

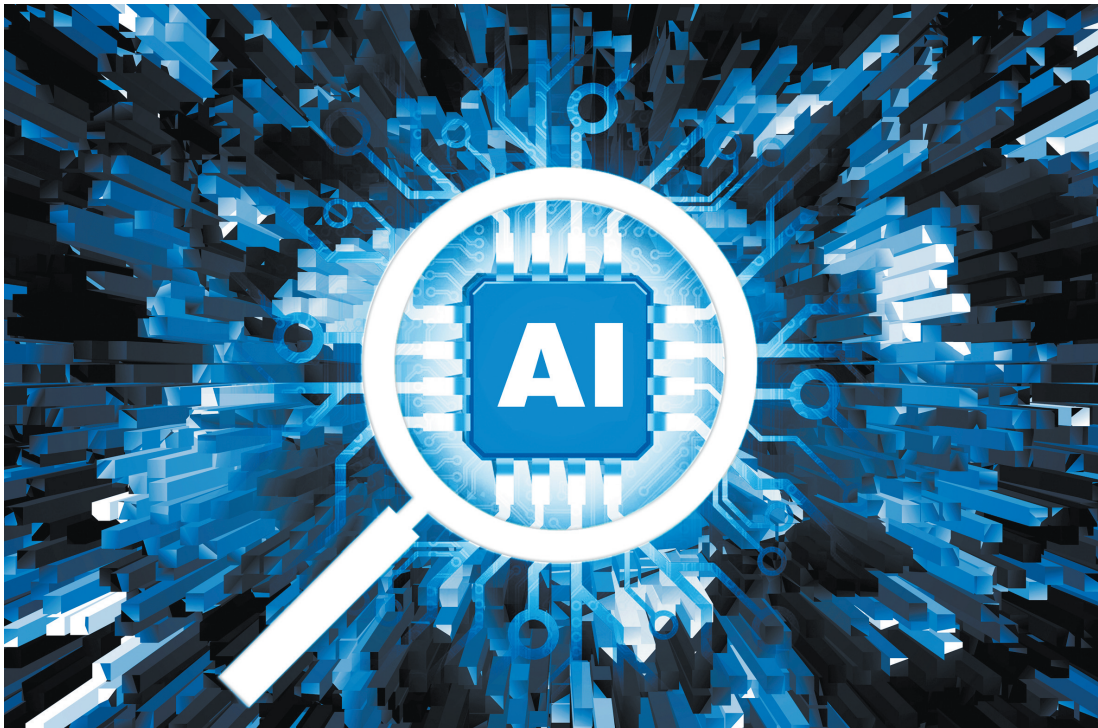
欧盟宣布扩大实施《人工智能法》

8月2日,欧盟《人工智能法》的透明度规则与通用人工智能模型监管条款正式启动实施。这标志着这部全球首部综合性人工智能监管法案,从纸面规则全面转向实际执法阶段,也意味着所有面向欧盟用户提供服务的AI产品,都必须完成一次面向公众的“自报家门”。从聊天机器人主动亮明AI身份,到深度伪造内容强制添加双轨标识,再到通用大模型接受系统性风险监管,欧盟此次落地新规,正在为全球AI治理划出一条清晰的“信任底线”。

从“隐身”到“现身”

在过去很长一段时间里,AI产品的“拟人化”曾被视为核心竞争力。不少聊天机器人、AI客服、虚拟陪伴产品,刻意模糊自身的非人类属性,通过模仿人类语气、隐藏系统提示,让用户误以为正在与真人对话。这种设计在提升用户体验的同时,也为大量欺骗、操纵行为埋下了隐患:从伪装成亲友的AI语音诈骗,到冒充客服诱导转账的AI对话,再到利用AI虚拟人进行的虚假营销,AI的“隐身”状态,正在不断击穿数字世界的信任基础。

欧盟此次落地的透明度规则,首先瞄准的就是这一核心痛点。根据新规要求,所有面向公众提供服务的交互式人工智能系统,必须在交互启动的第一时间,以清晰、显著、不可跳过的方式告知用户:你正在与人工智能系统互动,而非人类。这一要求覆盖的范围远



不止大众熟悉的通用聊天机器人,还包括各类AI客服系统、AI在线陪聊、AI虚拟主播、教育场景下的AI辅导助手等所有具备对话交互功能的AI产品。这意味着,未来欧盟用户打开任何一款AI对话工具,首先看到的不会是精心设计的欢迎语,而是明确的AI身份声明,从根源上切断AI“伪装成人”的可能性。

为了避免企业通过“小字提示”“角落弹窗”等方式规避义务,欧盟在此前发布的透明度实施指南中,进一步细化了执行标准。这些细致的执行标准,让“AI亮明身份”从一句原则性要求,变成了可落地、可核验的刚性规则。

这一规则的落地,正在彻底改变AI交互的底层逻辑。过去企业比拼的是“AI有多像人”,现在合规的底线变成了“AI必须明确不是人”。这种转变并非对AI技术的限制,而是把知情权完完整整交还给了用户。从这个角度看,强制AI“现身”,本质上是在AI与人类之间建立起一道清晰的“信任防火墙”。

从“无迹”到“可查”

如果说AI亮明身份是对交互环节的信任保护,那么深度伪造内容的强制标识规则,就是对整个数字内容生态的信任加固。近年来,AI生成内容技术的爆发式普及,让普通人只需要几秒钟就能生成一段足以以假乱真的伪造视频、音频或图片:一段伪造的公众人物发言音频,几小时内就能在社交平台引发舆论风暴;一张AI生成的虚假新闻现场图片,很容易被当成真实事件广泛传播;甚至一段合成的亲友求助视频,就能直接突破受害者的心理防线完成诈骗。这些AI生成的内容,过去大多处于“无迹可查”的状态,普通用户很难仅凭肉眼分辨真假,监管部门的溯源核验也面临巨大障碍。

欧盟此次同步生效的新规,针对AI生成或深度修改的图像、视频、音频内容,建立起

了“显式标识+机器可读标记”的双轨强制机制。所谓显式标识,就是所有AI生成或经过AI深度编辑的内容,必须在内容画面的显著位置添加清晰的“AI生成”提示,视频内容的标识不能被后期剪辑裁剪掉,音频内容也要在开头或结尾加入明确的语音提示,让普通用户第一眼就能识别出内容的AI属性。而机器可读标记,则是嵌入内容文件元数据、数字水印中的特殊标识,普通人肉眼无法看见,但所有支持核验的工具、平台都能快速读取,哪怕内容被二次截图、二次剪辑,这些底层标记也不会被轻易抹除。

这套双轨标识机制,覆盖了AI内容的生成、传播全链条:生成端的AI绘画、AI视频工具,在内容输出时必须自动完成双轨标识的添加,不能给用户提供“关闭标识”的选项;传播端的社交平台、内容网站,必须建立AI内容检测机制,对平台内上传的未标识AI生成内容,要自动补充提示,不能放任无标识的深度伪造内容直接传播;即便是用户自己用AI生成的私人内容,只要在欧盟境内的公共平台发布,也必须遵守标识要求,恶意删除、伪造AI标识的行为,都属于违规。

为了让这套机制真正落地,欧盟此前已经联合180多家全球主流科技企业、内容平台,共同签署了《人工智能生成内容透明度行为准则》,谷歌、微软、OpenAI、亚马逊等头部企业都在首批签署名单中。

从“放任”到“约束”

在透明度规则之外,欧盟此次同步启动的通用人工智能模型监管,是此次新规落地的另一核心看点。随着大模型参数规模不断突破,能力边界不断拓展,部分先进通用大模型已经具备了生成大量有害内容、发起自动化网络攻击甚至被大规模用于操纵公众认知的能力,这类模型带来的已经不是单个产品的使用风险,而是可能影响整个社会的系统

性风险。过去这类风险大多处于监管空白地带,模型提供商的安全约束完全依赖企业自律,一旦出现安全漏洞,很容易引发跨领域的大规模危害。

根据欧盟新规要求,从8月2日起,欧洲人工智能办公室正式获得对通用人工智能模型提供商的监管权限。所有在欧盟境内提供服务的通用大模型,都必须完成完整的模型安全文档备案,向监管部门披露模型的训练数据来源、版权情况、安全评估报告;而经过判定可能产生系统性风险的先进通用大模型,还需要履行额外的特殊义务:模型上线前必须完成全维度的安全测试,防范模型失控生成极端有害内容的风险;建立实时监测机制,及时拦截模型生成的网络攻击代码、恶意操纵话术等危险内容;针对可能出现的大规模滥用场景,提前制定应急响应方案,一旦出现风险,能在最短时间内切断影响。

值得注意的是,欧盟为这套监管体系预留了清晰的缓冲空间,考虑到高风险AI系统涉及招聘、教育、执法、医疗等大量民生关键领域,直接全面落地可能给企业和公共服务带来过大冲击,欧盟通过“综合简化一揽子计划”,将这类高风险AI系统的合规义务推迟到2027年12月适用,嵌入医疗器械、工业机械等实体产品中的AI系统,更是延后到2028年8月才正式执行。这种“先易后难、先轻后重”的分阶段落地节奏,既先把公众最急需的透明度规则落到实处,也给企业留下了充足的技术改造、流程适配时间,避免了监管与产业发展的对立。

有关分析认为,欧盟此次《人工智能法》透明度规则的落地,是全球AI监管史上的里程碑事件。它没有选择“一刀切”限制AI技术发展,也没有放任AI在无约束的环境下野蛮生长,而是从最基础的“身份透明”“内容可查”切入,用清晰、可执行的规则,在AI创新与公众利益之间找到了平衡点。

北京商报综合报道

聚焦

今年一季度全球商品贸易增长超预期

7月31日,世界贸易组织正式发布一季度全球商品贸易监测报告,一组超出市场普遍预期的数据,为原本笼罩在地缘冲突阴影下的全球贸易图景注入了鲜明的亮色。经季节调整后,2026年第一季度全球商品贸易量环比增长1.9%,同比增长3.2%;按价值口径统计,全球商品贸易环比增长2%,同比大幅攀升11%。这一表现打破了此前多数机构对一季度贸易增速不足1%的悲观预判,而支撑这份韧性的核心动力,正是同比增长超40%的人工智能相关电子元件贸易——这股新兴产业的强劲势能,直接抵消了2月底中东战事爆发带来的多重负面冲击,让全球贸易在不确定性中走出了一条超出预期的增长曲线。

回溯一季度的全球贸易环境,2月底突发的中东战事曾给市场投下浓重的阴霾。作为全球能源运输的核心枢纽,霍尔木兹海峡承担着全球近三分之一的海运石油贸易量,战事爆发后,海峡航运安全风险陡增,部分航线被迫临时绕行,国际能源价格在短短两周内出现两位数涨幅。这一变化直接推高了全球燃料净进口国的生产与物流成本,不少依赖能源进口的新兴经济体一度下调了该季度的经济增长预期,全球供应链的脆弱性再次暴露在市场面前。世贸组织在报告中坦言,若按照传统贸易结构测算,仅中东战事带来的运输中断和能源价格上涨,就可能让一季度全球商品贸易量同比增速回落至1%以下,远低于最终公布的3.2%实际增速。

而填补这一增长缺口甚至拉动整体贸易表现超预期核心变量,正是异军突起的人工智能相关电子元件贸易。数据显示,2026年第一季度,全球以美元计价的AI相关产品贸易额同比增长超过40%,涵盖高端算力芯片、AI存储模组、智能传感器、高速光模块等核心品类。这一轮增长并非短期脉冲

式行情,而是全球AI产业进入规模化落地阶段的必然结果:从北美科技巨头持续加码的算力基础设施建设,到亚洲制造业工厂大规模部署的工业AI系统,再到欧洲各国加速推进的智慧城市项目,全球范围内对AI硬件的需求在一季度集中释放,带动相关电子元件的跨境流量创下近年新高。

从区域贸易表现来看,AI相关贸易的拉动效应在亚洲市场体现得尤为突出。一季度亚洲地区出口量和进口量同比分别增长12.9%和14.6%,远高于全球平均水平,中国、新加坡、韩国、泰国等经济体成为这一轮增长的核心推动者。作为全球电子产业链的核心聚集地,亚洲经济体在AI硬件的研发、制造和流通环节形成了高度协同的产业网络:韩国的存储芯片、中国的AI服务器整机、新加坡的半导体分销、泰国的传感器封装,依托区域内成熟的贸易协定和跨境通道,形成了高效的产业内循环,让AI相关商品在区域内的流通效率大幅提升,直接推高了整个亚洲的进出口增速。与之形成对比的是北美市场,一季度北美出口同比增长7%,但进口同比下降10.7%,这一结

构性分化也侧面反映出,AI相关产业的贸易红利,正在向具备完整电子制造产业链的区域集中。

值得注意的是,这一轮AI驱动贸易增长,正在重塑全球贸易的增长逻辑。过去很长一段时间,全球商品贸易的增长动力高度依赖能源、大宗商品和传统消费品的流通,地缘冲突往往直接通过能源价格传导至全产业链,很容易引发整体贸易增速的大幅波动。但2026年一季度的表现证明,以AI电子元件为代表的高附加值、高技术密度产品,正在成为新的“贸易稳定器”:这类产品的单位价值高、供应链韧性更强,且需求来自全球数字化转型的长期刚性需求,不会因短期地缘冲突出现大幅萎缩。这种结构性变化,也让全球贸易的抗风险能力得到了前所未有的提升。

不过世贸组织也在报告中发出了审慎提醒,当前的超预期增长并不意味着后续贸易环境将一路向好。一季度中东战事的影响仅在最后一个月逐步显现,大量霍尔木兹海峡的航运中断效应尚未完全体现在贸易数据中,世贸组织预计二季度的贸易数据将更全面地反映出地缘冲突带来的后续冲击。与此同时,部分经济体推行的碎片化贸易政策、不断高企的关税壁垒,也可能给全球AI产业链的跨境流通带来新的阻碍。对于全球各国尤其是深度嵌入AI电子产业链的新兴经济体而言,如何抓住这一轮AI贸易的增长窗口,进一步巩固自身在产业链中的优势地位,同时做好风险对冲,将是未来一段时间把握贸易增长主动权的关键。

北京商报综合报道

· 图片新闻 ·

美签证保证金将涨价并长期化



美国国务院外景。视觉中国/图

美国《联邦政府纪事》于7月31日以上预告形式发布公告,正式宣布美国国务院将原本处于试点阶段的签证保证金制度长期化,覆盖范围扩展至50个国家的公民,部分申请者最高需缴纳2万美元保证金才能获得B1、B2类赴美签证。这一政策调整将于8月3日在《联邦政府纪事》正式刊登后即刻生效,迅速引发全球跨境出行市场的广泛关注。

根据公告内容,新规主要面向以商务活动、休闲旅游为目的申请美国B1、B2类非移民签证的人员。在实际审核流程中,美国领事官员将结合申请人的出行记录、资产状况、过往赴美合规情况等维度进行综合评估,有权将缴纳对应档位的保证金作为签发签证的附加条件,申请人完成缴费后才可进入后续贴签环节。

值得注意的是,在2025年8月启动的“签证保证金试行计划”阶段,美国官方将保证金设置为5000美元、1万美元和1.5万美元三档梯度。而本次落地的长期化新规中,不仅直接取消了门槛最低的5000美元档位,还将最高缴纳标准从1.5万美元上调至2万美元,整体缴费门槛出现明显抬升。按照规则,申请人正常缴纳保证金并

顺利入境美国后,只要全程遵守签证条款要求,在停留期届满前按时离境,即可申请全额退还保证金;一旦出现逾期滞留、违规务工等违反条款的行为,这笔保证金将被直接没收不予返还。

美国国务院在公告中强调,经过近一年的试点运行,已积累的“充分数据”能够证明,保证金制度是倒逼签证持有者严格遵守停留规定的“有效措施”,能够显著降低非移民签证的逾期滞留率,强化美国的边境管理效率。

但不少美国本土媒体和旅游行业协会对此持谨慎态度。分析指出,2万美元的保证金折合人民币约十余万元,对于普通出行群体而言是一笔不小的资金占用,大量潜在申请者会因无法承担这笔临时资金压力直接放弃赴美行程。在本次政策覆盖的50个国家中,有30个位于非洲,其余部分分布在亚洲和拉美地区,这些区域近年来正是美国入境旅游增长最快的新兴市场。依赖国际游客消费的洛杉矶、纽约、迈阿密等热门旅游城市,当地的酒店、免税零售、景区交通等相关产业都可能因国际客流下滑受到直接冲击,原本处于复苏通道的美国入境旅游业或将迎来新的不确定性。北京商报综合报道