

跨境电信网络诈骗：你会不会成为下一个受害者

□ 王惠茹

近年来，随着互联网技术应用的迅猛发展，跨境电信网络诈骗活动猖獗，成为威胁人民群众人身财产安全的社会公害。特别是随着基于人工智能的“深度伪造”、群聊群控等诈骗手法的传播和应用，跨境电信网络诈骗呈现出犯罪分子隐蔽性强、技术手段智能化高、风险群体集聚放大、运作方式集团化链条化、跨境电子证据调取难、侦查破案惩治难等显著特点。我国通过源头治理和综合治理防范电信网络诈骗已经取得一定成效，但仍然面临一些技术痛点难点，创新反制诈骗的技术防范治理体系成为当务之急。

打击跨境电信网络诈骗的技术治理难点

随着人工智能技术在电信网络诈骗领域的不断应用，诈骗实施者在精准信息获取、诈骗脚本设计、通信联络诱导、资金支付转移等方面的能力大幅提升，给打击治理电信网络诈骗带来新挑战。基于高科技设备、软件和算法的短信群发、电话改号、后门攻击、网银支付、AI换脸、拟声技术，为下游网络诈骗犯罪活动提供了土壤。凭借新颖的诈骗技术、精巧的诈骗脚本、逼真的换声换脸音视频，五花八门的电信网络诈骗让人防不胜防，成为当前电信网络诈骗治理的痛点难点。

尤其是人工智能技术为跨境电信网络诈骗防范治理工作带来新挑战。第一，在软件和算法方面，当前大量通过互联网开源社区直接对外公开发布的人工智能技术被诈骗分子不当利用，增加了人工智能技术滥用的社会风险与隐患。第二，在硬件设备方面，伪基站、虚拟网络设备、虚拟拨号设备等因其远程化、匿名化、移动化、智能化特点，成为不法分子实施诈骗、逃避追查的主要工具。第三，生成式人工智能和深度伪造技术迅猛发展，但与之相应的伪造识别技术研发难度更高、发展速度更慢。第四，由于电子设备存储数据及其软件的使用痕迹可擦除、可篡改，现有技术平

台在对电信网络诈骗进行电子证据提取和锁定、精准溯源方面的应对能力尚显不足，有待进一步探索和提升。第五，对人工智能应用在数据采集、传输、存储、使用、共享等各环节的隐私保护、数据安全等方面的监督力度亟待加强。尽管防范电信网络诈骗的企业责任监管体系在电信行业相对完善，但是在人工智能技术和业务快速发展的互联网相关领域的监管执行力度仍相对较弱，对于当前涉诈风险较大的群呼网关类人工智能设备的监管政策和管理方式仍需深入探讨。

人工智能技术在跨境电信网络诈骗防范治理中的应用

针对跨境电信网络诈骗犯罪的特点，网络攻防、信息化、大数据分析、机器学习、声纹特征识别、自然语言理解、智慧图谱、智慧安防等数字技术在公安机关打击防范电信网络诈骗犯罪工作中已有深入应用及探索，电信网络诈骗技术防范系统的识别准确度更高、监测拦截实时性更强、防护覆盖面更大，为推进当前治理工作提供了有力支撑，有效降低了电信网络诈骗的传播风险与社会危害。可以说人工智能技术在电信网络诈骗防范治理中的应用大有可为。第一，利用大数据相关性分析技术，可以对伪基站的移动轨迹、诈骗信息脚本、犯罪目标等主要犯罪要素进行识别和关联分析，有助于构建动态、精准与高效的网络空间安全威胁感知预警体系，有效提高警务预测的准确率，实现快速串案并案，提高破案效率。第二，利用自然语言处理、样本标记、特征选择、模块分析、用户画像等技术，可以精准识别诈骗电话、受害人以及潜在易感人群，有助于更有针对性地采取反诈预警或预防措施。第三，利用深度学习技术，可以主动生成与快速调整网络威胁防御策略，推动构建适应性强、反应迅速灵敏、分布式协同与演进优化的网络空间安全威胁主动防御体系。第四，利

用开放式框架、人机交互技术，可以构建具有安全控制功能的现场调控，使反电信网络诈骗系统不断完善其使用功能。第五，利用数字融媒体技术，构建数字媒体技术平台的反电信网络诈骗宣传体系，全面提升用户对电信网络诈骗的防范意识。

近年来，我国基于云计算、人工智能、大数据等技术，综合采取多种防范措施深入推进打击治理电信网络诈骗违法犯罪工作，陆续推出了国家反诈中心APP、预警劝阻专线、涉诈预警劝阻短信系统等反诈利器，为人民群众构筑起全方位、多形式、深层次的反诈“防火墙”，运用科技手段助力全民反诈取得良好成效。我国应进一步加强电信网络诈骗的反制技术研究，将人工智能技术应用于诈骗预警、嫌疑人识别、侦查破案等各个环节中，形成协同式、系统性的技术治理架构。

打击跨境电信网络诈骗的治理手段

面对来势汹汹、花样迭出的新型电信网络诈骗，要坚持以技制技、以网制网，建立多层次、立体化的打击跨境电信网络诈骗技术治理体系，完善人工智能技术应用法律规制，压实打击治理新型电信网络诈骗的各方主体责任。在技术应用的法律规制层面，我国适时出台了《网络音视频信息服务管理规定》《互联网信息服务合成管理规定》《生成式人工智能服务管理暂行办法》《人脸识别技术应用安全管理规定（试行）（征求意见稿）》，不断提升对人工智能技术应用的规范水平，对防治人工智能诈骗起到一定的约束作用。

在实践层面，我国要进一步建立健全反制电信网络诈骗的技术防范屏障。一是建立跨行业、跨部门的数据融合共享和系统联动，加强全国互联网反诈平台、部省级系统、基础电信企业、重点互联网企业的数据共享和联动处置机制，以实现对方数据的及时汇总和综合分析，满足多种应用场景的数据分析及预警需要。二是建

成国际、国内、网间、网内不同源头的诈骗电话防范系统，建立诈骗电话监控拦截系统和黑白名单管理系统，实现对不同源头诈骗电话实时监测处置，形成部省级系统协同联动的整体性技术防范体系。三是加强金融部门对银行卡办理、网银转账等业务的审核和监管，特别是加强对第三方支付平台的监管力度，对可疑交易账户建立快速止付和账户冻结机制。四是加强电信行业的整顿和规范力度，严格落实电话用户实名登记制度，严禁违规放号改号和违规租用线路，加快研发科技监管措施，打击利用虚拟拨号技术实施诈骗。五是加强对于前端的程序编写、脚本设计、伪基站等技术设备生产、非法提供个人信息等上游产业的查处力度，切断网络诈骗的技术支持。

除此之外，在打击电信网络诈骗的法律体系建设层面，我国相关法律法规体系要不断健全。全国人大常委会先后通过反洗钱法、关于加强网络信息保护的决定、网络安全法、个人信息保护法、反电信网络诈骗法，刑法、民法典也针对电信网络诈骗进行了相关规则修订，形成了多部门各司其职、协同治理电信网络诈骗活动的相对完善的治理制度，为有效打击遏制电信网络诈骗提供了法治保障。此外，我国还要与电信网络诈骗犯罪分子所在国家加强跨境执法领域的国际合作，搭建跨境调查取证、电子证据交换和警情联络分享平台，实现对跨境电信网络诈骗的识别、拦截、追踪和惩治。

面对不断迭代的电信网络诈骗手段，以更强大的科技力量震慑和打击不法分子是信息时代打击电信网络诈骗的必然趋势。要充分发挥现代技术手段在社会治理中的积极作用，推动打击电信网络诈骗治理向智能化、数字化转型。



防范人工智能给决策带来风险

□ 王艺潼

习近平总书记指出，“人工智能是引领新一轮科技革命和产业变革的战略性技术，具有溢出带动性很强的‘头雁’效应。”人工智能的快速发展不仅推动经济社会的深刻变革，同时也为政府决策模式的变革提供了新路径，对于建立健全大数据辅助科学决策机制、全面提升政府决策科学化民主化水平具有重要意义。

信息是决策的基础，但信息规模越大，结构性越复杂，意味着处理难度也越大。与人类决策相比，人工智能技术可以更加高效、快速、准确地搜集和处理海量非结构化数据，并将主次矛盾、因果关系、约束条件等呈现出来，为确定政策目标提供有价值的参考，便于决策者把握决策需求、认清问题症结、抓准主要矛盾、科学制定对策。

人工智能的机器学习方法可以通过分析数据中的模式和规律，自动训练和模拟模型，更加精准地预测潜在问题和风险的发生概率、复杂性与严重程度，事前预估不同政策方案实施后果，从而帮助决策者设置政策议程、优选政策方案。同时，人工智能的自然语言处理技术和文本情感分析技术使政府与公众可利用文字、声音、图片等多种形式进行互动，这不仅拓宽了公众参与决策的渠道，还丰富了政府回应民众诉求的途径，提高政府决策的透明度。政府还可利用计算机识别技术和深度学习技术对海量民意进行识别、整理、分析，了解公众共同的利益诉求、把握“最大公约数”，进而制定更符合民意的政策，实

现价值聚合，提高政府信任度。

尽管人工智能提高了政府的决策能力，但也给政府决策带来诸如决策失误等相关问题。

一是公平性风险。公平是政府决策的核心价值之一，但数据偏见和算法偏见使人工智能辅助政府决策面临公平性风险。一方面，大数据虽是海量数据，但却不是全数据。与理想化的全数据相比，大数据反映的现实是不完备的，例如，一些数字素养较弱群体的数据信息就难以被人工智能抓取。在带有“参与者偏差”的不完备数据基础上进行的决策可能会延续数据本身蕴含的价值偏差，加剧社会不公平。另一方面，算法决定了海量数据的应用方向及其计算效果，而算法设计过程中难免受到研发者价值倾向的影响。当前绝大多数算法由经营主体开发，其价值导向与公共部门未必完全一致，加之算法黑箱的存在使政府决策的公平性难以得到有效保证。

二是安全性风险。利用人工智能技术辅助政府决策通常需要收集大量数据，其中包含涉及个人隐私、商业机密、国家安全等敏感信息。有些信息单个或少量的存在并不敏感，但海量汇聚和挖掘分析后可能具有一定的敏感性。如果这些数据未能受到足够保护，可能会造成数据滥用甚至泄露，不仅损害个人和企业的隐私权，还可能对国家安全构成威胁。

三是伦理风险。算法和技术的加入使政府决策的影响因素日益复杂，原有的权责配置发生变化，造成责任主体虚化，带来伦理风险。运用人工

智能辅助政府决策在一定程度上赋予了算法与技术决策权，一旦出现算法失灵，就会导致决策失误，公共利益受损。由于人工智能算法并不拥有责任主体地位，因此，决策失灵的责任追究和政治问责出现困境。

为防范人工智能技术给政府决策带来的风险，更好地推动人工智能赋能政府决策，需要在审视现行决策模式和制度基础上，针对人工智能技术的特点，采取多方面措施。

一是建立参与式算法决策框架。公共的价值观既包括决策结果的公平公正，也包括决策过程的公开参与。为化解因数据偏见和算法偏见带来的公平性风险，一方面，吸纳政策利益相关主体代表参与算法设计与构建，提高算法的公开性和透明性，将公共价值融入算法设计中去。另一方面，加强对算法决策的前期审核与后期评估，建立人工智能辅助政府决策的伦理审查机制，组织技术专家、公众和协会等定期参与伦理审查，防范人工智能辅助政府决策的伦理风险。

二是加强适配算法决策的制度建设。一方面，建立算法救济制度。算法的不透明性与不可解释性客观上压缩了公众遭遇算法不公时的申诉与反馈渠道。为此，在制度上保障公众的知情权、选择权与要求人工介入权，畅通算法决策的救济渠道，及时根据公众意见修正算法缺陷，矫正价值偏差。另一方面，建立算法问责制度。当基于特定算法决策严重损害公共利益时，立即开展算法问责，清晰判定算法开发者、审查者和实施者责任，

倒逼各方以更高价值标准开发、审查和执行决策算法。

三是注重复合型人才的分散化储备。兼具技术能力和决策能力的复合型人才才是推动人工智能赋能政府决策的关键，可以有效降低决策人员与技术专家之间的沟通成本，预估并规避算法决策的潜在风险。而复合型人才在少数组织的过度集中可能阻碍技术进步，更可能导致掌握人工智能前沿技术的大企业不当介入和影响政府决策。为此，政府积极设立专门的人工智能技术部门，促进复合型人才的分散化储备，建立与经营主体的日常性互动及合作，掌握前沿技术进展，增强利用人工智能技术辅助决策的主动性。

四是动态选择决策模式。根据算法对决策过程主导性的高低，可将决策模式分为算法主导型、算法辅助型和算法咨询型三类。虽然人工智能为提高政府决策能力提供了重要的技术价值，但目前的算法决策仍然是一种有限理性的决策输出，还需要发挥人类决策在价值判断和自由裁量上的优势。因此，既要在制度上明确算法决策的地位和权限，赋予算法决策应有的权威，也要根据决策任务的复杂性审慎选择决策模式，实现人类决策与算法决策的耦合协同，有效防范政府决策风险。

