

“人工智能+”理性正视挑战

A 算法不透明导致的不可解释

2016 年,谷歌人工智能系统 AlphaGo 击败世界围棋冠军李世石,令世人大为震动。依靠人工智能深度学习理论的突破,计算机可以模仿人类作出决策,然而,这仅基于大量的数据学习,而非因果或规则推理,整个决策过程仍是一个“黑箱”,人类难以理解,导致追责难。

复旦大学计算机科学技术学院院长姜育刚举例,此前,美国 IBM 公司研发了人工智能系统“沃森”帮助医生进行诊疗决策。然而,许多医生很快发现在使用“沃森”时,系统给出了多个不安全、不正确的治疗意见,甚至在极端的诊断案例中,“沃森”给有出血症状的癌症病人开出了容易导致出血的药物,严重时可致患者死亡。然而,医生却并不知道为什么“沃森”给出了这样的意见。决策步骤的不可解释,带来诸多不确定性。

近年来,人工智能应用于新药研发被寄予厚望。然而,算法的不可解释性却横亘在前。相关研发和监管部门需要清楚地知道药物开发中使用的算法,从而理解人工智能主导的决策背后的逻辑。如果不对监管实现算法透明化,人工智能将会是一个无法进行严谨的科学评价及验证的“黑匣子”。这可能会导致在药物审批过程中出现种种无法预料的问题,比如对人工智能“发现”的生物标记物的接受度不明。此外,对于智能政务、无人驾驶这样安全性要求极高的行业,人工智能的引入自然更为谨慎。

“深度学习的算法和核心模型需要能够真正展开,让公众知晓它的机理模型”,上海人工智能研究院有限公司总经理宋海涛建议。中科院软件研究所研究员薛云志则指出,人工智能面向不同知识背景的用户,要以简单、清晰的方式,对决策过程的根据和原因进行说明,并能对系统决策过程关键节点的数据加以追溯并能够审计,这在未来人工智能应用大规模落地时,是特别需要关注的特性,也是实施监管的必要。

B 易受欺骗引发安全性质疑

作为人工智能技术的“大热选手”,深度学习可以通过对大量已知样本的训练,制作自己的样本,这是深度学习的特点,同样也是痛点。京东人工智能研究院院长周伯文坦言,人工智能目前在面向产业化落地时,遇到的巨大挑战正是真实环境的开放边界和规则模糊,数据的“噪音”非常多,使得智能模型的部分结果和使用情况难以让人信赖。

姜育刚指出,人工智能目前的智能判别模

语音识别、文本识别、视频识别……数字经济时代,人工智能技术已走近你我身边,被视为经济增长的新引擎、国际竞争的新阵地和推动智慧社会建设的有效工具。而加快“人工智能+”产业融合、赋能更多行业应用落地,更成为社会各界共同的期待。

然而,不久前在由中国人工智能学会主办的 2020 中国人工智能产业年会上,最新发布的报告指出,目前已成熟应用的人工智能技术仅为语音识别、机器学习、计算机视觉、自然语言处理、知识图谱、智能机器人等技术距离生长成熟尚需数年时间,而无人驾驶汽车在未来 10 年内都不太可能出现。

从实验室走向大规模商用,人工智能还需要多久?尚存在哪些“堵点”“痛点”?在许多业内专家看来,正视人工智能尚存在的诸多挑战,对技术赋能抱有理性期待,方能让其回归技术本质,成为更多产业变革创新的动力源泉。

式存在缺陷,容易被对抗样本所欺骗。比如图像识别,在一张人像图片上加入一些非常少量的干扰,人为视觉看上去基本没有区别,但人工智能模型就会产生识别错误;再如自动驾驶,一张“限速 80 码”的交通标牌,加入一些干扰后,就可能被机器识别成“禁止通行”。显然,存在很大的安全隐患。

语音识别领域也存在这种问题。技术人员在语音上任意加入非常微小的干扰,语音识别系统就可能识别错误。同样,在文本识别领域,改变一个字母就可以使得文本内容被错误分类。

此外,若深度学习的数据集中存在隐藏的偏见,人工智能系统无法发现,也不会否定。缺少反馈机制的“照单全收”,最终可能导致生成的结果并不客观。

例如在行业内已经出现的,人工智能在深度学习后对女性、少数民族、非主流文化群体产生“歧视”;亚马逊通过人工智能筛选简历,却发现了系统对女性存在偏见导致最终关闭。更为常见的是手机软件利用人工智能算法导致的大数据“杀熟”,如根据手机类型的不同,可能会推荐不同类型的商品,甚至打车时推荐不同价格、档次的车辆。

目前,“AI+金融”的发展如火如荼。但当金融机构均采用人工智能进行决策时,其市场信号解读就可能趋同与不断强化,导致形成偏离正常市场规律的结果。而这些不正常的市场变化也会成为人工智能的学习基础,将人工智能



的决策逻辑进一步简化,容易造成恶劣的后果。

以上这些问题,影响着人工智能赋能实体经济的安全性,凸显产业对技术可信赖性的呼唤。“从 AI 到可信赖 AI,意味着我们需要在技术层面上解决鲁棒性(稳定性)、可解释性和可复制性这些核心技术挑战。同时为了大规模产业化应用,我们必须考虑到人工智能的公平性和负责任。这几个维度是人工智能必须要解决的问题。”周伯文说。

C 法律规制和伦理问题待完善

“目前的智能算法还存在给出的决策不符合伦理道德要求的问题。”姜育刚指出,在应用中已发现,智能算法的决策没有从改善人类生活、服务人类社会的角度来进行。如智能音响在对话中出现“劝主人自杀”的内容,聊天机器人学会了骂脏话和种族歧视等。而这些不友好的决策都是模型从数据中学来的,并不是研发者对人工智能模型设置的目标。

同时,人工智能算法需要海量的数据驱动,训练数据可以被算法恢复,个人隐私存在泄露和被侵犯的风险,而大量的数据也存在共享壁垒。在人工智能赋能金融的过程中,这一问题尤被关注。最新报告显示,近年来,每年发生金融隐私泄露事件以大约 35% 的速度在增长。加之近年来人工智能技术在金融行业的广泛应用,

由此带来的银行数据、保险数据、网贷业务及大数据等个人信息保护问题日益凸显。

在 2020 年抗击新冠肺炎疫情期间,人工智能技术在我国响应速度快、介入力度大,帮助推出了 CT 影像的辅助诊断系统,提升了医生诊断的速度和信心。然而,医疗影像智能诊断发展也面临着法律规制问题。与其他人工智能赋能行业的大数据相比,获取高质量的医疗影像数据相对困难。不同医疗机构的数据,目前还很少互通、共享。而单个医疗机构积累的数据往往不足以训练出有效的深度学习模型。此外,使用医疗影像数据进行人工智能算法的训练还涉及保护病人隐私等非技术问题。

此外,近年来,随着人工智能技术的深入探索,科学界有人提出研发“人工生命”,成为又一个伦理话题。对此,中国工程院院士李德毅表示,生命不仅有智能,更要有意识。从伦理角度上,生命是人类的底线,触碰底线要慎之又慎。“所以,我们可以通过计算机技术继续研发没有意识、但有智能的高阶机器。让人类的智能在体外延伸,保持它的工具性,而非人工创造意识。”深圳云天励飞技术股份有限公司副总裁郑文先同时提醒,“人工智能的技术进步可以给社会带来非常正向的效益,不应因为对隐私保护机制等方面的忧虑而将人工智能的问题妖魔化。”他认为,当前人工智能的法律法规尚不健全,亟待有关部门进一步科学制定和完善,这样才能引导公众更加健康地看待这一新技术应用于产业。

“文具盲盒”流行 隐藏哪些套路

近日,浙江省宁波市海曙区的王女士向宁波市消保委诉称,自己的孩子目前就读小学三年级,现在班级流行“文具盲盒”,为了抽取到某一个隐藏款送人,孩子居然连续购买了 24 支笔的套装 20 套,总价 2000 余元,已经完全成瘾。浙江省宁波市消保委还接到数起咨询及投诉,为了抽中小概率的特别款、隐藏款、限量款,孩子频频向家长索要零花钱用于购买盲盒商品,导致精神恍惚影响学习,甚至产生家庭矛盾。

记者调查发现,各种“文具盲盒”在北京的小学生中也在悄然流行,中性笔盲盒、橡皮盲盒、修正带盲盒、胶带盲盒、印章盲盒、多款文具集合幸运盲袋等“文具盲盒”的价格比普通文具贵上 2-3 倍,但还有孩子为抽到盲盒中的隐藏款不惜花费上千元,这也引起了老师、家长和社会的担忧。

调查 为“隐藏款”重复购买“文具盲盒” 家长担忧引发学生过度消费

有调查显示,拆盲盒带来的惊喜正风靡年轻一代,国内盲盒行业市场规模预计 2021 年将突破百亿元。

在淘宝中搜索关键字“文具盲盒”,北青报记者看到,共有得力、晨光、yoofun/优凡文具、三年二班等数十个品牌,3700 多个产品网页。其中部分产品标注着“99% 的小朋友都要买”“包含隐藏款礼盒”等广告语,还配有各种店家打开盲盒抽中隐藏款的视频。

记者在西单某商场地下一层书店看到,各类“文具盲盒”占据门店显著位置,柯南、哈利波特、复仇者联盟等深受孩子们喜爱的人物形象,都被印在了“文具盲盒”的包装上,还印着大大小小的问号和“惊喜连连”等字样,花花绿绿种类繁多。一支盲盒笔基本售价在 3.5-6 元不等,文具集合盲袋售价则为 15-40 元不等,前来购买的学生络绎不绝。

书店工作人员表示,“文具盲盒”销量不错,越是新到的产品越受欢迎,有同学每天都会来转转;淘宝店家也表示,有家长为满足孩子的需求,甚至一次下单把一整套都购买下,以免孩子反反复复买相同款。

文具盲盒如何在学生中流行起来的?北青报记者了解到,有的同学为了得到隐藏款,在网上和各家文具店买买买,前后花了 500 多元。购买中难免有重复的文具,她便把不喜

欢的笔、尺子、胶带、本子等文具送给其他同学。“我被同学送了一支印着卡通图案的笔,这种笔与普通文具不同,大家都想得到不同的颜色和图案”,一位四年级小学生孙同学告诉北青报记者,“我渐渐也喜欢上‘文具盲盒’,总央求妈妈给我买新出的款,第二天可以到学校和同学们一块交流。”

盲盒里面的文具真的物超所值吗?例如一个晨光“林深不知处”“与子说”联名盲盒文具套装,包含一支中性笔、替芯一支、便签本一本、胶套本一本、荧光笔一支,售价 7.8 元。看起来文具盲盒并不贵,孙同学表示,但她买“文具盲盒”只想得到心仪的款式,与文具本身无关。实际上开学时家长已经给准备了足够用的文具,新买的盲盒里有些文具根本用不上。“便利贴、印章、尺子之类的文具,一开始抽到重复产品还会送人,后来大家都有很多了,送同学都没人要。每次到了文具店还是想买一袋拆拆看。”她吐露了自己的矛盾心理。

对于孩子沉迷“文具盲盒”,有家长感到担忧,文具盲盒过度吸引了孩子的注意力,令孩子不能专注于学习。“盲盒”在成人中大行其道,很多成年人尚且控制不住,对于自控能力差的孩子更是如此。有孩子除了用零用钱购买,甚至和同学借钱购买,着实令人担忧。

还有家长认为,文具本应被使用,而不是被



收藏的。“文具盲盒”的属性是文具,但其畸形的吸引力,正在推动孩子过度消费,养成浪费的习惯。一位五年级小学生家长说,自从孩子喜欢上文具盲盒,短短半年时间,家里书桌的抽屉、柜子里已装满文具,仅中性笔就有一抽屉上百支,一学期最多用掉 10 支,剩下的肯定会是一种浪费。

分析 过度包装和营销引发“买买买” 攀比心理容易导致孩子“上瘾”

盲盒经济一路走高后,从玩偶盲盒到机票盲盒之后,有网友调侃道“万物皆可盲盒”。相同的盒子中放置不同的商品,消费者事先不知道盒子里装的是哪一款,但有一定概率能够抽到自己心仪的商品,这种叫“盲盒”的消费让人“买买买”停不了手。

盲盒为何如此畅销?有哪些潜在消费陷阱?盲盒走红不是偶然的,商业的过度包装和营销是诱因。记者看到,有“文具盲盒”在产品上标注“99% 的小朋友都要买”“包含隐藏款礼盒”等广告语,还配有各种店家打开盲盒抽中隐藏款的视频,存在过度包装和营销的嫌疑。

宁波消保委分析认为,孩子本身并非真正喜欢或者为了该款产品的实用功能而买单,而是因为在他们学校拥有隐藏款或者稀有款的同学,就拥有了在同龄人中的话语权。同学之间的社交因为盲盒而发生了变化。孩子想要被别人

认可和喜欢的心理可能比成年人更强烈也更单纯。当学习成绩的提升路阻且长,他选择了一条最为轻松的捷径,就是拥有最稀有的文具盲盒,并用其来交换友谊,交换话语权。

还有专家分析,由于盲盒包装的特殊性,容易导致消费者和生产者“信息不对称”,加之盲盒分为普通版和隐藏版,可能引起孩子的攀比心理,导致孩子购买和使用该类产品容易“上瘾”。

D 亟待技术进步 发展新一代人工智能

面对技术落地所遇到的种种“痛点”,许多专家给出了这样的比喻:“人工智能相当于一个锤子,不能哪一个钉子都能砸。”

“我觉得,人工智能发展的第一步是辅助,让重复复杂的劳动量由机器完成,在这个基础上,我们再创造条件逐渐向智能决策的方向发展。”郑州大学教授蒋慧琴表示,对于业界有人提出“人工智能超越甚至取代人类”的期待和预计,应保持冷静,“只有沿着这样的方向坚持下来,才有可能达到我们的目标”。

中国科学技术发展战略研究院研究员李修全认为,在重复性操作的生产环节和基于海量数据的高强度计算优化求解上,人工智能具有明显优势,应当是当前应用于产业的主要方向。

华为云人工智能领域首席科学家田奇则认为,加速人工智能赋能产业落地,其与科学计算的深度融合应是显著趋势,在工业、气象、能源、生物、医学等领域,需要大量科学计算,人工智能技术能为传统科学计算带来新的思路、方法和工具,同时由于传统科学计算具有严密性,人工智能也可以提高它本身的可解释性。

“推动人工智能进入新的阶段,有赖于与数学、脑科学等结合实现底层理论的突破。”中国科学院院士、清华大学人工智能研究院院长张钹说,未来所需要的第三代人工智能应是可实现解释的、鲁棒的、可信安全的智能系统,依靠知识、数据、算法和算力四个要素,将实现从不带认知的人工智能转变为带认知的人工智能。

如何解释新一代人工智能?李德毅认为,传统人工智能是计算机智能,属于封闭型人工智能。新一代人工智能应该是开放性人工智能。当前,所有的计算机都是对软件工程师的智能编程代码进行一次又一次简单执行,“但我们希望这个机器在学习过程中能够解决新的问题,学习应成为新一代人工智能解决现实问题的基础”。

清华大学智能技术与系统国家重点实验室教授邓志东建议,数据和算力的增加总有天花板,要推动人工智能技术深度赋能更多行业,需要的是核心关键技术突破,特别是认知智能的进步,同时,还要依靠智能高端芯片、传感器等零部件的硬件支撑,再借助我国 5G 信息技术的优势,形成合力支撑产业落地和商业化应用。

此外,人工智能标准化工作也应加速展开。薛云志表示:“建立可信赖的人工智能需要标准化,一方面要从开发者训练、测试与实验、部署运营和监管的角度来做,另一方面则要从芯片等硬件、算法、产品系统出发,来制定标准和规范,同时对人工智能的风险、伦理、管理等标准研究也要尽快启动,这些都只是第一步。”

(据新华网)

提示 认清盲盒具有不确定性 防范商家营销套路

中消协早前曾发布消费提示,青少年群体好奇心强、喜欢攀比、消费观念尚不成熟,容易为盲盒“上瘾”,有的甚至为了抽中“隐藏款”而直接“端箱”——为买到只有 1% 甚至概率更低的商品,将上百个盲盒全部买下。盲盒与普通商品相比,具有很强的信息不对称性,消费者只能依靠商家的广告宣传来选购,这就很容易被商家的夸大商品价值、虚构中奖概率、颜色款式不符等虚假宣传所误导。

中消协提醒广大消费者,要认识到盲盒具有不确定性的本质,认清并防范商家过度营销的套路,切勿跟风与攀比;要结合自身经济能力、消费需求和兴趣爱好等,量力而行、理性消费。购买盲盒时,要尽量选择信誉高、口碑好、售后服务完善的商家进行交易。

6 月 1 日,市场监管总局发布《儿童用盲盒消费提示》,提醒盲盒可满足儿童的好奇心理,因此近年来在儿童和青少年中极为盛行。由于消费者购买时无法直观地辨别盲盒内产品的质量,因此,消费者应看包装、留凭证,避免买到不合格的产品。

专家提醒,家长应引导孩子购买儿童盲盒不要过分沉迷、“上瘾”。在购买盲盒时家长应引导孩子结合经济能力、消费需求等量力而行,不要过分沉迷、避免成瘾。

内存 市场监管总局开展 2021 年儿童和学生用品安全守护行动

6 月 1 日,市场监管总局部署开展 2021 年儿童和学生用品安全守护行动。此次行动将以儿童玩具、儿童餐饮具、儿童护具、儿童服装、儿童家具、学生文具、学生灯具、学生校服等社会高度关注、与儿童健康安全密切相关的产品为重点,围绕涉及质量安全的指标,组织质量监督专项检查。

与此同时,全国市场监管部门将开展流通领域“三无”产品专项清查及“网红玩具”等产品打假专项行动,坚决取缔“黑工厂”“黑窝点”“黑作坊”,积极发现问题,回溯生产源头,严厉打击销售假冒伪劣玩具等违法行为,适时公布典型案例,震慑质量违法行为。

本次行动还将加强儿童用品的风险评估和应急处置,提升消费者质量安全意识和防范能力;开展儿童和学生用品质量帮扶“巡回问诊”,进一步压实企业主体责任;健全标准体系,开展对标达标提质行动;充分发挥部门联合作用,形成质量安全社会共治格局。

(据新华网)