人工智能：“花海”之下仍有“荆棘”

经济日报·中国经济网记者 陈 静

热点追踪

人工智能可以同声传译、写新闻稿、协助医生看病、让机器人脸识别的精度高于人类、甚至写诗和战胜围棋世界冠军，其应用可谓“百花齐放”。

数据显示，截至2017年6月，全球人工智能企业总数达到2542家，预计到2030年，人工智能将为世界经济贡献15.7万亿美元

生产项目厂房内调试焊接机器人。 新华社记者 杨世尧 摄

图为工人在河北沧州中捷高新区一家汽车部件

在今年7月国务院印发的《新一代人工智能发展规划》（以下简称《规划》）中提出，到2020年，我国人工智能核心产业规模超过1500亿元，带动相关产业规模超过1万亿元。顶层设计相继出台，巨头发力布局生态，资本市场热情洋溢，细分行业独角兽不断涌现，人工智能这片“花海”已不止“看上去很美”。

但“花海”之下仍有“荆棘”。市场研究机构埃森哲大中华区信息技术服务总裁陈笑冰坦言：“人工智能也将会引发新的安全和伦理问题，鉴于未来人工智能将深入生活，政府也需要切实为人工智能制定监管规则，保证人工智能应用合理合规发展。”《规划》也同时提出：“人工智能发展的不确定性带来新挑战。人工智能是影响面广的颠覆性技术，可能带来改变就业结构、冲击法律与社会伦理、侵犯个人隐私、挑战国际关系准则等问题，将对政府管理、经济安全和社会稳定乃至全球治理产生深远影响。”

人工智能发展将面对怎样的挑战与风险？又应该设立怎样的“游戏规则”，让新技术能够与人类社会良性互动？

监管刚刚起步

人工智能不断融入人类生活的同时，也引发公众对人工智能的忧虑。对此，专家表示，应该建立监管机构来引导、促进和保障人工智能的健康发展

此前有报道称，“脸书”人工智能研究所中的两个聊天机器人“失控”，发展出了人类无法理解的语言，“被迫关闭”引发了广泛关注。尽管随后被证明是一场“乌龙”，只是因为工程师忘记加入“使用英语语法”这一条件。

但对事实的夸大报道，也显示出媒体和公众对人工智能的忧虑。在北京市中盾律师事务所律师陈涛看来，随着人工智能深入融入生产和生活，必须以立法来对其安全性进行监管，给公众吃下“定心丸”。互联网汽车的特斯拉埃隆·马斯克也表示，我们应该警惕人工智能崛起的潜在风险，并建立监管机构来引导这项强大技术的发展。

由于无人驾驶汽车的无人操作与各国现有道路交通法规抵触，相应立法和规范一直是其发展的重要前提条件。图为无人驾驶汽车的探测方式模拟图。

中国科技大学研制的智能机器人与小朋友互动。 （资料图片）

对人工智能进行立法监管，首先要解决人工智能使用中基本的安全问题，以及使用者与服务提供者的责任界定问题。以无人驾驶汽车为例，上路前，对其安全性如何全面评判？一旦无人驾驶汽车出现事故，如何判断使用者、软件提供商以及车辆制造商等多方主体的责任，如何在后续赔偿和保险理赔中进行规定？实际上，立法监管不仅降低风险，也让服务企业能够“有据可依”，从而促进和保障人工智能的健康发展。

从目前来看，各个国家的人工智能监管都刚刚被提上日程。在美国，2016年10月，总统行政办公室和国家科技委员会发布了两份重量级报告：《美国国家人工智能研究发展战略规划》与《为未来的人工智能做好准备》，后者提出了发展人工智能的7项关键战略，在第三条“社会影响战略”中，提出“理解和确定人工智能在法律、伦理和社会领域中的影响”；在第四条“安全战略”中，则提出“确保人工智能系统的安全和对公众的隐私保护”。

在欧盟，2016年欧盟法律事务委员会向欧盟提交了《欧盟机器人民事法律规则》，针对基于人工智能控制的机器人，提出了使用的责任规则、伦理原则、对人类自身和财产的伤害赔偿等监管原则。英国下议院科学技术委员会在今年4月表示，也将开展关于人工智能监管的研究。

在我国，《规划》中同样提出，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”。其中特别提出，要“开展与人工智能应用相关的民事与刑事责任确认、隐私和产权保护、信息安全利用等法律问题研究，建立追溯和问责制度，明确人工智能法律主体以及相关权利、义务和责任等”，“重点围绕自动驾驶、服务机器人等应用基础较好的细分领域，加快研究制定相关安全管理法规，为新技术的快速应用奠定法律基础”。

不过，对人工智能的监管也不能“闭门造车”。“立法的前提是了解人工智能的科学规律，需要充分准备、摸索和积累，对技术进步充分了解，同时考虑公众的实际需求。”陈涛表示。

安全仍有漏洞

安全是人工智能面临的巨大挑战。这其中既包括在应用层面的传统黑客攻击方式，也存在着对基础设施方面进行的数据库、云服务等攻击。但更关键的安全问题是从最核心的算法层面发起攻击

两张人眼看起来一模一样的熊猫图片，一张被神经网络正确识别为“熊猫”，另外一张却因为被加上了人眼难以察觉的微小扰动，就被神经网络以99.3%的置信度识别为“长臂猿”——这就是可以“愚弄”人工智能的对抗样本，直接折射出人工智能所面对的安全问题缩影。

专注于互联网安全的极棒实验室总监王海兵告诉《经济日报》记者：“安全是人工智能面临的巨大挑战。”他表示，一方面，人工智能要面对传统的黑客攻击方式，比如在应用层面，可以攻击它的操作系统或者逻辑漏洞。“比如说，通过对智能门锁的攻击，就能实现任意人脸都可以通过门禁。”在人工智能的基础设施方面，则可以对人工智能使用的数据库、云服务等进行攻击，“比如说，机器视觉经常调用的OpenCv库，机器学习用到的TensorFlow框架，人工智能的从业者可以直接调用这些服务，但不幸的是，这些基础设施同样有漏洞。”王海兵说。

然而，人工智能所面对的更关键安全问题，正是诸如熊猫图片这样的对抗样本。王海兵表示：“用对抗样本攻击人工智能，其实就是从最核心的算法层面来攻击它。”

美国加州大学伯克利分校教授宋晓冬这样介绍对抗样本攻击的危害：“比如，无人驾驶汽车根据交通标示进行决策。如果交通标示是一个对抗样本，那么人类可以完全不受干扰，但无人驾驶汽车却可能将它完全识别成错误信息，这将带来严重后果。”实际上，美国伊利诺伊大学的一项测试已经证明，自动驾驶系统有可能被对抗样本“蒙骗”。

“但公众不用过于担心，至少现在来看，针对自动驾驶的对抗样本对抗性很差。比如，它只能在0.5米的距离内让自动驾驶系统错判，但自动驾驶场景毕竟是逐渐接近交通标识的。”王海兵也表示，“未来会不会有更完美的对抗样本，仍是未知数”。

人工智能面对众多安全问题，对此，开发者也在努力总结与之对抗的手段。智能家居生产厂商BroadLink高级副总裁康海洋表示：“我们会将多方数据融合和统一分析，以提升数据的可信程度，同时也在尽量让整个系统变得更加透明。此外，我们还会及时销毁所有能销毁的数据，减少用户被攻击的可能性。”

伦理尚待明确

告诉人工智能何为“正确”，正在成为当务之急。如果不对其进化方向和目标形成共识，人工智能的伦理规则将无法“落地”

如果保持前行，会撞上沿途的5位行人；如果避开他们，就会撞上路边的墙，车中的两名乘客则可能有生命危险。在这种情况下，指挥自动驾驶的人工智能应该如何选择？英国伦敦玛丽女王大学高级讲师雅思密·艾登表示：“如果是人类驾驶员，大可以直接撞上行人，并表示‘是他们自己突然跳出来的’，但人工智能在道德上很难获得这么奢侈的原谅。”

这只是人工智能所处伦理困境的冰山一角。今年以来，麻省理工和哈佛大学联合推出了人工智能伦理研究计划，微软和谷歌等巨头也成立了人工智能伦理委员会，告诉人工智能何为“正确”，正在成为当务之急。《互联网进化论》一书的作者、计算机博士刘锋坦言：“尽管大方向上说，人工智能应当以造福人类为前提，但如果不对进化方向和目标形成共识，人工智能的伦理规则将无法‘落地’。”

对于人工智能来说，“伦理正确”的核心是正确的“算法”。美国一些法院使用的一个人工智能犯罪风险评估算法COMPAS，被第三方机构认为对黑人造成了系统性歧视。业界因此怀疑，小众人群有可能因为个体差异而承受“算法的歧视”。腾讯研究院研究员曹建峰表示，如果算法本身有问题，一旦将算法应用在犯罪评估、信用贷款、雇佣评估等关乎人身利益的场合，“因为它是规模化运作的，并不是仅仅针对某一个人，可能影响具有类似情况的一群人或者种族的利益。规模性是很大的”。

此外，还有来自数据的风险。以色列历史学家尤瓦尔·赫拉利表示，“人工智能技术的一个潜在结果是：促成数据集中到某一个地方，也进而导致权力的集中”。比如，大量互联网数据集中在少数几家巨头的手中，人工智能技术是否会因此遭到垄断？“AlphaGo之父”哈萨比斯就曾表示：“我提醒诸位，必须正确地使用人工智能。”他告诉记者，“人工智能技术不能仅为少数公司和少数人所使用，必须共享”。

AlphaGo超越了人类几千年来对围棋的理解，但人类并非能完全理解AlphaGo为何会如此决策。从这一点来看，人工智能像个“魔盒”，这也让透明性成为人工智能伦理中的重要组成部分。英国阿兰图灵研究所科研主管安德鲁·布莱克表示，算法可问责性的存在至关重要。“透明性规则应被作为伦理道德准则，编入算法之中，这样人们才能更为清晰地认知人工智能的社会影响，并在问题发生之时能够及时找出原因，调整策略。”

区块链：让医疗信息走出“孤岛”

本报记者 吴佳佳

随着区块链技术日益成熟，其在医疗体系中正发挥出巨大价值。

阿里健康日前宣布，与江苏常州市合作“医联体+区块链”试点项目：将最前沿的区块链科技，应用于常州医联体底层技术架构体系中。目前，项目采用低成本、高安全的方式，已实现当地部分医疗机构间安全、可控的数据互联互通，解决了长期困扰医疗机构的“信息孤岛”和数据安全问题。

“这是我国首个基于医疗场景的区块链应用。”阿里健康区块链技术负责人刘铁说，基于信息安全、医疗大数据等领域的技术积累，并结合部分开源框架技术，阿里健康研发出适合医疗场景的区块链解决方案。

常州是国家卫计委确定的首批“健康医疗大数据”4个国家试点城市之一。“但现有中心化区域卫生信息平台，在开发成本、响应速度方面都不能很好满足点对点的互联互通需求。”常州市天宁区卫计局副局长张科说。

以常州天宁区郑陆镇卫生院为例，这家社区医院面向郑陆镇14万人口提供基层医疗服务。院长张志宏表示，之前天宁区没有区域卫生信息平台，每家医疗机构的庞大信息都要分散传送到市医疗机构信息平台。但各医疗机构之间并不互通，很多业务诉求无法实现。同时，如何保证个人隐私安全，也是现有平台的难题。

引入区块链技术后，常州的情况大为改观。以分级诊疗就医体验为例：居民就近到卫生院体检，通过区块链上的体检报告分析，筛查出心脑血管慢病高危患者。其中，约5%需转诊的患者可由社区医生通过区块链实现病历向上级医院的授权和流转；上级医院被授权后，可迅速了解病人病史和体检信息，病人无需做二次基础检查，享受医联体内各级医生的“管家式”全程医疗服务，实现早发现早诊疗的“治未病”。

“阿里健康区块链技术利用我们旧有的IT设备和系统将信息串联在一起，接入成本低，安全性却更高，这帮助卫生院和区医院间从‘信息孤岛’到互联互通，老百姓也能享受便利。”张志宏说。

据介绍，区块链是一种分布式数据库的底层技术架构，采用密码学和共识算法等技术，确保了接入区块链网络的各节点在数据流通中的公平、互通和隐私保护。此外，常州区块链项目还被设置了多道数据的安全屏障：区块链内的数据存储、流转环节都是密文存储和密文传输，即便被截取或者盗取也无法解密；为常州医联体专门设计的数字资产协议和数据分级体系，明确约定了上下级医院和政府管理部门的访问和操作权限；并且，审计单位利用区块链防篡改、可追溯的技术特性，可以精准定位医疗敏感数据的全程流转情况，比如在什么时间点，被哪个医疗机构授权给了谁。

“我们看到了区块链技术大规模应用的优势，随着后续接入机构增多，会形成一张快速部署的信息网络，实现业务数据真正的互联互通。并且，数据密文流转授权、全程可追溯、可审计的特点，也增强了管理部门的信心。”张科说。

2016年国务院印发了《“十三五”国家信息化规划》，日益普及的区块链技术被首次列入其中，其为医疗领域带来的革新显而易见：既保护患者隐私，又可让医疗健康数据以更为安全、快捷的方式全网共享。

对于区块链医疗应用的未来，阿里健康智慧医疗区块链项目负责人张文娟表示，“阿里健康希望建立一个尽可能连接更多医疗卫生机构的区块链网络，实现医疗场景有价值信息的安全、便捷、可控流动”。

科技万象

我国...

本报讯 记者沈则瑾报道：近日，中科院低碳转化科学与工程重点实验室暨上海高研院—上海科技大学低碳能源联合实验室，在电催化二氧化碳（CO_2）还原转化生成甲酸和乙醇方面均取得重要进展，相关结果分别发表于国际知名期刊《德国应用化学》。

现代社会消耗了大量煤、石油和天然气等化石能源，导致大气中二氧化碳气体排放量急剧增加，引发全球环境问题日益严峻。对此，通过电催化CO_2转化成为一条可行之路：采用可再生的风电、太阳能等洁净电能为能源，在常温、常压条件下将CO_2直接一步转化为一氧化碳、甲酸、甲醇等燃料及化学品，并实现CO_2的资源化利用和洁净电能的有效存储，表现出极具潜力的应用前景。

然而，如何高效获得高附加值的化学品是CO_2电催化转化研究中极具挑战性的热点课题。

陈为工作组经过近两年的不断探索，筛选、尝试了大量金属、合金催化剂，最终发现由金属钯（Pd）、锡（Sn）组成的Pd-Sn合金催化剂具有非常优异的性能。只需施加非常低的电压，该催化剂就能将所输入电能的99%用于驱动CO_2转化生成高附加值化学品——甲酸。甲酸是基本有机化工原料之一，广泛用于农药、皮革、染料、医药和橡胶等工业。此项研究以CO_2为原料，利用可再生电能高效率合成甲酸，显示出良好的应用前景。

此外，通过电催化过程将CO_2转化生成含有两个（及以上）碳原子的产物，如乙烯、乙醇等非常困难，也是行内重点攻克的目标。该研究团队在前期纳米碳材料研究的基础上，开发出了氮掺杂的介孔碳（N-carbon）材料用于电催化CO_2转化。通过调控N-carbon的孔道结构和表面活性位构型，成功实现了CO_2直接转化生成乙醇。乙醇是用途最为广泛的基础化学品之一，应用于合成醋酸、饮料、香精、染料、燃料等，产业前景巨大。

此项研究工作为设计、创制高活性和高选择性生成多碳产物的电催化体系提供了新思路，受到《德国应用化学》审稿人的高度评价。

新一代石墨烯制备技术发布

破解“定性不能定量”难题

本报讯 记者马洪超报道：在近日举行的“中国碳谷——全球石墨烯制备新技术发布会”上，允升国际董事会联席主席、江阴碳谷科技有限公司首席专家戴加龙发布了新一代石墨烯制备技术——微机械剥离工艺。据介绍，该技术解决了长期困扰石墨烯产业的“定性不能定量”难题，并初步实现了物理法制备石墨烯的产业化。

石墨烯，又被称为“黑金”，有着新材料之王的美誉。戴加龙表示，微机械剥离工艺技术具有产率高、工艺线路短、能耗小、成本低的特点，而且产品品质优良、质量稳定。特别是在很多企业对石墨烯产业“跃跃欲试”，但是结构“零缺陷”的高品质石墨烯少之又少的情况下，新一代石墨烯制备技术为高品质石墨烯的实际操作树立了典范。

据悉，实际操作中，高品质石墨烯的制备应该包括前处理、中制备、后整理等3个阶段。“前处理是对石墨烯原料的清醒认知，中制备要在加工过程中弄清石墨烯的排列方式，后整理着重处理石墨烯二维结构的厚度难题。”戴加龙说。

新型催化剂有望推动充电电池换代

本版编辑 郎 冰
联系邮箱 jjrbxzh@163.com