



丰富公共数据应用场景 应处理好三方面关系

□ 王益民

近年来，党中央高度重视发挥数据要素作用和基础制度建设。从《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》提出“推进实施公共数据确权授权机制”到《“数据要素×”三年行动计划（2024—2026年）》强调“扩大公共数据资源供给”，再到2024年《政府工作报告》要求“大力推动数据开发开放和流通使用”，一系列政策文件的出台为更好发挥公共数据要素价值指明了方向。公共数据蕴藏着巨大的经济和社会价值，是数据要素市场的重要基础资源，推动公共数据开发开放对发挥数据要素价值具有重要的现实意义。

各地区、各部门公共数据资源开发利用的实践表明，我国在司法、金融、交通、医疗、市场监管、环保等领域的公共数据开发利用方面形成了较为丰富的数据产品，广泛服务于政府决策、公共服务和数字经济发展，形成了政府购买服务、授权企业运营和政企合作开发的数据运营模式。但总体来看，由于数据权责不明晰、数据监督管理复杂、数据安全保障机制不健全等因素，公共数据的开发开放还处在有限范围之内和有限种类选择之中，难以形成丰富多元的创新应用场景，阻碍了公共数据开发开放生态的活力激发。为推动高质量发展，充分发挥公共数据的要素价值，需要统筹处理好以下几个方面关系。

第一，从价值主张的角度，协调好公共数据各主体之间的关系。

公共数据开发开放涉及的利益相关主体较多，从数据供给方来看，有政务部门、公共企事业单位等；从数据管理和监督方来看，有数据管理机构、网信部门等；从数据运营方来看，有政府机构、企事业单位、科研院所等；从数据使用方来看，包含政府、企业、个人、社会组织等。因此，应围绕充分发挥数据价值，激发市场活力的价值主张，协调好各方之间的关系，才能形成多元主体良性互动、异质资源有效整合的局面，从而提供创造价值的数字产品或服务。一是数据管理部门与业务职能部门的关系。数据管理机构要发挥好对数据的统筹作用，其制定的数据政策法规、标准化工具、业务指导、监督考核指标体系等，以及推动构建的国家、地方、部门、企业等不同层面的数据开发开放机制要充分考虑业务职能部门的实际情况，激发其积极性，因为这些部门是数据的供给方，决定着数据开发开放的效果。二是数据治理链条上下游之间的关系。从数据开发利用链条上多元适配数据生成、管理、监督、授权、运营、开发利用等参与主体的价值诉求，形成政府主导、政企合作、政社协同的良性互动格局，推动构建安全高效的数据治理生态系统。

第二，从价值实现的角度，处理好公共数据供给与需求的关系。公共数据供给是数据开发开放、发挥数据要素价值的源头活水，制度环境优化将会带来新的变革，以更好发挥数据要素潜能，实现价值增

值，催生新产业、新模式、新动能，推动经济实现高质量发展。政府部门由于技术能力、运营条件和资金提供等方面的限制，在从数据的内部归集到外部授权的过程中还面临着很多挑战。如何实现数据价值，为不同的经营主体参与数据创新服务创造条件，处理好数据的供给与需求关系尤为重要。一是探索与实际需求相适应的数据供给模式。当前各地因地制宜在推动公共数据授权运营的过程中推出了不同的数据供给模式，有的地区在数据管理部门的推动下充分调动业务主管部门的积极性，让其负责各自领域和区域数据专区建设与运营，并授权给相应的国有控股企业，再由被授权方向公众、企业和社会组织提供服务。有的地区积极推动构建多部门参与的公共数据授权运营的协调机制，由公共数据主管部门负责从公告发布到协议签署、运营监管等数据授权运营的完整程序。这些不同的数据供给模式都是结合本地实际构建，取得了一定的效果。二是以需求为导向提升公共数据供给质量。在数据的合作开发过程中，要让数据的提供方、监督方、使用方实时参与到整个过程中，形成明晰的需求匹配机制。通过数据应用场景开发不断提升数据供给质量，形成多部门数据治理协同机制和数据全流程全生命周期质量管控体系，从发现问题到反馈问题再到修正问题，构建多方参与的数据闭环管理。

第三，从价值增值的角度，把

握好平台支撑与场景驱动的关系。公共数据从政府内部使用扩展到向社会提供服务，经历了政府采购技术服务于政府内部、政府开放原始数据服务于企业公众、政企合作与政府授权企业开发运营等探索过程。公共数据价值的增值在于公共数据的跨主体、跨区域、跨场景更广泛地融合开发利用，能创造出更多的应用场景，实现更深度的数据价值，数据授权运营平台的搭建为其提供了可能性。一是以应用场景为牵引提升数据运营平台的服务水平。数据运营平台作为供给侧、需求侧等多元数据的汇聚节点，在服务不同应用主体的过程中不断创新应用场景。在实践探索中，可通过广泛征集重点领域的需求确定被授权主体，探寻出个性化价值高、及时响应市场需求的数据授权服务场景。二是以使用方为中心构建数据开发开放满意度评价体系。不论是政府数据开放平台还是公共数据授权运营，最终目的是面向公众、企业和社会组织释放公共数据价值，服务数字经济发展。因此，需建立一种从用户满意度出发综合长效的评价机制与体系，催生公共数据服务的新理念、新模式、新机制、新手段和新应用，充分激发市场活力。



积极防范人工智能带来的安全新挑战

□ 翟立东

人工智能正日益成为新质生产力的重要要素和核心驱动力，推动生产方式和生产关系发生深刻变革。当前，一系列人工智能交叉领域的重大突破正在重新定义人类社会的数据交互、多模态生成、智能制造、信息连接和智算资源范式。以 Vision Pro 为代表的空间计算、以 Sora 为代表的生成式人工智能、以 Figure 01 为代表的具身机器人、以 Starlink 为代表的天地一体化网络和以 GB200 为代表的算力基础设施，都昭示着以人工智能为代表的战略性新兴产业集群对传统生产力和生产关系格局的重塑已成为不可逆转的趋势。人工智能新质生产力急速崛起，数字技术与实体经济加速融合，智能化发展成为社会共识。

人工智能技术的广泛应用，在促进数字社会发展的同时，也为网络攻击带来了新的途径和手段，并引发一系列亟待应对的安全挑战，比如，“奶奶漏洞”可以绕过人工智能伦理提示词攻击、GPU 算力芯片可被侧信道攻击、大模型深度伪造诈骗、生成式人工智能生成虚假新闻等，这些网络安全事件都暴露出人工智能安全问题的新变化。导致网络攻击加剧主要有以下三方面原因：一是人工智能赋能网络攻击手段升级。网络攻防技术呈现自动化、智能化、体系化快速演进等趋势，网络攻击更加隐蔽高效；二是人工智能系统自身安全挑战凸显。人工智能系统自身也面临数据中毒、模型窃取、算法歧视等诸多安

全风险，网络攻击更加多变难溯；三是人工智能引发的伦理与社会风险加剧。人工智能误判、滥用、失控、操纵等引发的连锁反应极可能导致灾难性后果，网络攻击更加未知。

人工智能发展带来的网络安全新挑战不容忽视，既有技术层面的攻防对抗，也有系统自身的脆弱性，更有深层次的伦理困境。如何筑牢人工智能安全防线，维护人工智能健康发展，事关国家安全、经济运行和社会稳定大局。

人工智能快速发展将使未来数字世界具有时空超越性和快速演进性两大新特征，目前已有的伴生性网络安全防护已无法有效解决网络攻击加剧的新挑战，亟须加快推动人工智能安全屏障的建设。一是坚持系统思维方式，从国家发展战略全局审视新兴安全挑战，注重人工智能安全韧性风险评估，提升战略威胁感知能力。二是提出新兴网络安全理念，由伴生防护向内生防御至新生防范转变，强化主动纵深防御体系。三是凝聚创新联合生态，汇聚交叉科学战略专家、技术团队和产业力量，集中攻研人工智能、数字孪生、网络安全等关键技术，形成国家战略科技新力量。四是建设关键数字基础设施，优先面向人工智能+产业数字化新场景，加快开展人工智能+先行先试试验平台能力建设，提高人工智能安全水平。

坚持高水平科技自立自强，积极开展人工智能安全领域技术攻

关。网络攻击当前难以彻底根除，应优先构建网安事件持续跟踪分析能力，可从人、机、物、态四个方面做安全风险评估，建立一套人工智能产业安全韧性指标体系，针对不同行业周期性指数评估排名，发挥长处、补齐短板，在考虑技术演进和业务迭代的前提下，充分结合不同行业的业务属性和技术特征，部署构建功能完备的数字孪生实验场景，开展网络安全能力评估工作。主动谋划、超前布局，积极达成我国战略威胁感知能力的实质性跃变目标。

未来网络空间将从静态的“场”走向动态的“境”，人工智能安全需要从单点式、场景化防御方式向全链条、情境化的主动防御能力转变。可以世情、国情、民情为基点，从存量、增量、变量三个方面系统性部署网络安全攻防场景，遵循“孪生一拟生一派生一演生一新生”的逻辑路径，运用生成式人工智能布置规划网络安全对抗系统，通过情境模拟动态评估未知安全态势变化，持续提升人工智能安全的风险感知、应急响应、快速处置能力，强化主动纵深防御体系，为构建高质量人工智能安全生态提供坚实保障。

人工智能领域具有强前沿交叉科学属性，人工智能安全队伍建设更需要跨领域、跨学科、跨行业乃至跨国界的人才聚合和交流，应充分发挥体制优势，积极构建人工智能安全产学研创新联合体，逐步打

通人才链的微循环、内循环、外循环和大循环，加速形成人工智能安全技术创新链和未来产业链，为数字经济做强做优做大提供高质量人才队伍。

当前人工智能安全领域的探索大多还处于实验室研究阶段，到应用场景的“最后一公里”有待进一步打通。应加快推进实验成果向真实场景的延伸，搭建人工智能安全攻防对抗试验平台，开展全流程、高频次的攻防演练，在实战环境中检验攻防技术，不断完善人工智能安全防护体系。通过从实验到试验的转变，夯实人工智能安全标准规范、法律法规的现实基础，为全面推进以人工智能为代表的未来产业健康发展保驾护航。

未来应掌握“场景到情境、存量到变量、孪生到新生、实验到试验”的技术路径演进规律，加快建设基于数字孪生的人工智能安全应用技术试验场，夯实人工智能安全基座，实现对人工智能风险的提早预防、实时监测、快速响应和持续应对，推动人工智能安全治理体系和治理能力的不断提高，为数字经济高质量发展筑牢安全之基。



随着大数据和深度学习的发展，生成式人工智能技术给世界政治、经济、文化领域带来极大冲击，技术创新进入新一轮活跃期。生成式人工智能技术在促进新质生产力发展，带来巨大商业价值的同时，也存在深度伪造、虚假信息、广告欺诈等问题，可能为不法分子提供新的技术工具，成为诈骗活动的“新武器”。预防、监测和治理生成式人工智能诈骗，保护公众免受智能诈骗行为的影响，促进人工智能技术健康发展和规范应用具有重要意义。

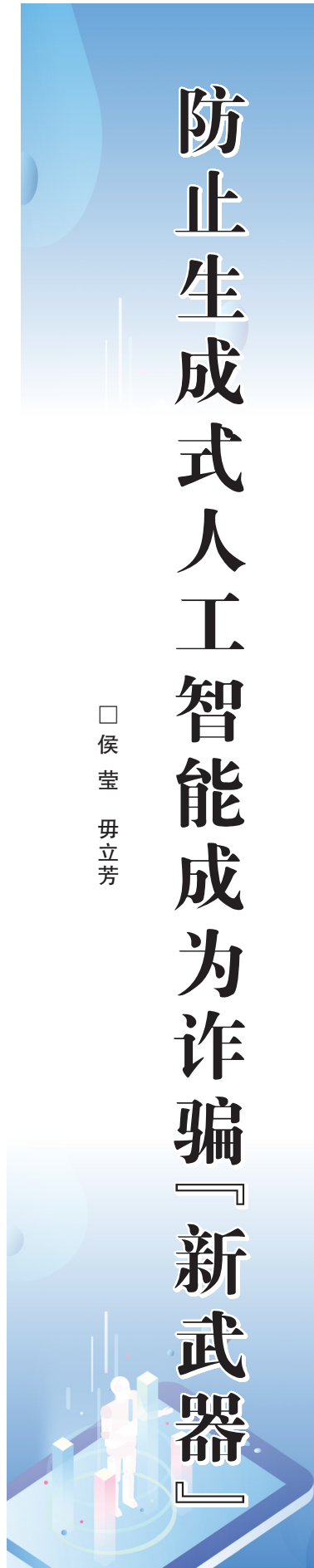
生成式人工智能技术基于迁移学习和人工神经网络，使用深度学习模型，传输和处理现有文本、图像和音视频信息，自动创建出新内容、新方法和新方案。随着生成式人工智能技术的发展，诈骗形式从线下诈骗、电话诈骗扩展到网络诈骗。常见的网络诈骗包括以下几种形式：网络购物诈骗，诈骗者使用虚假网站、虚假商品和虚假促销信息，诱骗消费者购买商品，通过虚假支付链接欺诈消费者；网络投资诈骗，诈骗者以高收益低风险为诱惑，通过虚假网站参与虚拟货币投资、股票期货等投资活动，骗取消费者钱财；网络视频诈骗，诈骗者利用提前录制的真人视频和盗录的视频影像，合成为欺诈视频，向视频被记录者的好友借钱，开展诈骗行为。

防止生成式人工智能成为诈骗新工具是一项系统工程，存在三大监控治理难点。一是全链路信息监管难。诈骗者通过短信、电话、互联网等通信渠道，与受害者联系，基于获取的个人信息和事前准备好的诈骗脚本，骗取受害者的信任，诱导受害者使用银行转账、网上支付、手机支付等方式向指定账户转账，并快速完成资金转移，获取非法经济利益。二是个人信息保护难。诈骗分子通过非法渠道窃取或购买个人信息，包括身份信息、电话号码、家庭住址、网络账号、银行卡账号等，精准获取社会上各行各业人员的个人信息，为实施诈骗构建个人信息基础数据库。三是智能生成产品识别破解难。诈骗分子基于开放数据流和获取的个人信息，使用深度合成技术，篡改图片或者视频信息，对原始信息进行深度伪造，获得人工智能生成产品，通过“换脸”“换声”等方式实施违法犯罪行为。因此，要坚持目标导向和问题导向，在全链路信息监管、个人信息保护和智能生成产品鉴别技术上深耕细作，建立健全政策法规，切实将发展与安全相结合，持续推动科技创新，不断增强反诈能力。

首先，建设公共算力和算法平台是防止诈骗的基础，应研发全链路的信息监管技术。一方面，政府部门牵头建立公共算力基础设施，采用安全可信的芯片、软件 and 工具，统一收集人工智能算法、鉴别算法和检测算法模型，形成算法数据库，规范人工智能服务提供者预训练、优化训练等数据处理行为，提升算力资源利用效能。另一方面，研发可溯源的网安类设备监管技术，基于分类分级监管规则，全链路监管查询、下载、使用和修改个人生物识别信息的行为。并且要提供各类已被识别的合成产品，积累识别样本，提升诈骗电话检测、恶意网址拦截、诈骗文本识别和诈骗风险预警的精准度。

其次，避免个人信息泄露是治理诈骗的根源，应研发个人信息保护技术。一方面，生成式人工智能服务提供者应对服务使用者信息的输入和使用记录依法履行保护义务，严禁采集非必要个人信息，不得非法向他人提供使用者的个人信息及使用记录，规范个人信息采集与共享行为。另一方面，采用匿名化、去标识化技术和加密技术，处理使用者个人信息，对个人信息的获取进行监测，确保使用者个人同意且符合法律法规。通过虚拟私人网络，建立信息安全通道，规范数据传输、处理与存储行为，监管信息使用情况，标注并拦截诈骗信息。

再次，鉴别生成产品是治理诈骗的关键，应研发人工智能生成品的识别破解技术。一方面，规范人工智能合成品的制作流程，扩大信息源取证范围，在信息采集设备中采用水印技术，对原始信息增加“数字水印”，保证源头信息的真实



□ 侯莹 毋立芳

防止生成式人工智能成为诈骗『新武器』

性。使用区块链和智能合约技术，运用数据加密、时间戳和分布式共识手段，在生成品中加入元数据，实现去中心化信用的点对点交易与协作，完成溯源防伪。另一方面，基于递归神经网络和胶囊网络，提取空域、时域和频域特征，通过检测合成品的混合边界及肉眼难辨的灰度元素，对图像和视频进行反向破解，解析图像和视频代码，判断人物与场景的一致性，鉴别原始信息和合成品。

最后，建立健全政策法规，增强公众风险教育，对于防止生成式人工智能诈骗至关重要。一方面，政府应制定针对生成式人工智能犯罪的法律规范，界定滥用生成式人工智能进行诈骗的法律责任，严格监管和执法，明确处罚措施，确保公共安全不受威胁。此外，鉴于数字诈骗的特殊性，还应加强国际合作，加大联合执法力度，打击跨境诈骗。另一方面，政府、企业 and 各级教育机构应大力宣传反诈知识，普及人工智能技术的潜在风险，提升大众的防范意识，提高识别和反诈技能。并且，应增加对未来科技从业者的教育，使其能够规范开发和使用人工智能技术。

生成式人工智能是一项前沿技术，对于提升多个领域的生产效率至关重要。然而，如果不加约束地滥用，可能会成为欺诈者手中的危险工具。只有通过不断研发反诈技术，采取多管齐下的管理政策，才能够助推科技跨越式发展，有效防止生成式人工智能成为诈骗“新武器”。

