近几年，科技企业在推广新一代信息技术产品时，数据安全、数据隐私等问题广受诟病。数据作为驱动人工智能快速发展的重要基础，其安全也决定了人工智能的安全。人工智能的加速发展给数据的安全治理带来了新的机遇和挑战。

视觉中国供图

# AI解锁无人时代 仍需数据安全保驾护航

◎侯树文 本报记者 王 春

验证码登陆、移动在线支付、人脸识别门禁……

随着新一代信息技术的发展，互联网和人工智能技术应用蓬勃发展，数据也被视为一种无形的资产。然而，技术是一把双刃剑，在给我们生产生活带来效率提升的同时，伴随的安全问题也不可忽视。

近几年，科技企业在推广新一代信息技术产品时，数据安全、数据隐私等问题广受诟病。数据安全成为当今数字化转型时代的关键紧迫议题。

在7月8日至10日举行的2021世界人工智能大会上，数据安全、数据治理、网络安全等问题备受关注。业界认为，在人工智能深入推进城市数字化转型过程中，企业应积极主动接受监管，推动产业健康持续发展。

## 数据安全治理面临新的机遇和挑战

近日，桔视记录仪等25款App因存在严重违法违规收集使用个人信息问题，被国家互联网信息办公室依据《中华人民共和国网络安全法》相关规定，通知应用商店下架。

此前，在上海车展特斯拉车主维权事件中，特斯拉公布了维权车主车辆事发前半小时的行车数据。该行为引发了众多争议：车企该不该将行车数据公开？人们如何确定数据的可靠性？

没有大数据的收集和基础，人工智能是无本之木。数据作为驱动人工智能快速发展的重要基础，其安全也决定了人工智能的安全。人工智能的加速发展给数据的安全治理带来了新的机遇和挑战。

“大数据驱动业务的开展，让数据安全对城市运转变得前所未有的重要，数据一旦遭到攻击，就意味着业务会停转，将造成严重的经济损失和社会后果。”360公司创始人、董事长兼CEO周鸿祎表示，最近几年，360公司接到大量医院的报警，称医院网站被勒索软件攻击之后不能进行手术，不能给病人挂号看病。

近年来，城市也成为了网络勒索的重要目标，而且网络攻击的对象不仅限于电脑、手机、设备、系统，还逐渐扩展到数据。人工智能数据的获取、处理和应用具有极强的隐私性与领域扩展性，关乎个人信息安全甚至国家信息安全。对政府、城市公共事业单位的数据勒索，会造成城市运转和服务陷入停摆。今年5月，美国最大的燃油输送管线遭遇网络攻击被迫关停，导致美国东海岸45%的汽油、柴油等燃料供应受到影响。

业界认为，针对上述情况，要让人工智能技术的头顶上高悬一把达摩克里斯之剑。

## 数据输入、分析等过程都存在相应风险

数据非法跨境流通可能危害国家主权和国家安全；数字信息的过度采集和非法使用，可能侵犯公民的权利和隐私；算法的偏好可能加剧社会的偏见或歧视，威胁公平正义；无人驾驶汽车紧急避险等智能决策可能威胁特定人群的生命……

全国政协社会和法制委员会副主任陈智敏在人工智能大会安全高端对话上指出，人工智能发展与安全发展风险同时并存，这不仅是一个技术问题，也是一个安全问题，同时还涉及伦理、法律和国际规则等相关问题。

国家工业信息安全发展研究中心副主任何小龙在人工智能大会上表示，人工智能带来的数据安全问题一方面加速了传统数据安全问题。人工智能大规模的运用使得过度采集数据安全问题进一步加剧。另一方面，也带来了新型数据安全的问题。人工智能的算法对数据具有较强的依赖性，可能会带来数据投毒等新型数据安全挑战。

算法、模型和数据构成机器学习三大基石。腾讯朱雀实验室首席AI安全专家朱季峰在人工智能大会主题论坛上表示，以算法构建过程中上下游的产业链来看，数据的输入、数据的分析、模型的训练、模型的决策、模型的上线部署应用以及模型的改造过程当中都存在相应的风险。

例如，在数据输入环节，如果攻击者控制了数据来源，或者攻击者能够对收集数据的设备本身产生安全攻击，最终将通过这个链条影响到算法模型。如通过超声波影响陀螺仪，最终可以使无人机坠落。或者在模型决策阶段，可以通过物理攻击，使得自动驾驶车辆最终视觉识别系统出问题，这样可能影响车辆自动行驶或者对行人的判断。

随着人工智能的应用，技术的滥用带来失控风险。验证码验证机制首当其冲。朱季峰介绍，早在2017年，地下的黑产就已经开始用机器学习的方法做二维码识别训练。资料表明，80%以上验证的准确性都可以通过机器学习算法自动完成线上的注册，这就产生了一系列的安全问题。

## 3大系统共筑数据安全防火墙

人脸识别技术依托于对海量视图数据的分析，因而数据安全直接影响着人脸识别技术的实战应用。人工智能技术在安防领域的应用是技术寻求落地进程最快、应用最早的训练场。

达闼创始人、董事长兼CEO黄晓庆表示，从数据采集到数据处理到数据传输，解决数据网络安全问题有很多手段。从网络和数据角度要完成三个重要的任务——物理隔离、网络隔离、应用端到端的保护。

除了技术，我国利用法律武器在数据立法上也做出了探索。

今年6月，我国颁布了《数据安全法》，9月1日将开始正式实施。《数据安全法》提出以数据分级分类为核心，搭建数据安全的监管制度，要求强化落实各级数据处理活动主体数据安全保护的义务与责任，为规范数据处理活动，保障数据安全提供法律依据。另外，《个人信息保护法（草案）》也即将进入三审阶段，两项法案相辅相成，推动我国个人信息保护和数据安全治理进入全新阶段。

在人工智能大会“大爱无疆·共生”论坛上，清华大学苏世民书院院长薛澜回顾人工智能治理模式历经回应式治理、集中治理和敏捷治理三个阶段。“现在我们进入了相对比较集中的治理模式。该模式明确了国家加强行业监管，促进制度落地的决心，对暴露出来的各种问题采取比较坚决的措施落实监管规则，同时触及到需要进一步研究的问题。”薛澜说。

目前，上海正研究立项公共场所人脸识别分级分类应用规范的地方标准，将成为全国首个立项的人脸识别的地方性标准；开展全市人工智能数据立法调研，规范数据确权，数据共享等重要内容，推动可信人工智能的研究。上海市人大也正在起草《上海市数据条例》。

此外，上海市数字证书认证中心、复旦大学计算机学院、上海交通大学电子信息与电气工程学院、移动互联网系统与应用安全国家工程实验室、上海赛博网络安全产业创新研究院共同发起筹建数字身份与数据流通信任技术实验室，该实验室将基于数字信任技术的产学研生态合作，开展隐私计算、区块链、前沿密码等数字信任技术攻关和产业应用，支撑城市数字化转型、数据要素市场构建和网络安全体系建设。

记者获悉，上海浦东新区将在数据资源共享、数据交易、数据开发利用等方面进行立法探索；临港新片区将试点开展企业法人数据的跨境流通的安全评估和服务监管，加强个人数据的全生命周期安全监控和防护。

热点追踪

### 山东省农科院向社会寻榜张榜揭榜

# 科研单位和社会力量该如何“无缝衔接”？

◎本报记者 王延斌 通讯员 李才林

在科研机制改革的道路上，没有完成时，只有进行时。这一次，被誉为“改革先锋”的山东省农科院再出大动作。

7月21日，山东省农科院副院长贾无对外宣布《关于面向社会公开寻榜张榜揭榜农业科技难题的通告》（以下简称通告）。该通告透露，本次破解农业难题的实践将分为3个阶段，即寻榜阶段，将面向各地市、企业、园区等公开征寻农业产业科技难题；之后的张榜阶段，山东省农科院将组织行业知名专家论证筛选，并向社会公开张榜；揭榜阶段，“身怀绝技”的揭榜方将与需求方对接，牵手合作。

在此过程中，山东省农科院搭建起了一个“技术需求方”与“创新优势方”之间的直接对接平台，利用其深厚的科研力量和广泛的专家智库，推动寻找农业需求，寻找解题高手，给出科研答案。作为平台搭建方，山东省农科院邀请专家负责寻榜、张榜、揭榜三个阶段全程的专业论证，甚至直接参与揭榜，让揭榜人员“凭本事说话”。

山东省农科院科研处处长刘开昌向记者表示，山东省农科院主动面向社会公开征寻农业产业科技难题并实施揭榜制，是“市场主体出题、科研单位答题”的一种科研机制创新，是面向农业经济主战场，坚持问题导向和目标导向，探索科研单位和社会力量“无缝衔接”，实施科技项目“揭榜挂帅”的新途径。

这不是山东省农科院在落实揭榜制上的第一次突破。今年4月24日，该院举行科技创新工程揭榜评审会，58个人围团队同台竞技，角逐29项“揭榜制”科研任务，最终29个团队成功揭榜。

这是该院在全国农科系统率先推行科研任务“揭榜制”和首席专家组阁制的尝试。

山东是农业大省，以约占全国6%的耕地和1%的淡水，生产约占全国8%的粮食、11%的水果、12%的蔬菜、13%的水产品。今年年初，经国家统计局确认，2020年，山东农林牧渔业总产值首次突破1万亿元，成为全国首个农业总产值过万亿元的省份。

但农业大省面临着如何向农业强省跨越的问题，科技无疑将扮演“第一生产力”的角色。

在此背景下，山东省农科院本次面向社会寻榜张榜揭榜，将聚集山东省内外农业优势科技力量突破一批农业“卡脖子”的重大关键技术，推动科技创新工作与农业产业发展“无缝连接”和深度融合，有效实现产业链、人才链、创新链和资金链的“一体化”，打通科技创新到产业应用的通道，支撑农业企业提高产品市场竞争力和区域农业转型升级水平，推动实现山东省由农业大省向农业强省的跨越。

今年5月21日，中央全面深化改革委员会第十九次会议审议通过了《关于完善科技成果评价机制的指导意见》（以下简称意见），意见提出“细化完善有利于转化的职务科技成果评估政策，鼓励广大科技工作者把论文写在祖国大地上。”

为此，山东省农科院创新性地推动揭榜制更好地落地，这既是落实中央意见精神的题中之意，也能更好地履行服务农业经济发展的责任，更好地把论文写在祖国大地上。

视觉中国供图

### “网赚”机会？“网暴”讹财！

# 警惕网络犯罪黑手伸向青少年

◎新华社记者 毛一竹 孙 飞 毛 鑫

只因和同学发生误会，一名13岁的初中女生被“网络水军”发文辱骂为“渣女”。这些不法分子还以“有偿删帖”为名对该女生进行敲诈勒索，致其身心受创。这不是电影《少年的你》中的情节，而是发生在现实生活中的一起网络霸凌未成年人案件。

正值暑假，青少年群体在网络上十分活跃。然而，其中一些人却被所谓“网赚”机会吸引，误入网络犯罪陷阱。

## 现实版《少年的你》

13岁的佳佳（化名）是深圳市一名刚上初中的女学生。因和同学发生误会，辱骂、污蔑佳佳“交往多名男友是‘渣女’”的内容突然出现在多个微信公众号上，并在同学间迅速传播，令佳佳痛苦不堪。

经警方调查，发布这些不实文章的微信公众号与深圳某文化传媒有限公司、长沙某文化传媒有限公司有关。这两家公司均为湖南男子文某某开设。

据负责办理该案的深圳市光明区检察院检察官张恒莉介绍，该团伙发布的文章内容多涉及校园矛盾、感情纠纷。这一团伙的不少非法收益来自“有偿删帖”。张恒莉说：“一些人看到自己的隐私和个人信息被泄露，找到客服想要删帖，团伙成员便借机敲诈，按照阅读量的30%至50%收取数百元到数千元不等的删帖费。”

“这实际上是一种实施网络霸凌、精神压迫的新型软暴力犯罪。”张恒莉说，网络团伙利用网络的隐秘性、犯罪成本的低廉性实施犯罪，对未成年人的身心和名誉都造成了不可挽回的伤害。

## 法律意识淡薄导致未成年人犯罪

2020年底，文某某被法院以敲诈勒索罪判处有期徒刑10个月，另外两名团伙成员也分别被法院判处有期徒刑7个月。

张恒莉告诉记者，该案中不仅有不少未成年人受害者，文某某等3名被告人也均为“00后”，作案时刚刚成年。由于文化程度不高，社会阅历较浅，法律意识淡薄，三人都没有意识到自己的水军行为是犯罪。

记者调查发现，当前网络违法犯罪团伙往往利用青少年特别是未成年人“贪小利”“见识浅”的特点，以“聊聊天发发帖”就能“轻松网赚”的谎言诱骗他们成为帮凶。

近期，广州警方打掉了章某强恶意索赔犯罪团伙，抓获犯罪嫌疑人13名。经查，犯罪嫌疑人章某强发展骨干成员30多名，并不断招揽在校学生、社会闲散人员发展下线，组建网络社团“大猪组”，以大量恶意评论、差评、灌水等手段要挟网店商家，索要“保护费”“赔偿款”。

广州市公安局南沙分局重案大队副大队长邝磊介绍：“该团伙利用未成年人心智未成熟、容易受利诱的特点，不断灌输不正当的牟利方法。”邝磊说，“案发时正值疫情期间，青少年群体的网络活跃度较高，不少人受到‘网赚’氛围负面影响，想借机赚点零花钱。”

## 加大打击网络犯罪黑灰产业链

专家认为，此类案件暴露出网络违法犯罪团伙向青少年特别是未成年人群体蔓延的趋势，特别值得警惕。敲诈勒索、散布谣言等违法现象泛滥网络，不但严重扰乱线上线下社会秩序，还将严重影响未成年人身心健康。

中国人民大学法学院教授万勇建议，进一步提高治理网络黑灰产的法治化水平刻不容缓，不仅要筑牢“网络并非法外之地”的思想意识底线，更要在网络治理中能将每个人的网络行为纳入法律框架之内。

记者从全国“扫黄打非”办公室了解到，当前全国范围正开展“秋风2021”专项行动。严厉打击自媒体从事虚假新闻、扰乱网络传播秩序等活动，保持打击“网络水军”“黑公关”的高压态势，清理关闭一批违法违规自媒体账号是该行动重要内容。

张恒莉认为，相关互联网内容平台要增强自我监管意识，将社会责任切实转化为经营行动，比如，进一步完善投诉反馈渠道，遇有举报信息应及时受理核实，涉嫌违法的要向有关部门及时报案。

“当前针对未成年人的法治教育应当突出法律的保护功能。”广州市律师协会未成年人保护法律专业委员会主任郑子殷说，“过往由于普法教育往往以预防违法犯罪为目的，采取的手段多以震慑为主，导致未成年人遇到侵害的时候不敢、不懂运用法律保护自己，选择服软、妥协、退缩。”

> 进一步提高治理网络黑灰产的法治化水平刻不容缓，不仅要筑牢“网络并非法外之地”的思想意识底线，更要在网络治理中能将每个人的网络行为纳入法律框架之内。
>
> **万勇**
> 中国人民大学法学院教授

# 整治网络“饭圈”乱象等 7类网上危害未成年人问题

**新华社讯** （记者**王思北**）记者7月21日从中央网信办获悉，为营造未成年人良好上网环境，有效解决网络生态突出问题，中央网信办即日起启动“清朗·暑期未成年人网络环境整治”专项行动，聚焦解决7类网上危害未成年人身心健康的突出问题。

中央网信办有关负责人表示，7类突出问题包括：直播、短视频平台涉未成年人问题；未成年人在线教育平台问题；儿童不良动漫动画作品问题；论坛社区、群圈等环节危害未成年人问题；网络“饭圈”乱象问题；不良社交行为和不良文化问题；以及防沉迷系统和“青少年模式”效能发挥不足问题。

其中，针对直播、短视频平台涉未成年人问题，严禁16岁以下未成年人出镜直播，严肃查处炒作“网红儿童”行为，禁止诱导未成年人打赏行为，防止炫富拜金、奢靡享乐、卖惨“审丑”等现象对未成年人形成不良导向。坚决清理散布暴力血腥、暗黑恐怖、教唆犯罪等内容的“邪典”视频。此外，还将深入整治诱导未成年人应援集资、高额消费、投票打榜、互撕谩骂、拉踩引战、刷量控评等“饭圈”乱象行为。

记者了解到，近期，针对快手、腾讯QQ、淘宝、新浪微博、小红书等平台传播儿童软色情表情包、利用未成年人性暗示短视频引流等问题，网信部门依法约谈平台负责人，责令限期整改，全面清理处置相关违法违规信息和账号，并对平台实施罚款处罚。

中央网信办有关负责人指出，专项行动期间，将进一步加大对违法违规行为的处置处罚力度，对于侵害未成年人合法权益的问题保持“零容忍”态度，坚持露头就打、从严从重，大力整治网上危害未成年人身心健康问题乱象。各网站平台要积极履行主体责任，主动发声、深入自查、堵塞漏洞，确保专项行动取得实效，切实为未成年人营造文明、健康、向上的网络环境。