

国家安全,你我共筑!

国家网信办等五部门

联合公布《人工智能拟人化互动服务管理暂行办法》

记者从国家网信办获悉:10日,国家网信办、国家发展改革委、工业和信息化部、公安部、市场监管总局联合公布《人工智能拟人化互动服务管理暂行办法》,自2026年7月15日起施行。

国家网信办有关负责人表示,《办法》旨在促进人工智能拟人化互动服务健康发展和规范应用,维护国家安全和社会公共利益,保护公民、法人和其他组织的合法权益。

近年来,人工智能拟人化互动服务快速发展,在文化传播、适幼照护、适老陪伴等领域的创新应用不断涌现。与此同时,危害未成年人身心健康、影响网络信息安全等问

题日益显现。出台《办法》,既是促进人工智能拟人化互动服务健康发展的重要要求,也是防范有关安全风险的现实需要。

《办法》践行以人为本、智能向善的理念,明确国家坚持发展和安全并重、促进创新和依法治理相结合的原则,鼓励人工智能拟人化互动服务创新发展,对人工智能拟人化互动服务实行包容审慎和分类分级监管;提出人工智能拟人化互动服务促进措施,明确支持技术研发创新,鼓励有序拓展文化传播、适老陪伴等相关领域应用;规定提供人工智能拟人化互动服务的基本要求,明确不得从事生成危害国家安全、荣誉和利

益,煽动颠覆国家政权、推翻社会主义制度等内容的活动,规定人工智能拟人化互动服务提供者的安全管理义务;完善网络用户权益保护制度,规定人工智能拟人化互动服务提供者的未成年人、老年人权益保护和个人信息保护等义务。此外,《办法》还规定了安全评估、算法备案、指导推动人工智能沙箱安全服务平台建设等制度。

国家网信办有关负责人表示,人工智能拟人化互动服务的发展与治理需要政府、企业、社会、网民等多方参与,共同维护良好网络生态,促进人工智能向上向善。

(据《人民日报》)

出了新国标,原来的充电宝还能用吗

强制性国家标准《移动电源安全技术规范》4月3日发布,将于2027年4月1日正式实施。新国标出台,消费者手中的充电宝还能继续使用吗?使用充电宝,有哪些注意事项?

充电宝安全为何重要

读者关切:去年起有的充电宝不让带上飞机,如今又出台新国标,充电宝安全隐患大吗?

充电宝已成为很多人出行的“标配”,它不只是一个随身小物件,而是与车、船、飞机等交通工具紧密相连的“移动能源单元”,事关广大乘客生命财产安全,因此必须经受住严苛的安全考验。

去年,中国民航局出台新规,自2025年6月28日起禁止旅客携带没有强制性产品认证(CCC认证)标识、标识不清晰、被召回型号或批次的充电宝乘坐境内航班。这源于机上充电宝起火冒烟事件频发,多家航司的航班曾因此备降、返航或紧急处置。

不仅是飞机上,充电宝放在桌上充电约5小时后突然爆炸、酒店客房内充电宝被压在枕头下充电引发火灾等事件暴露安全隐患。2025年,市场监管总局督促企业召回问题充电宝139.77万台。

为最大限度减少安全隐患,新国标在移动电源电池、保护电路、电池原材料和电池生产过程等方面的要求均有较大提升。新国标以多项安全标准升级划出“新红线”,为产品质量筑牢“防火墙”,为广大消费者撑起“安全伞”,也有利于行业高质量发展。

新国标有哪些变化

读者关切:与此前标准相比,新国标有哪些新要求?

新国标明确提升移动电源在高温、过充、挤压等滥用场景下的安全防护能力,从源头降

低安全风险。

电池内部短路是引起移动电源起火、爆炸的主要原因之一。造成内部短路的原因主要是挤压等外部应力、内部电极老化析锂以及材料和生产过程中混入杂质等。对此,新国标提出新规定:加严挤压试验条件、在消费类电池中首先引入针刺试验、引入300次充放电循环后的析锂检测,增加来料检测和生产过程管理等。

新国标将电池充满后继续充电(过充电)试验电压提高到充电限制电压的1.3倍,要求在现有一层保护电路设计的基础上额外增加一层保护电路,并新增过压禁用功能。上述新要求分别从提升电池过充条件下本质安全水平、降低电池遭受大电压过充概率、杜绝移动电源“带病”使用可能性三个方面提出了解决方案。

新国标推行产品唯一性编码管理,移动电源将标注专属“身份证号码”,消费者可通过该编码查询电池品牌等重要信息。

过渡期后充电宝需要换吗

读者关切:手上的充电宝用了好几年,正准备换个新的。新国标一年后就实施了,现在买的还能继续用吗?

新国标实施后,消费者已购买的取得CCC认证的合规移动电源产品,可以继续正常持有和使用。通过CCC认证的充电宝,只要符合民航现行相关规定,仍可正常携带乘机。

新国标实施有一年过渡期,这样设置主要有两点目的:一是为企业新产品研发、设计与生产线调整预留时间,确保标准正式实施后,符合新标准的产品能够及时、有序投放市场;二是为渠道和终端经销商留出消化库存产品的空间,避免社会资源浪费和行业波动,保障市场供给稳定。

(据《人民日报》)

什么是国家安全?

根据《中华人民共和国国家安全法》第二条规定,国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态,以及保障持续安全状态的能力。

全民国家安全教育日的由来

2015年7月1日,第十二届全国人民代表大会常务委员会第十五次会议通过的《中华人民共和国国家安全法》规定:每年4月15日为全民国家安全教育日。

公民和组织在维护国家安全中的义务有哪些?

- (一)遵守宪法、法律关于国家安全的有关规定;
- (二)及时报告危害国家安全活动的线索;
- (三)如实提供所知悉的涉及危害国家安全活动的证据;
- (四)为国家安全工作提供便利条件或者其他协助;
- (五)向国家安全机关、公安机关和有关军事机关提供必要的支持和协助;
- (六)保守所知悉的国家秘密;
- (七)法律、行政法规规定的其他义务。

任何个人和组织不得有危害国家安全的行为,不得向危害国家安全的个人或者组织提供任何资助或者协助。

公民和组织在维护国家安全中有哪些权利?

*公民和组织支持、协助国家安全工作的行为受法律保护。

因支持、协助国家安全工作,本人或者其近亲属的人身安全面临危险的,可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

*公民和组织因支持、协助国家安全工作导致财产损失的,按照国家有关规定给予补偿;造成人身伤害或者死亡的,按照国家有关规定给予抚恤优待。

*公民和组织对国家安全工作有向国家机关提出批评建议的权利,对国家机关及其工作人员在国家安全工作中的违法失职行为有提出申诉、控告和检举的权利。

*在国家安全工作中,需要采取限制公民权利和自由的特别措施时,应当依法进行,并以维护国家安全的实际需要为限度。

什么是12339?

“12339”是国家安全机关受理公民和组织举报电话。这条热线是由国家安全机关设立的,受理个人和组织发现的危害中华人民共和国国家安全的情况线索举报。



别让消费分期成为非法放贷的“挡箭牌”

一笔看似寻常的黄金买卖合同,背后竟暗藏环环相扣的非法放贷陷阱;一次“分期回购”的消费交易,实则是年化利率远超法定上限的高利贷……据媒体报道,伴随着贵金属投资和金饰品交易火爆,一种名叫“黄金分期”的业务趋势兴起,号称零首付、低利率,背后却暗藏非法借贷的风险,以消费为名,行放贷之实。

这类骗局的套路设计极具迷惑性。不法分子以“低门槛分期购”“无抵押快速变现”为诱饵,将黄金等易变现商品作为套现载体,刻意拆分交易环节,精准围猎征信存在瑕疵、难以正常贷款的人群。这些消费者往往被表面的低月供所吸引,却忽略了会员费、服务费等隐性成本。一旦签署协议,便落入精心编织的牢笼,陷入“借少还多”的债务陷阱。

这类骗局并非孤立的单次交易,而是一条精心谋划的完整产业链:从虚假宣传引流、设置合同陷阱,到后续的暴力催收、恶意提起司法诉讼,每个环节都经过周密设计,让消费者维权之路举步维艰。值得警惕的是,这种消费为名、放贷为实的骗局已悄然渗透多个领域。除黄金等贵金属交易外,在电商平台储值卡等高频流通商品交易中,类似套路屡见不鲜。

此类骗局中,不法分子利用消费者对分期产品的认知盲区,将非法放贷精心包装成“消费升级服务”,刻意模糊金融与消费的边界。更有甚者,凭借事先拟定的格式合同,在消费者无力偿还高额债务时,不法分子以买卖合同纠纷为由提起诉讼,利用表面合规的合同文本误导司法机关,企图通过法院判决强制消费者履行“霸王条款”。这种“以合法形式掩盖非法目的”的行为,不仅侵害消费者的权益,更是公然挑战司法公正,损害司法权威。

整治分期套路贷骗局,需要监管部门形成打击合力。一方面,应尽快明确界定消费分期与非法放贷的边界,加强对黄金、数码产品等高频涉案领域的监管排查力度,依法严惩无放贷资质却从事高利放贷的机构及个人;另一方面,应建立健全跨部门协同机制,打通市场监管、金融监管、司法机关之间的信息壁垒,实现信息共享、联动执法,从源头阻断骗局的产业链条,防止不法分子利用司法程序谋取不正当利益。

对消费者而言,务必擦亮双眼、提高警惕,增强自我保护意识。选择分期消费时,应仔细核验商家的资质,认真研读合同条款,远离“低月供、高隐性成本”的陷阱。更重要的是,一旦发现疑似套路贷行为,要及时留存合同文本、交易记录、沟通信息等证据,并第一时间向监管部门举报,通过合法途径维护自身合法权益。

消费分期本应是便利生活、促进消费的有效工具,绝不能成为非法放贷的“挡箭牌”。彻底撕开“黄金分期”骗局的伪装,更要严厉打击背后的非法放贷行为,让金融消费回归法治化轨道。唯其如此,才能切实保护消费者合法权益,维护金融市场秩序与司法公信力。

(据光明网)

让法治护航“人工智能+”行稳致远

工业场景下平均无故障工作时间突破1万小时、任务成功率超过99%。全国人大代表、小鹏汽车董事长何小鹏则聚焦加速人形机器人“端侧本地大脑”的部署,认为在本地部署具备自主感知、决策、执行能力的高阶人形机器人,更有利于在工业、商业乃至家庭场景中推广使用。

在医疗、教育等民生领域,人工智能同样大显身手。全国人大代表、好医生集团董事长耿福能在调研中发现,遇到疑难病例时,AI智能体助力基层医生查阅资料、辅助判断,进一步提升诊疗的准确性。

“人工智能+”是推动产业转型升级、形成新经济增长点的重要抓手。3月6日举行的十四届全国人大四次会议经济主题记者会上,传递出积极信号:我国将进一步深化“人工智能+”行动,赋能千行百业、服务千家万户,预计到“十五五”末,人工智能相关产业规模将增长到10万亿元以上。

“2026年将正式迈入‘百亿智能体时代’。站在‘十五五’开局之年,人工智能正由‘技术突破期’加速迈入‘产业落地期’。”全国政协委员、360集团创始人周鸿祎说。

侵权、算法偏见、深度伪造等潜在风险不容忽视——用户权益与信息安全保障迫在眉睫

技术的狂飙突进,从未能绕过安全的深水区。人工智能带来的侵权、算法偏见、深度伪造等风险,也给用户权益与信息安带来严峻挑战。今年全国两会上,这些问题成为代表委员关注的焦点。

随着人工智能深度参与生产生活,数据安全与隐私保护问题备受社会关切。全国人大代表、中兴通讯股份有限公司高级副总裁苗伟介绍,人脸机器人在仿生交互、表情模拟等领域取得突破的同时,也带来数据采集与存储环节风险突出、监管滞后于技术发展等挑战。在全国人大代表、海尔集团董事局主席周云杰看来,自动化决策、生成式人工智能等技术的滥用,已催生电信网络诈骗、知识产权侵害等社会问题。

内容生产领域同样面临挑战。全国政协

委员、知乎创始人周源指出,当前互联网中长期沉淀的高质量专业内容尚未得到充分利用,而版权争议频发等问题,不仅损害原创者权益,更制约了行业发展。

我国拥有丰富、活跃的移动互联网应用生态,这为“人工智能+”服务经济社会的方方面面提供了得天独厚的土壤。人工智能释放巨大赋能效用的同时,也给网络安全带来新挑战。

“人工智能带来的新风险主要归因于AI向‘超人化’演进。”全国政协委员、奇安信集团董事长齐向东认为,“AI超人”有超级权限、超级能力,它加剧了数据安全危机、安全“易攻难守”危机和网络安全“链式”危机。而周鸿祎直言,“黑客智能体”兴起,人工智能自身风险加剧,一旦与业务系统深度结合,可能带来更复杂的安全隐患。

来自公安系统的代表委员对此也十分关切。全国人大代表、黑龙江省大庆市公安局网络警察分局副局长贾晓亮认为,当前,人工智能给网络安全带来的新挑战,主要表现为攻击手段智能化、诈骗更逼真、更难识别;技术迭代快、应用场景复杂,新型违法犯罪层出不穷,传统监管模式难以有效覆盖。

全国人大代表、广东省佛山市公安局高明分局政委孙建国在调研时发现,人工智能逐渐深度融入群众日常生活,丰富消费场景,带来诸多便利,但也不能忽视其产生的风险。他介绍,当前利用人工智能实施诈骗的手段不断翻新,个人信息、企业数据易被非法抓取和滥用,群众难以辨别,传统防护手段应对吃力,证据提取难度大。

多位代表委员认为安全是发展的底线——呼吁加快完善人工智能法治化建设

面对机遇与挑战并存的人工智能新时代,多位代表委员认为:安全是发展的底线,必须加快完善人工智能法治化建设,实现“创新和安全的动态平衡”。

首场“部长通道”上,李乐成提到,“在人工智能产业发展当中,一定要统筹发展和安全,坚持人工智能为人所用、为人服务、为人所控。”这一信号,为人工智能发展指明“航向”。

“没有安全的创新走不远,也不稳。”齐向东认为,近年来大模型、智能体、具身智能等遭受的网络攻击来看,非常有必要有人工智能预设“安全护栏”。他建议,要把安全能力嵌入人工智能应用的全生命周期,做到纵深防御,明确合规红线,夯实安全主体责任,强化权限与内容管控,坚持“用AI对抗AI,让安全能力始终比安全风险快一步。”

全国政协委员、大湾区进出口商业总会会长龙安连续两年就“人工智能+”建言。今年,他从监管角度出发,提出完善人工智能发展规管体系,建议加快构建统一协调的立法与行业标准体系,推动监管从事后追责向全流程动态管控升级。

“人工智能的法治化治理是一项复杂而长期的系统工程。”全国人大代表、河北齐心律师事务所主任齐秀敏建议,将人工智能立法纳入立法规划,推动加快立法研究和立法进度,确立政府、企业、研究机构、用户等各方主体的基本权利和义务,建立涵盖研发、部署、应用、退出全生命周期的基本监管框架,并针对知识产权保护、侵权责任、算法治理等方面问题,采取制定单行条例、修改现有法律等方式快速响应。

来自公安执法一线的代表委员有着更为具体的思考。贾晓亮表示,公安机关要以“零容忍”的态度,坚决打击利用人工智能实施犯罪的行为,强化主动发现、精准打击,对相关案件做到快侦快破,形成有力震慑,切实维护人民群众的财产安全和数据权益。同时,公安、网信等部门要加强联动,推动数据安全、算法安全、内容安全一体化防护,构建起协同治理格局。

孙建国表示,公安机关要提升对深度伪造和智能攻击的实时识别、快速拦截能力,强化防范“AI诈骗”宣传。他呼吁广大群众不断提高对相关风险的识别能力和防范意识,共同筑牢反“AI诈骗”安全防线。在建言献策和交流讨论中,代表委员逐渐形成共识:抢抓发展机遇,必须筑牢安全底线,以法治的确定性应对技术风险的不确定性,让“人工智能+”行稳致远,让智能经济新形态更好赋能千行百业、服务千家万户。

(据学习强国)