重要数据保护另有规定的除外。

前款活动应当同时符合下列条件：

（一）不以向公众提供商业服务为目的；

（二）训练数据来源合法；

（三）采取必要的安全措施；

（四）保存相关科研记录。

第一百一十二条（定义）本法下列用语的含义：

（一） 人工智能，是指以一定自主程度运行，服务于特定或者通用的目标，能够通过预测、推荐或者决策等方式影响物理或者虚拟环境的自动化系统，包括数据、特征、模型、服务提供接口和所嵌入的终端设备等。

（二） 基础模型，是指累计投入一定规模以上算力进行训练，服务于通用的目的，能够为广泛的下游服务提供技术支持的人工智能模型。基础模型认定的浮点运算及其他算力标准由国家人工智能主管机关组织制定、公开发布并定期更新。

（三）开源人工智能，是指在开源许可证框架下，以可获取形式向社会公众公开发布的人工智能系统，其技术组件应当包含基础模型权重、参数等核心要素，并按照技术特性附有适度公开的训练数据集、完整的模型参数说明或者相应的安全合

规文档等。开源人工智能的开放程度应当符合降低技术复用门槛、实现本地部署和修改自由的实际需要。

（四）人工智能研发者，是指以训练、优化人工智能系统的算法、模型等为目的，实施研发活动，但不直接向使用者提供人工智能产品、服务的个人或者组织。从事人工智能辅助性技术开发的，不属于本法规定的研发者。

（五）人工智能提供者，是指以自己名义向他人提供人工智能系统功能，并对该系统的调用、运行、管理具有实质控制能力的个人或者组织。

（六）人工智能使用者，是指依照人工智能的性能和用途对其加以利用的个人或者组织。

（七）智能体，是指具备自主感知、记忆、决策、交互与执行能力，连接使用者与应用程序等服务工具的人工智能系统。

（八）终端设备，是指可以接入网络、具有操作系统、能够由用户自行安装应用软件的手机、计算机等网络终端产品。

（九）内部举报人，是指在人工智能研发者、提供者、使用者所属机构在职或者曾经在职，因工作关系知悉相关信息并进行举报的自然人。

第一百一十三条（负面清单公开和更新制度）国家人工智能主管机关应当不晚于本法实施之日前六个月发布人工智能负面清单，并在定期更新后及时公开。

第一百一十四条（施行日期）本法自 年 月 日起施行。