

走好网上群众路线

践行全过程人民民主

□ 柴宝勇

协同治理转变。”我们需要充分发挥网络对于聚民心、汇民智、集民力的作用，为人民群众充分、有序参与到国家治理的各个领域创造便利条件，把全过程人民民主的制度优势更好转化为治理效能。

走好网上群众路线为发展全过程人民民主注入强大动力。一是有利于进一步筑牢社会主义民主政治建设的群众基础。全过程人民民主以党的领导为根本保障，党的领导地位和执政基础稳固，全过程人民民主才能逐步建立成熟的制度程序、形成完整的参与实践，全链条、全方位、全覆盖地发挥民主效能。通过走好网上群众路线，党的领导力量能够覆盖更广泛的社会发展领域，更充分地调动群众参与到社会主义民主政治建设中来。二是有利于促进党群干群关系的良性互动。互联网高效、便捷、平等、互动的特点，显著提升了民主制度的运行效率，有助于党领导人民群众依托互联网围绕特定议题及时展开沟通和协商，确保党的政策主张既符合人民群众期待，又能够激发人民群众的干事创业热情。三是有利于强化民主参与的整合能力。党的二十届三中全会提出：“走好新时代党的群众路线，把社会期盼、群众智慧、专家意见、基层经验充分吸收到改革设计中来。”全过程人民民主不仅要求各类社会主体平等表达意见，还要求协调利益冲突、整合社会力量、实现求同存异，通过完整的民主制度链条，凝聚更广泛的进步力量。走好网上群众路线注重发挥整合功能，促进各方面制度的衔接与配合，这一整合过程是在智能信息技术的辅助下对网上社情民意的甄别、筛选与融合，而非网络数据的简单相加。

走好网上群众路线对践行全过程人民民主提出了新要求。走好网上群众路线是新时代发展全过程人民民主、保障人民当家作主的必由之路，应树立系统思维，进一步画好网上网下群众工作“同心圆”。

一是将培养党员干部网络思维和提升群众用网能力结合起来。以现代网络技术为基础建立起的各种电子公共服务平台，已经成为联结人民群众和各级党委、政府的重要纽带，这要求党员干部深入把握新时代群众路线智能化、网络化要求，提升信息工作素养，避免失语失声，增强抵御意识形态风险、应对网络突发事件的危机意识。同时，用好宣传、教育等工作抓手，增强人民群众依法文明用网、抵制网络谣言的能力，引导广大网民合理表达建议诉求、有序参与政治生活。

二是将健全配套基础设施和提供完备制度供给结合起来。一方面，以现有社情民意征集平台为基础继续整合信息化资源，打造更加高效便捷、均衡持续的公共服务渠道，同时用好人智能、大数据、云计算等智能信息技术，实现各方面信息集成共享、各领域工作衔接配合，打造有助于提升人民群众参与感、获得感的网络工作模式。另一方面，制定有利于网民有序融入政治生活的制度规范，确保各行各业群众的网络政治参与在法治轨道上健康运行。

三是将线上平台交互联动和线上线下有机衔接结合起来。走好网上群众路线，就要利用好互联网的信息技术优势提升党领导各方面群众工作的实践效能，利用技术手段打破政务服务平台之间的“信息孤岛”，跨部门、跨系统打通社情民意征集渠道，形成“数字人大”“数字政府”“数字政协”等共建共享的政务信息服务体系，同时，遵循线上线下紧密融合的内在要求，打通全过程人民民主实践基地同政务服务平台的数据通道，把打造和优化人民建议征集系统的“先手棋”“慢功夫”在线下做实做足。

四是将发掘典型工作案例和推广民主参与经验结合起来。近年来，我国一些地区和部门以走好网上群众路线为牵引，不断创新网络上的民主参与形式，增强广大网民的民主意识和民主能力。要深入剖析走好网上群众路线在社会主义民主政治建设中的引领作用、工作路径以及在激发群众自治活力中的注意事项，加强宣传阐释和经验总结，发挥典型案例对基层实践的带动作用，在全社会营造走好网上群众路线的良好氛围。



如何应对大语言模型的法律风险

□ 苏 宇

大语言模型是基于深度学习技术构建的，能够处理和生成自然语言文本的复杂系统，当前已成为人工智能领域最引人注目的代表性应用之一，不仅在自然语言处理方面取得了显著成就，还在跨语言交流、智能客服、内容创作等多个领域展现出广阔的应用前景，对于培育和发展新质生产力、抓住新一轮科技革命和产业变革机遇而言有重要价值。与此同时，大语言模型也可能引发一系列风险，需要紧扣相关技术规律和产业特性，形成科学、系统、精准的治理思路，促成技术创新、产业发展与安全保障目标的融合实现。

从本质上说，大语言模型是一种从训练数据中学习一定模式的概率模型，训练数据、学习进程和应用过程都包含了复杂的风险来源，这些风险大致可归结为以下类别。

一是信息内容安全风险。在大语言模型的训练数据中，若存在质量缺陷、认知偏差或价值倾向等问题，模型在生成文本时就可能输出违法、不良或误导性的信息。更为复杂的是，模型还可能因为“模型幻觉”，即模型对训练数据的过度拟合或误解而产生错误的信息输出。随着网络空间中由大语言模型生成的信息越来越多，个人查询大模型以获取信息和知识的行为日益普遍，如对此不加规制，此种信息内容安全风险将日益复杂和庞大，甚至可能造成严重的认知误导和信息污染。

二是数据安全风险。训练大模型需要处理大量数据，应用大模型需要向大模型输入一定信息，在线精调和后训练等操作也需要向大模型提供各种数据，这些数据来源广泛，涵盖公

开数据集、网络爬取数据、用户生成内容等，每个环节都可能造成数据安全隐患。既可能因模型学习了敏感信息而被使用者通过一定方式推理、还原，也可能因用户向模型提供敏感数据或个人信息而被国内外相关服务提供者获取，存在安全漏洞。

三是恶意利用风险。由于大语言模型学习了广泛的知识 and 信息，部分模型甚至具备编写和修改代码的能力，这使得它们有可能被不法分子恶意利用于制作病毒木马、制造危险物品、生成诈骗素材等违法犯罪活动。尽管模型开发者通常会设置一定的安全防护措施，但这些措施大部分比较容易攻破，难以完全抵御恶意攻击者的技术手段。因此，恶意利用风险始终是大语言模型法律治理中的一块难啃的硬骨头。

四是侵权风险。在训练模型时，收集和处理数据可能侵犯他人的知识产权和个人信息；在模型应用时，输出的信息也可能构成对公民名誉权、隐私权等权益的侵害。特别是在多模态大模型领域，由于其融合了图像、音频等多种信息形式，使得侵权问题更加复杂和多样。近年来，国内外已经出现了一系列涉及大模型的法律纠纷和司法裁判，引起社会关注。

在上述风险之外，大语言模型的训练和应用还可能引起多种其他风险，如学术不端风险、大规模劳动岗位替代风险、输出错误行动指令的风险等。大语言模型属于新生事物，其技术基础、行业应用和产业链条都在快速发展演化之中，对大模型的风险治理并无现成的成功经验可循，各种治理工具仍处于探索阶段。不仅如此，大语言模型的法律治理还需要兼

顾发展和安全、国际竞争和生产关系变革等不同方面的考量，应对这一挑战并非易事。

习近平总书记指出：“谁能把握大数据、人工智能等新经济发展机遇，谁就把准了时代脉搏。”大语言模型在人工智能的发展中占据关键位置，把握时代脉搏、应对治理挑战刻不容缓。我们不能等到大语言模型的风险充分暴露、治理措施及其技术基础完全成熟才着手展开治理，而是应当及早研判风险、梳理需求、整合可用技术、探索措施组合，基于合理可行的原则，逐步形成有针对性的治理路径。

一是平衡多重目标。人工智能的治理不能陷入单纯的风险规制视角，相关法律与政策应兼顾伦理维护、风险防控、创新激励、市场培育、权益保障等多方面的目标，寻求最佳的多目标融合实现方案。当前，大语言模型之间的竞争涉及人类科技“奇点”的抢占：谁先实现真正意义上的通用人工智能（AGI），谁就在未来的科技竞争乃至综合实力竞争中占据优势。我们必须加以高度重视，既要牢牢守住底线，又要想方设法使相关规制目标以负担较轻的合理方式融入模型开发与应用过程，避免影响人工智能底层技术发展、限制人工智能产业的创造性与竞争力。

二是保持规制弹性。鉴于大语言模型技术、应用、业态、产业都在不断发展演化，相关的立法应保持足够的弹性以应对技术创新、产业发展和风险治理的不确定性，避免刻舟求剑。保持“规制弹性”并不等于不需要“规制刚性”，而是需要根据新技术、新趋势、新证据，及时调整各项风险认知与评价结果，并通过法治方

式精细调整和更新规制措施，同时保持制度预期的稳定性。

三是探索综合治理。大语言模型及其应用有独特的技术规律和产业特点，需要建立健全相应的“治理工具箱”，不能寄希望于单一的规制措施或治理工具。在算法备案和技术标准等已有治理工具的基础上，还需要探索发展模型测评、红队测试、算法解释、应急预案、监管沙盒、安全港等“工具包”及其组合运用方案，通过治理工具的选择、配合与结构化调整实现精准治理。对于大模型的法律治理而言，开源生态培育、基础模型安全、领域模型监管、测评体系构筑、规制负担分配等关键难题，对于整个人工智能的发展和安举足轻重。我们应深入研究切实可行、动态迭代的组合式治理方案，逐步充实和完善人工智能法治体系。

四是加强国际合作。基于人工智能产业发展与风险链条全球联动的特点，人工智能的治理应积极加强国际合作，既有利于寻求主动形成价值与制度共识，也有利于预判外部风险、增强国际支持和形成治理合力。在加强国际合作的过程中不可避免遭遇国际规则博弈，这就更需要提前谋划，充分研判可能由外部输入的技术、产业与监管风险，在规则协调、技术普惠、安全可控等方面不断取得突破，以确保人工智能的发展符合全人类的共同利益。



共同织就更牢固的人脸识别“安全网”

□ 丁晓东

侵害消费者的合法权益。

建立精准化、差异化的治理体系是应对人脸识别风险的关键。一是落实好“非唯一验证”原则。《办法》第十条明确规定，“实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，应当提供其他合理、便捷的方式”。这一规定明确了人脸识别作为验证方式的非唯一性，兼顾人脸识别技术所带来的效率与隐私考量，对相关主体提出了更高的服务要求，也是让公众个人隐私得到真正尊重的应有之举。为了落实这一原则，相关主体应当在产品设计阶段就嵌入多元化认证机制。例如，金融机构可以开发“刷脸+短信验证+人工复核”的多层次认证系统；社区物业可以保留传统门禁卡与数字密码并行的出入方式，既确保安全性，又尊重居民的选择权。特别是，应建立便捷的申诉渠道，当人们遇到强制刷脸等情况时，能够通过投诉举报等途径有效维护自身权益。二是强化特殊群体保护。未成年人由于其身心发育特点，对人脸识别的风险缺乏必要的认知和警惕性，甚至有的由于好奇心驱使而轻易向平台提供其人脸信息，这些信息如被擅自分析、泄露或被滥用，可能对其成长产生不利影响，甚至导致其成为一些犯罪行为（如绑架拐骗）的受害对象。对未成年人的个人信息特别是敏感信息给予特别保护，是各国的普遍做法。《办法》不仅规定处理不满十四周岁未成年人人脸信息时，应当取得其父母或其他监护人的同意，还要求个人信息处理者在存储、使用、转移、披露等方面制定专门的处理规则，以充分保护未

成年人个人信息安全，为未成年人营造一个健康成长的环境。此外，对于残疾人、老年人等而言，可能会遇到人脸识别障碍，导致他们不仅享受不了刷脸的便利，还可能在办理银行、人社、医保、交通出行等相关事务时受阻。《办法》规定，对于处理残疾人、老年人人脸信息的，还应当符合国家有关无障碍环境建设的规定。这就要求相关主体在系统设计中应充分考虑无障碍需求，不能将无法刷脸的特殊人群关在“门外”，确保技术应用包容性。三是严格限制私密空间应用，划清人脸识别的边界。在公共场所安装人脸识别设备，应当为维护公共安全所必需，依法合理确定人脸信息采集区域，并设置显著提示标识。同时，除法律明文规定的情况外，对更衣室、卫生间等明确属于私密空间的区域，应当全面禁止安装人脸识别设备。

全流程风险防控是强化人脸识别安全性的重要保障。我国个人信息保护法第二十八条第二款规定，“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息”。人脸识别信息作为敏感个人信息，其应用也应当遵循特定目的、充分必要、严格保护措施的要求，建立起全周期的治理方式。一方面，保护关口应当进一步前移。个人信息处理者在应用人脸识别技术处理人脸信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知处理人脸信息的必要性以及对个人权益的影响，当获取个人在充分知情前提下所作出的自愿、明确、单独同意后，才能实施人脸信息的抓取与处理。《办法》引入了备案机制，规定人脸识别数据的个人信息处理者在“人脸信息存储数

量达到10万人之日起30个工作日内向所在地省级以上网信部门履行备案手续”，要求提供基本情况、处理目的、处理方式以及操作规程等内容，既给企业划定了合规红线，也为监管部门提供了治理抓手。下一步，应当进一步细化备案标准和程序，确保备案工作的顺利开展。另一方面，定期审计与及时销毁同样重要。我国某些地方的企业已经引入了“数据保质期”概念，对超过使用期限的人脸数据自动触发删除程序，而对于必要保留的数据，则每季度进行安全评估，及时发现并修补漏洞。这种动态化管理模式不仅有助于保护个人隐私安全，还能有效防止数据泄露风险的发生。这样的探索值得借鉴和推广，以提升行业的数据安全管理水平。

平衡技术发展与安全保障是推进人脸识别规范化的基本原则。《办法》第二条明确其调整对象为我国境内“应用人脸识别技术处理人脸信息的活动”，同时规定“在中华人民共和国境内为从事人脸识别技术研发、算法训练活动应用人脸识别技术处理人脸信息的，不适用本办法的规定”。这一对技术研发活动的豁免条款，体现了立法者对创新规律的尊重，为人脸识别技术的研发预留了空间，有利于相关产业的发展。在落实《办法》的过程中，既要严格执行相关的禁止性规定，守住安全底线，也要为技术创新预留合理空间，特别是在医疗健康、公共安全等民生领域，应积极推动人脸识别技术的应用走上更加规范、健康的发展轨道，共同营造一个安全、可信、可控的社会环境。



发展全过程人民民主