『神奇动物』风险暗藏

当前，一些追求潮流、猎奇的宠物爱好者，掀起饲养“异宠”的热潮。但“异宠”交易、饲养、救治、弃养等行为潜藏安全风险，关乎生态安全和生物安全，需加以重视。

资料图片

关于“异宠”知几何？

“异宠”是“异域宠物”或“另类宠物”的简称，是指有别于传统猫、狗等宠物之外，被人们当作宠物饲养、观赏和经济利用的外来野生动物，既包括昆虫等无脊椎动物，也包括鸟、兽、两栖、爬行等脊椎动物。

全球野生动物每年的贸易额逐年增长，涉及数十亿野生动物，人们对“异宠”的关注度也越来越高。在我国，“异宠”需求和交易正快速增长，《2025年中国宠物行业白皮书（消费报告）》显示，2024年，饲养“异宠”的人群持续上升；有数据统计，我国已有约1707万人在饲养“异宠”，市场规模逼近百亿元人民币；社交平台上，分享养宠攻略和“盘玩”秘籍的博主比比皆是。

然而，人类饲养“异宠”的历史普遍较短，对它们携带的病原微生物以及在交易、养殖过程中可能造成的疫病传播尚缺乏深入了解和有效对策，容易引发各种潜在风险。

“异宠”真的“易宠”吗？

2023年中央一号文件首次将加强对“异宠”的管理纳入其中，强调要“严厉打击非法引入外来物种行为，实施重大危害入侵物种防控攻坚行动”“加强‘异宠’交易与放生规范管理”。那么，“外来物种”究竟如何定义，又是否等同于“外来入侵物种”呢？让我们一同看看我国《外来入侵物种管理办法》怎么说？

外来物种。是指中华人民共和国境内无天然分布，经自然或人为途径传入的物种，包括该物种所有可能存活和繁殖的部分。任何单位和个人未经批准，不得擅自引进、释放或者丢弃外来物种。

外来入侵物种。是指传入定殖并对生态系统、生境、物种带来威胁或者危害，影响我国生态环境，损害农林牧渔业可持续发展和生物多样性的外来物种。

事实上，大多数受热捧的“异宠”在国内没有自然分布，属于外来物种，它们可能在新环境中缺乏本土天敌等生物和非生物制约因素，在生存竞争中处于优势，会抢夺和挤占本土物种的食物资源和生存空间，导致本土物种的生存及其所在的生态系统受到冲击。一旦这些“异宠”逃逸或被弃养，极有可能破坏生物多样性和生态系统稳定，威胁我生物安全，甚至会引发生态灾难。

国家安全机关提示

“异宠”可以宠，但不能随意宠，在追求新奇与热爱的路上，唯有理性和依规，方能使人与自然和谐共舞。广大公民应提高国家安全意识，自觉防范“异宠”饲养潜在安全风险，争当生物安全防线“守护人”。

遵守法律。《中华人民共和国生物安全法》规定，任何单位和个人未经批准，不得擅自引进、释放或者丢弃外来物种。《中华人民共和国刑法》规定，违反国家规定，非法引进、释放或者丢弃外来入侵物种，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。任何公民和组织应严格遵守相关法律法规，依法依规开展“异宠”交易、饲养、运输和放生等，坚决筑牢维护生态安全和生物安全的人民防线。

理性饲养。“异宠”消费者购买前需确认物种是否属于《国家重点保护野生动物名录》或《濒危野生动植物种国际贸易公约》附录中的物种，并核查商家资质。购买时应选择合法养殖场，拒绝走私或野外捕获的动物，同时要求商家提供检疫证明，观察动物是否活跃、有无异常分泌物等，慎养善养宠物。

广大公民如发现可疑线索，可通过12339国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关举报。

人工智能安全新挑战，警惕“数据投毒”

当前，人工智能已深度融入经济社会发展的方方面面，在深刻改变人类生产生活方式的同时，也成为关乎高质量发展和高水平安全的关键领域。然而，人工智能的训练数据存在良莠不齐的问题，其中不乏虚假信息、虚构内容和偏见性观点，造成数据源污染，给人工智能安全带来新的挑战。

数据是人工智能的基础

人工智能的三大核心要素是算法、算力和数据，其中数据是训练AI模型的基础要素，也是AI应用的核心资源。

提供AI模型的原料。海量数据为AI模型提供了充足的训练素材，使其得以学习数据的内在规律和模式，实现语义理解、智能决策和内容生成。同时，数据也驱动人工智能不断优化性能和精度，实现模型的迭代升级，以适应新需求。

影响AI模型的性能。AI模型对数据的数量、质量及多样性要求极高。充足的数据量是充分训练大规模模型的前提；高准确性、完整性和一致性的数据能有效避免误导模型；覆盖多个领域的多样化数据，则能提升模型应对实际复杂场景的能力。

促进AI模型的应用。数据资源的日益丰富，加速了“人工智能+”行动的落地，有力促进了人工智能与经济社会各领域的深度融合。这不仅培育和发展了新质生产力，更推动我国科技跨越式发展、产业优化升级、生产力整体跃升。

数据污染冲击安全防线

高质量的数据能够显著提升模型的准确性和可靠性，但数据一旦受到污染，则可能导致模型决策失误甚至AI系统失效，存在一定的安全隐患。

投放有害内容。通过篡改、虚构和重复等“数据投毒”行为产生的污染数据，将干扰模型在训练阶段的参数调整，削弱模型性能、降低其准确性，甚至诱发有害输出。研究显示，当训练数据集中仅有0.01%的虚假文本时，模型输出的有害内容会增加11.2%；即使是0.001%的虚假文本，其有害输出也会相应上升7.2%。

造成递归污染。受到数据污染的人工智能生成的虚假内容，可能成为后续模型训练的数据源，形成具有延续性的“污染遗留效应”。当前，互联网AI生成内容在数量上已远超人类生产的真实内容，大量低质量及非客观数据充斥其中，导致AI训练数据集中的错误信息逐代累积，最终扭曲模型本身的认知能力。

引发现实风险。数据污染还可能引发一系列现实风险，尤其在金融市场、公共安全和医疗健康等领域。在金融领域，不法分子利用AI炮制虚假信息，造成数据污染，可能引发股价异常波动，构成新型市场操纵风险；在公共安全领域，数据污染容易扰动公众认知、误导社会舆论，诱发社会恐慌情绪；在医疗健康领域，数据污染则可能致使模型生成错误诊疗建议，不仅危及患者生命安全，也加剧伪科学的传播。

筑牢人工智能数据底座

加强源头监管，防范污染生成。以《网络安全法》《数据安全法》《个人信息保护法》等法律法规为依据，建立AI数据分类分级保护制度，从根本上防范污染数据的产生，助力有效防范AI数据安全威胁。

强化风险评估，保障数据流通。加强对人工智能数据安全风险的整体评估，确保数据在采集、存储、传输、使用、交换和备份等全生命周期环节安全。同步加快构建人工智能安全风险分类管理体系，不断提高数据安全综合保障能力。

末端清洗修复，构建治理框架。定期依据法规标准清洗修复受污数据。依据相关法律法规及行业标准，制定数据清洗的具体规则。逐步构建模块化、可监测、可扩展的数据治理框架，实现持续管理与质量把控。

国家安全机关将在以习近平同志为核心的党中央坚强领导下，全面贯彻总体国家安全观，与有关部门一道防范针对我人工智能领域的数据污染风险，依法维护人工智能安全和数据安全，不断筑牢国家安全屏障。

（均转自国家安全部微信公号）

责任编辑/王睿卿 E-mail:fzbfzyzk@126.com