

生成涉企不实文章,姚某未经核实即在其10余个自媒体账号发布,全网浏览量迅速上涨,引发网民对该茶饮企业的质疑。另一嫌疑人陈某为推广其人工智能培训课程,将网络传言用人工智能工具“洗稿”后交由好友赵某发布,其余嫌疑人也分别通过人工智能洗稿、盲目转载等方式参与造谣,以达到引流、涨粉等目的。姚某等8人被公安机关依法采取刑事强制措施。

网络时代,类似事件并不鲜见。像为“珠峰装电梯”“长城贴瓷砖”“黄河设玻璃护栏”等,是近几年出现的典型的网络谣言,网传图文视频为人工智能生成的虚假信息,内容虽然荒唐,但因传播广泛,官方不得不紧急辟谣,提醒网民切勿相信此类谣言。“人工智能生成不实信息,到底应该怎么办?”这一疑问指向的正是人工智能的健康发展问题。以生成式人工智能为例,在收集、处理并生成敏感信息时,极易引发侵犯隐私、泄露数据等新型风险。人工智能治理语境中,如何在促进科技创新与安全风险防范间寻求平衡成为破题关键。

《中华人民共和国网络安全法》施行八年迎来首次修改,人工智能被正式纳入法条。其中明确规定,国家支持人工智能基础理论研究和算法等关键技术研发,推进训练数据资源、算力等基础设施建设,完善人工智能伦理规范,加强风险监测评估和安全监管,促进人工智能应用和健康发展。国家支持创新网络安全管理方式,运用人工智能等新技术,提升网络安全保护水平。

### 亮点2

#### 网络运营者对用户信息须严格保密

近期,国家计算机病毒应急处理中



资料图片

心检测发现,71款App存在违法违规收集使用个人信息情况,有的在首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则;有的隐私政策未逐一列出(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等;还有的未征得用户同意就开始收集个人信息或打开可收集个人信息的权限。近年来,个人信息安全问题层出不穷:线上招聘平台将公民简历信息违规提供给他人;医院的云端问诊系统因存储服务器未开启加密保护,导致问诊数据泄露;犯罪团伙勾结快递行业工作人员,窃取个人信息并出售牟利……如今,个人信息保护机制遭遇多重风险,部分App成“隐私刺客”,威胁公众的人身和财产安全。

在此背景下,新修改的网络安全法第四十二条新增条款,强调网络运营者负有对其收集的用户信息严格保密的义务,并建立健全用户信息保护制度。

此外,第四十三条规定再次对网络运营者收集和使用个人信息划定了红

线,即网络运营者收集、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。

此次网络安全法修改加强了与民法典、数据安全法等相关法律的有机衔接,旨在避免因概念交叉、责任竞合等导致数据和个人信息保护空白。对于社会公众而言,如果发现App违规收集、处理个人信息时,进行维权的法律依据更加明确,新法通过法律层面明确权益保障,为网络安全筑牢屏障。

### 亮点3

#### 为严重违法设定更高处罚标准

近日,湖南某科技公司工作人员将大量用户数据拷贝至企业内网数据库,并打开企业内网的公共互联网访问端口,导致相关数据大规模暴露。网络运营者是网络危险源开启与控制的责任主体,实践中因网络运营者建立网络安全和数据安全管理制度不完善、未采取