# 人大代表呼吁治理AIGC乱象

▶ 孙立彬

人工智能生成技术（AIGC）的浪潮席卷全球，在内容生产方面，其正以前所未有的效率重构传统的运行规则，文、视、图、声等合成和制作门槛大幅降低。与此同时，由于人工智能（AI）幻觉、恶意传播与法律法规滞后等诸多因素并存，致使生成式内容的制作和传播处于混乱状态。

今年全国两会期间，代表委员敏锐注意到上述问题，就打击AIGC虚假信息、完善AI视频传播管理机制等思考提出建议。

## 他们都看到了什么

全国人大代表、科大讯飞董事长刘庆峰表示，生成式人工智能存在幻觉，特别是深度推理模型逻辑自洽性的提升，使得AI生成内容真假难辨。带有算法偏差的虚假信息会被新一代AI系统循环学习，形成恶性循环，影响公众信任和社会稳定。

全国人大代表，美的集团党委副书记、集团副总裁兼首席财务官钟铮注意到，随着目前AI技术的快速发展，视频合成和制作门槛大幅降低，导致网络上出现大量AI生成的视频内容真假难辨，且成为一种常态。在一些视频中，有的模仿明星或专家的形象声音进行传播，有的则虚构人设，用于推销产品，误导消费者购买不必要的商品，以至产生信任危机；还有一些视频通过流量变现，进一步加剧这一类乱象愈演愈烈。

全国人大代表、TCL创始人、董事长李东生表示，随着生成式人工智能技术的发展，深度伪造技术快速发展，而一旦被不法分子利用，可能会导致新的社会问题。近年来，我国相关立法对这一议题虽有关注，但已出台的规章制度不成体系，尚不具备可操作的细则和明确的处罚标准。

关于深度伪造问题，全国人大代表、小米集团董事长兼CEO雷军也非常关注。他表示：“‘AI换脸拟声’不当滥用造成的违法侵权行为已成为重灾区，易引发侵犯肖像权、侵犯公民个人信息以及诈骗等违法行为。AI深度合成技术所需素材获取便利、技术使用门槛低、侵权主体及其手段隐蔽性强等特点，给治理带来较大挑战。”

## 他们建议这样解决

针对AI幻觉问题，刘庆峰建议构建安全可信数据标签体系，提升内容可靠性：建立安全可信、动态更新的信源和数据知识库，对不同类型数据的可信度和危害程度建立标签体系，降低人工智能幻觉出现概率，提升生成内容可靠性；同时研发AIGC幻觉治理技术和平台，定期清理幻觉数据，研究幻觉自动分析的技术和软件平台，开展幻觉自动分析、AIGC深度鉴伪、虚假信息检测、有害内容识别以及互联网传播溯源，由相关部门定期清理幻觉数据，为公众提供AIGC幻觉信息检测工具与服务。

对于AI生成视频的传播，钟铮建议，一是完善法律法规体系，加强原创版权和隐私保护；二是探索利用AI技术审核AI合成的视频内容，确保视频传播内容审核的效率与准确性；三是进一步加强行业自律与政府监管，对违法违规行为进行严厉惩治，督促行业健康发展。

李东生认为，要规范对于这一新兴技术的不当利用行为，有必要要求深度合成服务提供商对人工智能生成的内容进行强制标识，减少恶意滥用，并厘清责任、对违法犯罪行为追责。

李东生建议：第一，加快人工智能深度合成内容标识管理规章制度的出台。第二，明确对人工智能深度合成服务商未履行标识义务的惩罚制度。完善对深度合成内容服务提供商未按要求进行标识的行为界定、分类细则，以及相应的处罚标准。第三，加强深度合成内容标识技术标准和发布的管理。出台深度合成内容标识的技术标准，保障标识的有效性。此外，对相关内容平台提出要求，用户在发布深度合成的视频、音频等内容时，有义务对其进行标识。第四，加强国际合作，形成人工智能生成合成内容的有效监管。

雷军建议，首先，应加快单行法立法进程，在安全与发展并重的基础上提升立法位阶；其次，强化行业自律共治，压实平台企业等各方的责任和义务；第三，加大普法宣传的广度力度，增强民众的警惕性和鉴别力。

两会声音

全国人大代表伊彤：

## 加强人工智能安全风险防范体系建设

**本报讯（记者 李洋）**今年全国两会期间，全国人大代表、北京市科学技术研究院创新发展战略研究所所长伊彤呼吁，既要大力推动人工智能技术发展和产业赋能应用，也要重视人工智能安全技术的发展，统筹规划建设能够覆盖多领域的人工智能安全风险防范体系，以提升对新兴技术安全风险的防范应对能力，确保人工智能发展安全、可靠、可控。

伊彤的建议为如下3点：

一是制定完善人工智能安全监管法律法规和相关标准。强化人工智能安全监管顶层设计，加快人工智能领域立法进程，明确人工智能技术研发、使用、治理应遵循的法律法规。推动制定人工智能相关国家和行业标准，全面规制安全风险，倒逼人工智能产业高质量发展。

二是建立健全人工智能安全监管制度。严格人工智能工具、软件监管治理，对人工智能技术生成合成他人音频、视频的功能进行限制和管理，对人脸驱动、声音克隆相关算法的传播进行严格监管。压实网络平台管理责任，加强人工智能生成合成内容的标识管理，加大传播受众群体提示提醒力度，避免群众发生误判情况。

三是强化模型安全防范核心技术攻关。统筹推进规范化、标准化、精细化人工智能风险防范技术能力体系建设，大力推动人工智能安全相关技术革新，加强人工智能有害信息感知发现、内容检测，人工智能模型安全评估、漏洞检测防御等技术攻坚，全面提升安全风险预警防范及应对处置能力。

全国政协委员齐向东：

## 提升人工智能安全防御能力

**本报讯（记者 张伟）**今年全国两会期间，全国政协委员、全国工商联副主席、奇安信科技集团董事长齐向东提出，随着人工智能技术的深度应用，大模型所面临的安全挑战也日益严峻，由此需提升安全防御能力。

“作为网络和数据安全领域从业者，保障人工智能时代的网络空间安全是扛在我们肩上的重任。因此，我期待能够用一些切实可行的举措，为人工智能安全发展贡献力量。”齐向东说。

对此，齐向东提出3个方面的针对性建议：建立适配大模型的纵深防御体系，筑牢人工智能的安全根基；制定大模型安全强制合规要求，夯实人工智能安全发展的制度保障；推广“AI+安全”创新成果落地，走好提升安全能力的必经之路。

齐向东还希望出台大模型网络数据安全强制合规要求方面政策，对企业做好人工智能时代的安全防护工作给予清晰指引；鼓励产业内定期开展网络和数据安全“体检”，帮助企业进行安全能力的查漏补缺，实现安全能力的持续提升；设立专项基金促进“AI+安全”创新成果落地，推动各领域头部企业与专业的网络安全企业开展联合创新，提升智慧城市、智慧能源、智慧金融等新兴场景的安全防护效能。

全国政协委员周鸿祎：

## 人工智能安全需要“以模制模”

**本报讯（记者 张伟）**今年是全国政协委员、九三学社中央委员、360集团创始人周鸿祎第8年参加全国两会。今年，周鸿祎关注的依然是网络安全和人工智能两个领域。

今年农历春节期间，DeepSeek异军突起成为AI发展史上的重要里程碑。周鸿祎表示，DeepSeek作为基座模型，存在着幻觉、提示注入攻击等问题。“当大模型渗透率提升时，应用安全问题也迫在眉睫。”

“传统网络安全已经无法应对新挑战，建议应由既懂安全又懂AI的企业牵头，以模制模，通过打造安全大模型解决大模型的应用安全问题。”周鸿祎说。

周鸿祎认为，传统行业纷纷进行数转智改背景下，网络安全和大模型安全问题日益凸显。越来越多的企业开始打造自己的安全体系。但一直以来，我国安全行业内卷严重，很多厂商只是一味地卖硬件软件，客户无法得到想要的安全服务，致使行业面临普遍性经营困境，造成客户和厂商双输的局面。

“建议相关部门从政策上支持采购安全服务，特别是鼓励采购SaaS化安全服务，实现安全的普惠。”周鸿祎说。