

拥抱“人工智能+”，安全科技是“方向盘”

青岛财经日报/首页新闻讯 当“人工智能+”首现政府工作报告,“人工智能”话题就变得格外火热。从2015年提出的“互联网+”到2019年提出的“智能+”,它们在不同阶段推动了产业的转型升级。如今,随着大模型等人工智能技术成为引领新一代产业变革的核心力量,政府工作报告中首次提出的“人工智能+”行动,不仅顺应了全球AI发展的潮流,更与中国产业升级的大势紧密相连。这一行动无疑将为人工智能技术在各行业的广泛应用开启新篇章。



“人工智能+”加的是什么？

不难发现,这两年人工智能的地位确实“不一样”。从热搜上数,ChatGPT、文心一言、Sora等人工智能模型频频霸榜;往朋友圈里瞧,AI报表、AI相机、AI主播多了不少。从中央层面观察,为生成式人工智能服务“立规矩”,召开“AI赋能产业焕新”专题推进会,旨在加速布局、审慎推进;从地方动作来看,多地出台新一代人工智能发展规划,广东在“新春第一会”上专门强调人工智能,足见其重要性。业界更是普遍认为,具有前沿性、颠覆性的人工智能技术,将改变各行各业的面貌,成为新一轮科技革命和产业变革的关键动力。

事实上,我国人工智能产业的发展已驶入快车道。中国信息通信研究院公布的数据显示,2023年我国人工智能核心产业规模达5784亿元,增速13.9%。工业和信息化部赛迪研究院数据显示,2023年,我国生成式人工智能的企业采用率已达15%,市场规模约为14.4万亿元。迅猛的发展态势和广阔的市场空间,为“人工智能+”行动的顺利实施奠定了坚实的基础。

不仅如此,人工智能技术在多个领域的创新应用也取得了显著成果。前不久,国家自然科学基金委员会公布的“2023年度中国科学十大进展”中,“人工智能大模型为精准天气预报带来新突破”位列第一。利用人工智能大模型可以在10秒内完成全球7天重要气象要素的预报,比现有的数值预报方法快了超过1万倍——这种惊人的效率提升,不仅展示了人工智能技术的巨大潜力,也为“人工智能+”行动提供了生动的案例。

“人工智能+”,“+”的是什么?在全国人大代表、小米集团创始人、董事长雷军看来,“+”就是“+

各行各业”以及“+各种应用场景”,把人工智能有效应用到国民经济的方方面面。

“+”意味着人工智能技术与经济社会生活的深度互动,与各领域的有效融合。通过人工智能来支撑各行业应用创新,赋能百业智能化转型升级。简而言之,“+”是生产效率的提高,是创新活力的激发,是产业生态的重塑。

可见,为引领未来的战略性技术,“人工智能+”是新一轮科技革命和产业变革的核心驱动力,才被普遍确认为新质生产力的典型代表和重要引擎。

警惕技术双刃剑

不过,随着ChatGPT、Sora等大模型的开放和应用,AI生成技术使用的门槛持续降低,也进一步增加了各界对人工智能安全与合规的担忧。网络安全公司Darktrace报告显示,ChatGPT这样的生成式AI导致网络钓鱼邮件攻击增长135%。

此外,“深度伪造”技术利用机器的深度学习,实现了图像、声音、视频的篡改、伪造,可产生高度逼真且难以辨识的内容,对公众认知和判断造成严重干扰。

记者从一家权威机构处获悉,过去两年其开展了人脸识别安全评测情况统计。数据显示,多家机构产品首次送检突破概率高达71%,二次突破概率也有25%。

“历史经验表明,越是先进的东西,出现安全事故带来的损失和影响就越大。数字工厂出现网络安全事故,损失远远大于传统工厂。”全国政协委员、奇安信董事长齐向东表示。

在他看来,人工智能带来了三大挑战:一是AI投毒安全隐患加重,攻击者可以通过在训练数据中

开展“人工智能+”行动,这些领域有望率先“动起来”

2024年国务院政府工作报告中多次提到人工智能,并提出开展“人工智能+”行动。对于“人工智能+”行动,多位全国政协委员和人工智能相关企业认为,“人工智能+场景创新”“人工智能+算力基础”“人工智能+法治建设”有望率先“动起来”。

人工智能+场景创新 推动大模型与数字化系统融为一体

我国人工智能技术快速发展,数据和算力资源日益丰富,应用场景不断拓展,为开展人工智能场景创新奠定了坚实基础,当前人工智能技术已经在医疗保险、交通运输、智能制造、智能家居、教育等领域广泛运用。

全国政协委员、上海移动总经理陈力对记者表示,要明确我国人工智能所要解决的技术、社会和经济发展等问题,在此基础上锚定我国人工智能的发展模式和方向。明确人工智能产业发展规划布局,集中资源投入上游基础层企业,解决中高端人工智能产品自主供应能力不足的问题。提升我国人工智能主管部门与其他部门的联动,自上而下地激发人工智能与各行各业的融合活力。

全国政协委员、360集团创始人周鸿祎在接受记者采访时表示,中国发展人工智能大模型的一个重要方向是借助产业和场景的优势,将大模型与业务流程、产品功能相结合,寻求多场景应用、垂直化和产业化的落地。

昆仑万维董事长兼CEO方汉向记者介绍,在交通物流行业,人工智能技术应用可以助力企业提升运输效率,降低全社会物流的成本;在文化旅游行业开发文化大模型,能够贯通各类文化机构的数据中心,充分挖掘文化数据的价值;在科技创新领域以科学数据支撑大模型的开发,可以更深入地挖掘各类科学数据和科技的文献应用。

人工智能+算力基础 建立全国一体化算力大市场

从ChatGPT到Sora,从单模态到多模态,从单一智能到通用智能,人工智能大模型技术正在引领新一轮全球人工智能创新热潮,同时,大模型计算也带来了智能算力需求激增,随着“东数西算”工程推进,去年以来全国多地掀起了智算中心建设热潮。

全国政协委员、天娱数科副总经理、山西数据流量生态园董事长贺晗在接受记者采访时表示,需要鼓励引导市场主体建设区域级、行业级、企业级等多层次智算聚合服务平台、算力并网平台,广泛汇聚多方算力资源,整合闲置算力,特别是各地政

府主导建设智算资源,实现多地算力资源的共享和最优利用,减少投资浪费,增加有效供给。

贺晗提出,健全算力调度标准规范体系,为算力资源供给方提供能力自查参考,同时为算力需求方提供算力调度能力使用参考,引导新建算力资源按统一标准建设及接入。

全国政协委员、中国信息通信研究院院长余晓晖对记者说,要发挥全国超大规模市场优势,利用互联网发展成功经验,以算力先互联、再成网、构建大市场为主线,基于统一标识符实现多样性算力互联感知,通过弹性网络能力和标准化架构接口实现业务和数据流动互通,进而打造智能感知、高速弹性、安全绿色、先进普惠的算力互联网。

人工智能+法治建设 确保人类“守法”、机器“守德”

去年7月份发布的《生成式人工智能服务管理办》,促进生成式人工智能健康发展和规范应用;去年10月份发布的《全球人工智能治理倡议》,围绕人工智能发展、安全和治理三个方面系统阐述了人工智能治理的中国方案。

全国政协委员、陕西省高级人民法院副院长巩富文表示,应当以《全球人工智能治理倡议》为指引,全面整合相关法律、法规,形成“中国特色”人工智能伦理指南,建立科技伦理审查及负面清单准入、分级分类管理、协同监管等制度,确保人类“守法”、机器“守德”。

巩富文建议设立新型财产权——“人工智能生成物著作权”,认定其权利主体为人工智能生成程序的使用人,不仅可以明确生成物法律地位和归属,推动其进入相关产业链、价值链,激励人工智能生成物的创作传播和产业投资,还可以为侵权责任认定打下良好基础,降低人工智能生成物对现有创作市场的冲击,以达到激励人工智能生成物的生产传播与公共领域保留相平衡的目的。

全国政协委员、金杜律师事务所高级合伙人张毅对记者表示,应该尽快推进《人工智能法》的制定和出台,以《人工智能法》及配套的监管工具为核心,形成完整的人工智能技术法律体系。

全国政协委员、南方科技大学副校长金李对记者表示,我们在消费过程中,逐渐从现金支付到手机二维码支付,再到人脸识别支付,科技让我们的生活变得更加便捷高效,但这背后也面临着身份信息泄露和隐私安全风险,在科技的便利性和隐私保护之间,需要法律与监管尺度进行平衡,人工智能等新一代信息技术的发展,带来更多新的商业模式和应用创新,相关法治建设也要与时俱进。

据《证券日报》郭冀川 张敏 周尚仟/文

加入精心构造的异常数据,破坏训练数据集的准确性;二是数据篡改隐患加重,AI的大规模内容生产能力可能产生真假难辨的信息,控制社交软件乃至媒体的舆论声音,激化意识形态矛盾;三是数据泄露隐患加重,在向人工智能投喂数据的过程中,也会产生商业机密泄露问题,进而导致企业丧失核心竞争力。

上述挑战也引发学界关注。中国社会科学院大学数字中国研究院近期发布的《数字时代安全科技价值报告》(以下简称《价值报告》)将AI安全风险分为三类:第一类是人工智能系统内部所产生的“内生安全问题”,如“数据有毒”“价值对齐”“决策黑盒”等问题;第二类是“衍生安全问题”,比如生成假新闻、深度合成伪造进行诈骗或钓鱼攻击,涉及隐私保护、国家安全、伦理道德等与社会治理有关的挑战性问题;第三类是“外生安全问题”,即面向人工智能系统的外部网络攻击对抗。

中国社会科学院大学数字中国研究院执行院长吕鹏认为:有新技术的地方,就有新的安全风险,两者是不可分割的伴生关系。人工智能作为最具颠覆性和战略性的核心关键技术,能够帮助各行各业在数字化的基础上进一步实现智能化,成为未来的发动机。而安全科技将作为方向盘,始终将各种新兴科技控制在向善的道路上。

事实上,上述安全科技的提法与2024年政府工作报告中“人工智能+”与“提高网络、数据等安全保障能力”的表述不谋而合。

《价值报告》认为:安全已成为AI产业发展的核心要素,安全科技具有“压舱石”与“助燃剂”的双重价值。“压舱石”指的是守住技术的安全底线,防御外部风险隐患,让技术“难作恶”,支撑数字社会稳步运行。“助燃剂”体现在提高技术的安全上限,降低技术运行的成本,让产业焕发新机,让更多人受益。

但需要看到,当前市场对于人工智能的安全治理以及“以技治技”能力还需持续探索。

中国信息通信研究院自2019年起持续跟踪“人工智能+安全”的技术和产业发展,目前已经完成了不良信息检测、深度合成检测、生物特征识别安全等方面的标准规范十余份。

信通院人工智能研究中心安全与元宇宙部业务主管陈文驶向记者透露:当前国内企业对于如何将较为抽象的法律法规、伦理原则落实到技术、产品和应用中较为困难,尤其是在模型算法的全生命周期中,切实防范各类安全风险的能力尚且不足。此外,产业界较为倾向于采取防御措施,注重预防漏洞和抵御攻击,尚缺乏主动研发安全技术,探索“以技治技”的技术手段。

在齐向东看来,解决AI带来的安全问题,既要发挥人的引领作用,也要充分利用极其强大的智能分析和自动研判能力。他建议:应该大力推进

相关链接

AI技术改变“00后”就业 直播带“岗”求职更精准

以AI技术为基础的数字化模式打破了传统就业的边界,求职者的岗位选择范围更广了,就业精准度也得以随之提升。

刷一刷脸、轻按几下屏幕,短短10秒内,求职者就在“1号求职机”上完成了一次云应聘。刚刚过去的周末,2024年“乐业上海优+”春季促进就业专项行动大型招聘会暨高校毕业生择业对接会(下称“招聘会”)现场人头攒动,一张张年轻的面孔上写满了对未来的期待。在此次招聘会新设的“智慧就业专区”,科技提升给出了更大的可能,可以为求职者提供AI模拟面试、VR虚拟求职、刷脸智能应聘等体验。作为上述这台搭载了多项AI技术的智慧设备开发方,小砖块网络科技创始人荣海旭告诉记者,“1号求职机”目前已服务了近70万家用工企业,对接了5000多万求职者,对特定的行业求职效率颇有验证,“根据跟踪发现,新兴制造、工业智能化以上述方式的就业成功率超过50%”。

业内人士称,以AI技术为基础的数字化模式打破了传统就业的边界,求职者的岗位选择范围更广了,就业精准度也得以随之提升。

AI求职为青年人加分

同样,在“智慧就业专区”,酷似太空舱的可移动“智慧就业E站”也赚足眼球,灯光、幕布、封闭隔音与新风系统等一应俱全。“该设备可实现长时间的直播带岗、就业指导、视频面试、职业测评等,目前正计划在上海各区域的‘15分钟就业服务圈’做落地投放。”该智慧设备开发方、创新集团首席政府事务官侯旭告诉记者。

基于多年数字化就业系统的开发经验,荣海旭表示,数字化就业的基础设施建设,或应该成为行业发力重点。“比如,通过抖音刷到了某个企业的岗位推荐,有意向的用户可以直接跳转到发布信息的企业页面上进行直接沟通。”

荣海旭举例说,AI技术在就业领域的应用还有一些有趣发现,一些缺乏简历优化能力的“蓝领(如钳工、电工等)”很愿意通过刷脸方式应聘,认为简单便捷;再比如,跨省求职意向最高的几组,是云南和上海、贵州和浙江、河南和广州等。

事实上,除了刷脸、求职,AI或能完善求职者

“AI+安全”的科技创新能力,把AI安全技术融入数字化场景当中,鼓励头部企业与专业安全厂商在关键行业选取典型场景开展联合创新。鼓励企业和高校把最新的AI科研成果和网络安全攻防技术相融合。

针对安全问题,全国人大代表、科大讯飞董事长刘庆峰建议:围绕大模型的数据安全、隐私泄露、可靠性、知识产权等几大关键方面制定法律法规,同时,完善向社会开放的大模型的准入和运行规则,明确责任分配与问责机制。

AI到了要立法的时候吗？

随着AI的快速发展,越来越多的人对公民隐私权的保障、AI企业的自律、伦理的挑战等问题提出了疑问,并呼吁法治轨道推动人工智能快速健康发展。

2月2日,欧盟27国代表在比利时布鲁塞尔投票一致支持《人工智能法案》文本,该法案的出炉受到全球瞩目,如果获得批准,这将是全球首个全面监管人工智能(AI)的法案。

那么,国内AI立法还有多远?全国人大代表、四川省律师协会会长李世亮表示,随着AI技术的飞速发展,其背后的风险也日益增多,甚至已发生了因AI技术引发的诉讼案件。然而,国内AI立法“不用太着急”,应当给予市场一定的发展空间,等两三年出台才正是时候。

“这是一个经济关系,当AI技术发展相对成熟,并暴露出一些问题时,就需要立法来进行规范。”李世亮说,我国目前处于AI技术发展的起步阶段,现在立法还没有必要。此外,由于没有相对成熟的市场经验,因此精准立法的条件还不成熟。

全国政协委员、陕西省高级人民法院副院长巩富文表示,人工智能相关立法既要考虑到推动技术的进步、推动产业的发展,也要考虑到对国家利益的维护、避免侵害他人合法权益,“必须统筹考虑”。

据巩富文介绍,早在2017年7月,国务院就印发了《新一代人工智能发展规划》,当时提出分三步走的战略目标:到2020年,部分领域的人工智能伦理规范和政策法规初步建立;到2025年,初步建立人工智能法律法规、伦理规范和政策体系,形成人工智能安全评估和管控能力;到2030年,建成更加完善的人工智能法律法规、伦理规范和政策体系。2023年6月,国务院发布2023年度立法工作计划,人工智能法草案就被列入其中。2023年7月,国家网信办联合国家发展改革委、教育部、科技部、工业和信息化部、公安部、广电总局发布了《生成式人工智能服务管理暂行办法》,在人工智能监管上布局了先手棋。另外,2022年,深圳出台了我国第一部人工智能地方性法规《深圳经济特区人工智能产业促进条例》。

解决就业错配

借助AI技术与智慧设备,一方面,求职者快速定位到合适岗位,并获取一些岗位推荐和职业发展建议;另一方面,用工企业则可以以更低的面试成本招聘到更合适的人才。

“从高校毕业生的现场咨询情况来看,一些毕业生仍然不了解自身专业,以及自身专业在当下高度细分化的职场中,应该选择哪些岗位先入手,毕业生对打破信息壁垒、更好地对外部职业做探索的能力也较为缺乏。”此次招聘会“职业指导”专区的资深导师李弘说。

她告诉记者,AI技术的应用,某种程度上会比导师更好地了解行业细分情况,可以帮助上述求职者迅速了解行业及上下游发展。“假设一名毕业生对汽车行业感兴趣,搭载了AI技术可以呈现汽车从整车到质量控制再到零部件的每一个环节所需要的岗位,帮助求职者做好职业探索;而作为用工企业,则可以制作一张公司全岗位地图,帮助求职者做好职业延展,为其发现更多的职业可能性。”李弘说。

AI技术的应用或能解决人力资源错配的问题。李弘举例,比如,计算机专业的毕业生在高校期间已经读过代码学习课程,但进了企业则需要直接上手做“支付”功能的产品,这一类产品对数据安全要求很高,毕业生根本没法将所学用到工作中去,会觉得自身能力不足;再比如,一些掌握了C++语言编程能力的毕业生,进入职场后,按照工作目标,发现还需要去学习Java语言等技能。

据《第一财经》邹臻杰/文