用好实干这把“金钥匙”

实干，是最质朴的方法论，也是攻坚克难的金钥匙。习近平总书记强调：“要树立和践行正确政绩观，坚持从实际出发、按规律办事，自觉为人民出政绩、以实干出政绩。”本期大家谈，围绕实干这一主题，我们选刊3篇来稿，与大家一起分享3位作者的所思所悟。——编者

杜绝“只喊号子不拉纤”

河南省郑州市 郭桉

开局之年，各地担当作为、奋勇争先氛围浓厚，但也需警惕“只喊号子不拉纤”的现象。

比如，工作谋划存在调研不充分、思考不深入的问题，仅凭主观判断定计划、做方案；不推不动、不催不动，习惯听口令做动作、等指示抓落实，挑着干、慢慢干；缺少主动攻坚意识，不主动挑重担、解难题、攻难关。重表态、轻实干，就会让好思路、好方案止于“纸上”，滋生形式主义，甚至阻碍发展。

谋事是基础，干事是关键，成事是目的。杜绝“只喊号子不拉纤”，既要在思想认识上着力，引导干部牢固树立和践行正确政绩观，多想想群众需要什么、满意不满意，从中找突破口，攻克难点工作，解决棘手问题；也要在体制机制上下功夫，完善谋划、部署、推进、督查闭环机制，开展常态化跟踪问效，及时发现问题、加压提速。

坚持说了算、定了干、干必成，才能更好把规划图变成施工图、把任务单变为成绩单。

“等等看”不如“抓紧干”

河北省承德市 汪泽

“可能有风险，先等一等看”“举措没有先例，再观察观察”……有的干部在推进工作中，存在“等等看”的心态，习惯于等上级指示、等他人经验，缺乏敢闯、敢拼、敢试的劲头。

蓝图已绘就、条件已具备，落实就不容慢半拍、搞变通。以“等等看”作为托辞，实质是不作为、慢作为的体现。一方面，在于政绩观错位，或是不想干，不愿啃硬骨头，或是将“不出事”摆在“干成事”前面，不想为探索创新承担风险；另一方面，在于本领不足，面对新形势带来的新考验，缺乏破题思路，因本领恐慌只能一拖再拖。

一味“等等看”，很可能让一地错失发展机遇。“等等看”不如“抓紧干”。当然，“抓紧干”并非是不顾实情、不讲章法地蛮干乱干，而是要求干部既要有迎难而上、直面问题的担当和勇气，也要切实做到脚踏实地、摸清规律，在“实践—认识—再实践—再认识”的良性循环中推动事业发展。涵养只争朝夕的责任感与紧迫感，善学善思、边干边学，才能为发展添砖加瓦、增光添彩。

化难为易靠“笨功夫”

安徽省六安市 黄纯

常听到一些基层干部喊难：群众工作难做，规定的任务难落实，工作目标难实现。确实，基层工作十分繁杂，群众需求多元多样，做好哪一项工作都不容易。问题在于，如何化难为易？

路要一步一步走，事要一点一点干。我所在的社区里有个商业广场，每天产生大量餐饮垃圾，久而久之，垃圾转运点的异味影响到附近居民。经营的需求要照顾，群众的诉求要解决，怎么办？我们先是抓住“垃圾不过夜”这个关键，增加清运频次，确保少产生异味，随后又引入除臭设备，增加保洁人员。一步一个脚印，异味少了，环境好了，最后商户和住户都满意。把难题拆解开来，先抓主要矛盾，再一点一点攻克次要矛盾，问题清单就有可能逐步变成成效清单。

千难万难，下足“笨功夫”就不难。功夫重在平时。群众的思想“疙瘩”是什么？乡村、社区居民有什么新需求？抓好落实有哪些有利条件？不能浅尝辄止、走马观花，要把情况摸清楚、把实情了解透，如此，谋划才能切中要害，落实才能有的放矢，最终才能化难为易、取得良好成效。 **（来源：人民日报）**

网络法治须与技术创新同频共振

赵精武

近段时间以来，OpenClaw应用下载与使用情况火爆，其强大的自主决策功能吸引了不少用户安装体验。阿里、腾讯等互联网企业相继跟进部署服务，在社交平台上甚至出现了上门收费代装OpenClaw的服务，一场“养虾”热潮迅速升温。

与“豆包”“元宝”等公众熟知的人工智能产品不同，OpenClaw的突破在于电脑桌面端部署与开源生态：其接入基础模型应用程序编程接口，以系统权限调度本地与网络资源，并与移动端实时互联，从而打通了从指令到执行的闭环。在OpenClaw的帮助下，用户可通过自然语言指令让AI直接操作系统工具，实现文件整理、邮件发送、数据分析等全流程自动化，且可以在后台24小时运行，让智能体首次具备了真正意义上的“数字员工”属性。

然而，高度自主决策功能的实现，依赖用户开放足够的数据访问权限，这也意味着用户本地存储的文件、数据、密钥均处于风险不确定状态。从媒体公开报道看，部分用户已遭遇OpenClaw错误删除电子邮件、重要文档等技术故障。尤其需要注意的是，若用户未能正确卸载，残留文件仍会对用户的个人计算机产生安全威胁。这些风险的出现，也印证了技术创新背后机遇与风险并存的客观规律，人工智能技术也不例外。近期，国家互联网应急中心、中国互联网金融协会等部门也陆续发布风险提示，提醒公众重视安全风险，审慎安装。

2026年1月1日起施行的新修订的网络安全法明确提出，加强风险监测评估和安全监管，促进人工智能应用健康发展。当前智能体应用尚处于创新探索阶段，其存在的网络安全风险也确实为治理实践提出诸多新问题：一方面，智能体的功能定位是“私人定制”的专属服务，需要获取足够多的用户个人信息进行训练，进而形成符合用户使用习惯的信息服务模式，但这也让个人信息保护法中的“最小必要原则”面临被虚置的风险。由于智能体的作用是为用户提供全方位的便捷化服务，因此难以界定哪些信息属于实现其功能所“必要”的范畴。另一方面，以开源社区为依托的智能体应用技术更新周期极短，网络安全风险更为复杂。这既包括开源生态体系固有的技术漏洞、恶意代码植入等安全风险，也涉及高频率更新带来的质量不稳定、故障频发等问题。

人工智能技术的创新迭代，对现行网络安全法治体系提出了更高的延展性要求，即网络安全规范体系应当与人工智能技术保持同步规划、同步发展的状态。现行的网络安全法等法律法规已逐渐明确了核心治理逻辑和治理规则，因此当下的工作重点除了“立法”更要“释法”，即明确现有网络安全法律条款如何适用于智能体安全风险治理实践。

第一，网络安全法治体系需要延展网络安全风险的分级分类框架，为不同风险等级的智能体行为设置差异化的保护措施。例如，对于资金流出、安全配置修改等风险极高的行为，可一律禁止智能体自主执行；对于邮件回复等行为，则需要由人来进行最终确认。同时，要对不同领域的风险容忍度进行分级，在此基础上出台智能体技术应用的负面清单，并根据技术发展、产业动态等因素适时调整。如对涉及国家安全、金融安全及关键信息基础设施等高风险敏感领域，应明确禁止使用端侧智能体；对风险容忍度相对较高的领域，则可基于行业特征，明确不得使用智能体的具体场景。

第二，网络安全法治体系需要扩展智能体网络安全漏洞的专项治理措施。具体而言，可以考虑将提示词注入、视觉对抗攻击、数据“投毒”及其他针对多模态大模型感知、推理技术特征的攻击方式，纳入网络安全法所述的“恶意程序”和“安全缺陷、漏洞”范畴，从而将其纳入人工智能安全法律规制范围。

第三，网络安全法治体系需要囊括智能体开源社区与开源平台的主体责任。开源社区应当塑造开发者“技术向善”的伦理规范，防范开源社区和开源平台成为网络攻击的重灾区或中转站，通过社群规范等方式，强化安全风险提示与说明。

智能体应用的网络安全治理，既关系到人工智能产业的创新发展，也关系到我国现代化治理能力和治理水平的提升。面对智能体等人工智能技术难以预料的创新周期和发展方向，网络安全法治体系需以更灵活、全面的方式，预防相伴而行的风险，同时也要为技术创新预留探索空间，最终实现技术创新与法治体系的一体化发展。

（作者系北京航空航天大学法学院副教授、工业和信息化智慧法治工信部重点实验室执行主任） （来源：法治日报）

多做“口碑工程” 不搞“口号工程”

新华社记者 张丽娜

中部某地盲目上马“百亿级产业园”沦为“口号工程”，被媒体曝光后引发关注。近年来，一些地方“有轨电车”“物流新城”“仿古小镇”等项目，也因决策脱离实际，陷入拆留两难、后患无穷的窘境。这些“口号工程”变成“烂尾工程”，背后折射出一些党员干部政绩观出现偏差问题。

今年的政府工作报告提出，努力为人民群众多办实事。“十五五”规划纲要中，109项重大工程项目中民生工程达25项。实事办得实不实，工程建得好不好，一个重要标尺就是能不能成为百姓心坎上的“口碑工程”，而非劳民伤财的“口号工程”。

“天地之间有杆秤，那秤砣是老百姓。”政绩分量足不足，最终都要在这杆秤上称一称。

报表可修饰，数据可美化，现场可包装，民心无法作假。有一些党员干部在这杆秤前失了分寸、政绩观跑偏：有的败家子，把寅吃卯粮当“魄力”，留下一屁股债让群众戳脊梁骨；有的官油子，领导面前一套、群众面前一套，把芝麻吹成西瓜；有的表演派，眼里只有短期“轰动效应”，舆情来了连夜办，风头过了原样搁……凡此种种，病根都是政绩观出了问题。

“入党为什么，当‘官’干什么，身后留什么？”这个问题，每一位党员干部都应常思常想。真正的口碑，不在材料报表里，而在百姓心头上。离任多年，老百姓谈起那些年、那些干部，还会由衷地念叨一句“那届班子干了实事”，这才是沉甸甸的褒奖。不少打基础、利长远的工作，党员干部任期内可能看不到轰轰烈烈的效果，也许多年后才逐渐生发影响：当年种下的树苗已渐成荫、规划的项目已让群众得了实惠、培养的人才已成栋梁……这都是树立和践行正确政绩观的生动注脚。

金杯银杯，不如老百姓的口碑。当每一位党员干部都深明此理，那些急功近利的“口号工程”就会失去市场，惠及长远的“口碑工程”就能在百姓心中闪光。

使用大模型 要有批判性思维

南熙

人工智能飞速融入日常，大模型作为人工智能最主要的阶段性成果，已成为人们获取信息、辅助决策、创作内容的重要工具。很多人以为，大模型没有情绪、没有立场、没有私心，输出内容理应客观公正，然而，近日有媒体报道的AI（人工智能）“投毒”黑产，揭开了生成式AI商业化进程中的灰色地带。事实上，大模型从诞生到应用，从来都不是客观中立的存在，而是人类社会、技术规则与用户偏好三重倾向共同塑造的“数字投影”。

“机器无情感，是客观的”，是当下对人工智能最普遍的误解之一。这种误解忽略了一个核心逻辑：大模型的一切能力，都源于对人类数据的学习，它不会凭空产生“思想”，只会复刻、整合、放大训练过程中接收到的信息与倾向。大模型的“不中立”，并非技术缺陷，而是由数据、训练、使用三个环节共同决定的必然结果。

首先，训练数据自带偏见，AI学的就是“不完美的人类”。因此，大模型是社会偏见的“镜子”，甚至可能是“放大镜”“哈哈镜”。大模型的知识体系，建立在海量文本、书籍、新闻、论坛、网页等数据之上。这些数据不是凭空产生的，而是人类社会的数字化记录。而人类社会从来都不是绝对的，文化差异、历史叙事差异等都早已渗透在文字与表达中。

模型一边学习语言规律、知识关联，一边会不自觉地内化其中的“偏见”。如果部分数据对某一群体、性别、地域、文化带有负面描述，模型在无干预情况下，就可能输出歧视。它不会主动判断“对错”，只遵循数据里的概率。

其次，对齐过程植入价值观，让大模型自带“立场倾向”。为了让模型更安全、更有用、更符合人类标准，开发者会通过RLHF（基于人类反馈的强化学习）等技术进行“对齐”。简单说，就是让标注员对模型的不同输出结果进行排序或者打分，判断哪个更有用、更无害、更得体。这个对齐过程，看似在追求“规范”，实则是把人类的价值观植入模型。

标注员的文化背景、教育水平、道德观念、地域立场，都会直接影响“好答案”的评判标准。不同文化对同一议题的看法可能天差地别。当标注人员背景趋同、视角单一时，模型就会偏向这一群体的价值观。这种价值观不是极端的，而是润物细无声的——在社会议题、文化判断、道德选择中，悄悄偏向某一种共识，忽略其他合理视角。

最后，用户偏好引导偏见，AI很擅长“顺着你说”，大模型更像“迎合者”而非“裁判员”。

这一点，我们每个人都在经历，却很少察觉。你偏向什么观点，AI往往就顺着你说；你相信什么结论，AI就帮你找什么理由。它会不断强化你本来就相信的东西，让你待在舒适区里，慢慢困在自己的信息茧房，甚至是“思维茧房”。

如果说数据和训练是模型的“先天基因”，那么用户使用就是模型的“后天环境”。大模型的输出，高度依赖提示词、上下文与用户偏好。用户从提问开始，就自带立场、情绪和预设，而模型的优化方向，本就包含“理解用户、满足需求、提供情绪与逻辑认同”。

面对带有偏向的提问，模型很容易顺着用户的思路展开，强化其既有观点，而不是主动纠正。随着模型对用户习惯的记忆与适配越来越强，这种“迎合”还会更加明显：同样的问题，不同用户、不同提示词，可能得到完全相反的结论。

这三重偏见叠加，让大模型不可能做到“客观中立”。它不是一面客观反映世界的镜子，而是一台同时放大知识与偏见、智慧与狭隘的机器。这种非中立性，带来的影响远超想象：在招聘、贷款、教育评估等场景，模型偏见可能固化歧视；在公共舆论与信息获取中，会加剧立场对立、思维封闭；在跨文化交流中，还可能因文化偏见引发误解与冲突。人们越是盲目相信AI，越容易被其中隐藏的偏见误导。

认清大模型非中立的本质，不是否定其价值，而是为了更理性、更安全地使用它。首先要认识到，大模型是强大的工具，是高效的助手，是文化与知识的载体，但它绝不是真理的化身。然后，要真正负责任地使用它，例如不把模型答案当作唯一标准，重要决策坚持多源交叉验证；在公共场景使用时，引入伦理审核与人工监督；在技术层面持续优化数据与对齐机制，减少隐性偏见；对于每一个使用者，都应保持批判性思维。 **（来源：光明日报）**