网安联
Wang An Lian

网络与数据安全治理

FRONTIERS OF REGULATORY OVERSIGHT IN CYBERSECURITY AND DATA GOVERNANCE

前沿洞察（月刊）

2026年6月第6期（总第35期）

2026年6月12日

网络与数据安全治理前沿洞察月刊

Frontiers of Regulatory Oversight in Cyber Security and Data Governance: Monthly Insights

2026 年 6 月第 6 期（总第 35 期）

2026 年 6 月 12 日

樊建功 南昌市网络信息安全协会 会长

王胜军 南宁市信息网络安全协会 会长

谭　莉 贵阳市信息网络协会 办公室主任

杨建东 昆明市网络安全协会 秘书长

沈　泓 宁波市计算机信息网络安全协会 秘书长

卜庆亚 徐州市网络安全协会 理事长

孙　逊 佛山市信息协会 秘书长

谢照光 惠州市计算机信息网络安全协会 常务副理事长

程　谦 河源市网络空间安全协会 秘书长

孔德剑 曲靖市网络安全协会 会长

李　丹 榆林市网络安全协会 秘书长

编委会委员：（排名不分先后）

黄汝锡 北京网络空间安全协会流动联合党支部 书记

方满意 广东省网络空间安全协会 常务副会长

王　嫣 上海市信息网络安全管理协会 部长

成珍苑 网安联认证中心 副主任

黎明瑶 广东新兴国家网络安全和信息化发展研究院 研究员

陈菊珍 广东计安信息网络培训中心

黄丽佳 揭阳网络空间安全协会 秘书长

编辑部主任：梁思雨

编　辑　部：何治乐 胡文华 李　坤 吴若恒 李睿恒
胡柯洋 薛　波 罗智玲 王咏诗 肖华程

发行部主任：周贵招

发　行　部：林永健 蔡舒婷 高梓源

声　明：本刊定位于网络与数据安全前沿动态梳理，侧重全面跟踪、及时掌握，如需针对特定领域或前沿动态进行针对性专题研究，请将需求发送至 cinsabj@163.com。

目　录

境内前沿观察一：政策立法

导读：5 月，网络安全标识、电子数据取证、互联网信息内容多渠道分发等领域的部委层面制度供给和治理实践持续推进。地方层面，北京、天津、宁夏、上海等地围绕数据跨境流动、公共数据资源管理、数据权益等作出制度安排。

部委层面，国家互联网信息办公室公开征求《消费类网联摄像头网络安全标识实施规则》及相关标准意见，围绕网络安全标识样式规格、网络安全能力检测、网络安全标识信息确定、备案以及基础级、增强级、领先级消费类网联摄像头安全能力要求等作出安排。公安部发布《公安机关电子数据取证规则（征求意见稿）》，围绕电子数据勘验、扣押与冻结、提取、调取电子数据等作出规定，并对账号密码获取、电子数据转化适用、人工智能生成信息识别等问题作出安排。国家网信办等五部门公布《互联网信息内容多渠道分发服务管理规定》，对互联网信息内容多渠道分发服务机构的设立运行、服务规范、监督检查和法律责任作出规定。

地方层面，北京市印发《中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境负面清单管理办法（试行）》以及数据出境负面清单（2025 版），围绕管理体系再完善、申报审批再简化、安全监管再优化等方面展开。天津市发布《天津市数据条例（草案征求意见稿）》，围绕数据权益、公共数据资源管理、公共数据授权运营和公共数据资源登记等作出规定。宁夏印发《公共数据资源目录编制指南》，明确公共数据

资源目录结构、目录分类、责任分工和编制流程。广西、重庆分别发布数字政府发展规划和数字重庆建设规划征求意见稿，围绕数字政府建设、公共数据资源共享利用、政务人工智能应用基础、公共数据开放运营等提出措施。

关键词：网络安全标识；电子数据取证；数据跨境流动；公共数据资源

（一）部委层面动向

1. 国家互联网信息办公室公开征求《消费类网联摄像头网络安全标识实施规则》及相关标准意见

5 月 8 日，国家互联网信息办公室公开征求《消费类网联摄像头网络安全标识实施规则（征求意见稿）》《网络安全标识 消费类网联摄像头安全要求（征求意见稿）》意见。

《实施规则（征求意见稿）》包括总则、网络安全标识的样式和规格、网络安全能力检测、网络安全标识信息的确定、网络安全标识的备案等内容。

网络安全标识信息确定方面，《规则》提出七项措施：一是产品生产者名称是指对产品质量负有法律责任的产品品牌所有者或使用者的名称；二是产品规格型号与产品铭牌规格型号一致；三是产品网络安全能力等级与检测报告上展示的网络安全能力等级保持一致；四是消费类网联摄像头网络安全标识有效期为 3 年，起始时间为产品备案信息公告时间；五是检测实验室名称是对产品网络安全能力进行检测的自有检测实验室、第三方检测机构的名称，与检测报告上检测机构一致；六是检测依据为《网络安全标识 消费类网联摄像头安全要求》现行有效版本；七是产品备案信息码由备案管理平台在备案完成后生成。

《安全要求（征求意见稿）》分别对基础级、增强级、领先级消费类网联摄像头，从物理与硬件安全、系统与软件安全、网络与通信安全、数

据安全与个人信息保护和安全保障 5 个方面提出安全能力要求。例如，基础级网联摄像头数据安全与个人信息保护方面，征求意见稿提出六项措施：一是数据销毁应当符合《数据安全技术 电子产品信息清除技术要求》（GB 46864-2025）要求的信息清除功能；二是具备个人信息处理规则，并在产品管理相关界面、说明书等提供的链接页面公开展示，供用户查阅、复制或下载后查阅；三是个人信息收集应符合《信息安全技术 个人信息安全规范》（GB/T 35273-2020）中 5.2、5.4 的要求；四是个人信息存储应符合《信息安全技术 个人信息安全规范》GB/T 35273-2020 中 6.1.6.3 的要求；五是未经用户同意，不应对所收集图片、视频中个人的身份进行关联分析，但履行法定义务和法律法规另有规定的除外；六是处理用户敏感个人信息应符合《数据安全技术 敏感个人信息处理安全要求》（GB/T 45574-2025）中第 5 章及 6.1 的要求。（来源：网信中国）

2. 公安部发布《公安机关电子数据取证规则（征求意见稿）》

5 月 22 日，公安部发布《公安机关电子数据取证规则（征求意见稿）》，共六章六十一条，包括电子数据勘验、扣押与冻结、提取、调取电子数据等内容。

征求意见稿规定，公安机关在依法立案后，开展电子数据取证工作时，确需输入与案件相关的智能终端等账号密码的，应当依照下列次序进行：一是由电子数据持有人提供账号密码；二是电子数据持有人不提供账号密码的，经县级以上公安机关负责人批准，制作《公安机关电子数据取证获取账号密码决定书》，在明确告知电子数据持有人或者有见证人见证的情

况下，可以采取相应措施获取账号密码。电子数据持有人或者见证人应当在《公安机关电子数据取证获取账号密码决定书》上签名或者盖章；电子数据持有人、见证人无法或者拒绝签名、盖章的，应当同步录音、录像，并注明有关情况。电子数据持有人不提供账号密码，且不立即提取电子数据可能造成电子数据灭失等严重后果的，可以先行采取措施获取账号密码，但必须在 24 小时内补办批准手续。

征求意见稿强调，在刑事立案调查核实或者行政执法、查办案件过程中依法收集的电子数据，可以作为刑事案件的证据使用；在刑事案件侦办过程中依法收集的电子数据，可以作为行政案件的证据使用。公安机关与其他行政机关建立健全电子数据移送机制，明确移送案件的证明要求，加强证据固定和保全，确保电子数据依法转化适用。

征求意见稿提出，为了查明案情，解决案件中应用程序功能分析、人工智能生成信息识别等专门性问题，应当指派、聘请有专门知识的人进行鉴定，或者委托公安部指定的机构出具报告。需要聘请有专门知识的人进行鉴定，或者委托公安部指定的机构出具报告的，应当经县级以上公安机关负责人批准。（来源：公安部网安局）

3. 国家网信办等五部门联合公布《互联网信息内容多渠道分发服务管理规定》

5 月 29 日，国家互联网信息办公室、公安部、文化和旅游部、国家市场监督管理总局、国家广播电视总局联合公布《互联网信息内容多渠道分

发服务管理规定》，共五章三十一条，包括设立运行、服务规范、监督检查和法律责任等内容。

《管理规定》规定，互联网信息内容多渠道分发服务机构应当依法办理经营主体登记，登记的经营范围应当包含“互联网信息内容多渠道分发服务”的表述。已依法办理经营主体登记的相关服务机构，应当自本规定施行之日起30日内办理经营范围变更登记。市场监管部门及时将登记信息与网信、公安、文化和旅游、广播电视、新闻出版等有关部门共享。互联网信息内容多渠道分发服务机构从事互联网文化活动、网络表演经纪活动、网络出版服务、网络视听节目服务和互联网新闻信息服务的，应当依法取得相应行政许可，禁止未经许可或者超越许可范围提供相关服务。互联网信息内容多渠道分发服务机构应当设立信息内容管理负责人，配备与业务范围和服务规模相适应的内容管理团队，制定信息内容管理、人员管理、应急处置等规则。

《管理规定》强调，平台信息服务提供者应当要求在本平台入驻的互联网信息内容多渠道分发服务机构注册后台管理账号，通过后台管理账号加强对签约互联网用户公众账号的管理，并以显著方式在签约互联网用户公众账号信息页面展示该账号所属互联网信息内容多渠道分发服务机构名称。发现签约互联网用户公众账号未展示所属互联网信息内容多渠道分发服务机构名称的，平台信息服务提供者应当及时提示。经提示后仍未展示的，平台信息服务提供者可以依法依约采取限制账号功能、暂停营利权限等措施。（来源：网信中国）

4. 中央网信办等四部门印发《2026 年提升全民数字素养与技能工作要点》

5 月 29 日消息，中央网信办、教育部、工业和信息化部、人力资源社会保障部近日联合印发《2026 年提升全民数字素养与技能工作要点》。

《工作要点》部署 6 个方面 15 项重点任务。一是完善数字素养培育体系，包括强化数字资源供给开放、拓宽数字素养提升渠道；二是深化数字应用场景建设，包括提升数字生活品质、提升数字工作能力、激发数字创新活力；三是提升全民人工智能素养，包括强化人工智能赋能教育、加快人工智能人才培育、深化人工智能普及应用；四是促进数字普惠包容发展，包括深化信息无障碍环境建设、打造数字助老惠民公益项目；五是营造安全有序网络空间，包括引导全民文明依法上网用网、筑牢全民网络安全防护意识、促进人工智能安全规范发展；六是健全协同联动工作机制，包括完善多方协作机制、深化国际交流合作。（来源：网信中国）

（二）地方层面动向

1. 湖南省工信厅印发《湖南省算力券补贴政策实施细则》

5 月 6 日，湖南省工信厅印发《湖南省算力券补贴政策实施细则》，包括参与主体条件、补贴范围及标准、申请、使用及兑付流程等。

《细则》指出，算力券补贴是由湖南省级财政安排，用于支持符合条件的算力需求方购买合规算力服务的补助资金。《细则》提出，符合条件的算力需求方和算力供给方可以申请补贴。算力需求方需要符合以下条件：

一是申报主体是具有独立承担民事责任能力的企业，近三年内无重大违法违规经营记录，未被列入严重违法失信名单；二是年购买算力费用5万元（含）以上；三是具备明确的算力应用场景规划和真实的算力使用需求，相关应用项目应具有可行性和创新性；四是与算力供给方无直接投资与被投资、隶属、共建、产权纽带等影响公平公正市场交易的关联关系，且所使用算力的供给方须为符合条件并完成信息登记的主体。（来源：湖南省政府）

2. 北京市三部门印发《中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境负面清单管理办法（试行）》以及数据出境负面清单（2025版）

5月8日，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局三部门印发《中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境负面清单管理办法（试行）》以及数据出境负面清单（2025版）。

《管理办法（试行）》共六章二十四条，包括负面清单制定及管理、负面清单实施、监督管理等内容。办法自发布之日起施行，原《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》同步废止。办法施行前，已依据原办法取得相关组团出具备案结果通知书的，视为已满足北京市“两区”数据出境负面清单备案管理要求，其备案结果继续有效。

新版管理办法主要对以下三个方面进行制度优化：一是管理体系再完善。健全市区两级管理体系，即市网信办、市商务局、市政务和数据局等

市级部门牵头，17 个区（含经开区）具体组织实施，各区建立跨部门协调机制，明确牵头部门和职责分工；二是申报审批再简化。综合评估前期自贸区负面清单政策实施情况和企业反馈，进一步压减企业申报流程和材料，按照最小必要原则仅保留“一表”“一书”（即《使用申请表》和《企业承诺书》），其他申报材料全部取消；三是安全监管再优化。将风险防控从“普检普查”向“精准高效”转变，坚持分类施策，构建跨领域风险研判和联管联控机制，完善“信用+风险”分级分类精准监管体系，对合规意识与合规能力强的高评级企业实施轻量化监管，对高风险的业务场景加强风险识别管控，持续提升监管精准度和有效性。

负面清单共涵盖 9 个行业领域、67 个业务场景和 612 个字段，主要包括两类：一是首批自贸区负面清单直接转为“两区”清单，主要包括汽车、医药、民航、零售、人工智能等 5 个领域；二是新编制的“两区”负面清单，着眼北京市生物医药、高级别自动驾驶、双机场国际物流枢纽、国际金融服务等重点产业发展方向，新编制医疗器械、自动驾驶（智能网联汽车）、贸易物流、银行业等 4 个领域负面清单。同时，按照国家“一地创新、多地适用”原则，建立外省市负面清单应用机制，对于北京市企业后续确有使用需求的外省市负面清单，履行评估备案程序后动态纳入北京市负面清单体系。后续将按照动态管理机制，持续丰富拓展清单覆盖领域，成熟一批发布一批。（来源：北京市政务服务和数据管理局）

3. 广西壮族自治区大数据发展局发布《广西数字政府发展“十五五”规划（征求意见稿）》

5月12日，广西壮族自治区大数据发展局发布《广西数字政府发展“十五五”规划（征求意见稿）》，围绕支撑政府履职协同高效、推动安全防线自主可控、促进运营管理科学规范、促进数据资源共享利用、驱动数字底座智能集约、以数字政府发展引领驱动全域数智化转型六个方面提出二十二项措施。

促进数据资源共享利用方面，征求意见稿提出夯实数据资源治理基础。升级一体化智能化公共数据平台，构建覆盖公共数据全生命周期的统一底座，强化数据采集、汇聚、存储、加工、流通等基础支撑能力，实现全区公共数据资源“一本账”。加快实施基础综合数据仓建设工程，升级完善人口、法人、自然资源和空间地理、宏观经济、社会信用等数据基础库。深入推进数据治理，深化“一数一源”权威数据认定机制，探索非结构化数据智能治理。实施数据质量提升行动，建立健全数据质量核查与评价指标体系，强化全流程质量管控，鼓励行业组织、市场主体及社会公众参与公共数据治理，形成多元共治格局。加快推进数据流通利用基础设施建设，加大对数据基础设施和高质量数据集建设的投入。

驱动数字底座智能集约方面，征求意见稿提出建强政务人工智能应用基础。建设全区统一的“人工智能+”技术底座，构建“算力+平台+数据+模型+智能体”“五位一体”的人工智能公共服务平台，支撑低成本、低门槛、多种类的政务大模型训练服务。重点推动政务大模型语料库建设，整

合政务热线、政策文件、办事指南等高质量数据资源，形成覆盖全面、标注精准、动态更新的政务语料集。聚焦全区共性需求，加快构建智能问答、智能审核、智能问数、智能办公等通用智能体。鼓励部门和基层围绕审批管理、监管执法、社会治理、民生服务等场景，探索个性化智能体创新与应用，形成“通用+场景”的政务智能体矩阵。（来源：广西壮族自治区大数据发展局）

4. 重庆市大数据应用发展管理局发布《重庆市“十五五”数字重庆建设规划（2026—2030 年）（征求意见稿）》

5 月 14 日，重庆市大数据应用发展管理局发布《重庆市“十五五”数字重庆建设规划（2026—2030 年）（征求意见稿）》，从加快探索数智赋能超大城市治理新范式、强化数字重庆和人工智能双向赋能、加速数智技术和产业创新融合、持续深化数据要素市场化配置改革、深化数智领域开放合作、强化数智人才队伍建设六个方面提出措施。

加快探索数智赋能超大城市治理新范式方面，征求意见稿提出优化基层智治体系，包括健全基层智治统筹协调机制、建设风险隐患一体化防控体系等。例如，推动应急、消防、公安、气象等系统贯通集成，增强多元风险数据融合与智能分析能力，赋能镇街风险态势动态感知、精准研判与前瞻预警。强化预警响应五级一体贯通，预警信息自动触发基层智能预案，响应指令智能分拨、精准派送至责任岗位。重构数字化应急指挥体系与多跨数字预案，推动重点人员协同共管、应急抢险联动处置、多跨事件高效办理，全面提升条块协同联动水平。

持续深化数据要素市场化配置改革方面，征求意见稿提出推动公共数据开放运营。采取整体授权模式，深度挖掘民生服务、产业发展等领域高价值应用场景，打造形成更多优质公共数据产品和服务。结合惠医便民公益需求以及相关产业发展市场需求，推进肿瘤公共数据资源依场景授权运营。逐步探索分领域授权模式，激发行业活力。积极培育经营主体，鼓励经营主体参与公共数据产品与服务再开发。健全公共数据资源授权运营价格形成机制，加强对授权运营实施机构、运营机构的监督管理，促进公共数据资源合规高效流通使用。探索开展公共数据资产权益在特定领域和经营主体范围内入股、质押等。（来源：重庆市大数据应用发展管理局）

5. 广东省互联网信息办公室等三部门发布《中国（广东）自由贸易试验区数据出境负面清单管理办法（试行）》以及数据出境负面清单（2025 版）

5 月 15 日，广东省互联网信息办公室、广东省商务厅、广东省政务服务和数据管理局发布《中国（广东）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（广东）自由贸易试验区数据出境管理清单（负面清单）（2025 版）》。

《办法（试行）》共六章，包括职责及分工、负面清单制定及管理、负面清单实施等内容。《办法》规定，负面清单制定主要包括五项流程：需求调研、重要数据识别、业务场景分析、论证与征求意见以及履行审批报备流程。例如，重要数据识别方面，省级管理部门应当明确重要数据识别标准，对数据进行分类分级，形成广东自贸试验区和河套深圳园区重要

数据目录，并按程序向国家数据安全工作协调机制办公室备案。行业主管部门已公开发布或已在行业内部发布本行业、本领域数据分类分级标准规范的，优先按照其规定识别重要数据；行业主管部门未明确判定标准的，按照《中国（广东）自由贸易试验区数据分类分级参考规则》识别重要数据。

《办法》强调，负面清单实行动态管理。省级管理部门对于已出台的负面清单，跟踪评估实施情况和安全风险，统筹开展负面清单修订工作。对于尚未出台负面清单的行业、领域，及时研判数据出境实际需求，研究制定相应行业、领域负面清单，不断完善广东自贸试验区和河套深圳园区数据跨境流动管理政策体系。

《负面清单（2025 版）》涉及个人征信服务业、智能装备制造业两个行业，分别提出需要通过数据出境安全评估的数据清单，以及需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单。各清单包含数据类别、数据子类和数据基本特征与描述三项数据要素。（来源：粤港澳大湾区门户网）

6. 天津市数据局发布《天津市数据条例（草案征求意见稿）》

5 月 19 日，天津市数据局发布《天津市数据条例（草案征求意见稿）》，共十章五十八条，包括数据权益、数据资源、数据流通、赋能发展等内容。

草案征求意见稿规定，数据处理者对其合法取得的数据，依法享有数据持有权益，可以自主管控其持有的数据；对其合法持有的数据，依法或者按照约定享有数据使用权益，可以进行开发利用；对其合法持有的数据

以及通过加工、分析等形成的数据产品和服务，包括在此过程中所形成的衍生数据，依法或者按照约定享有数据经营权益。数据处理者委托他人处理数据的，数据处理者和受托方按照法律、行政法规规定或者合同约定享有数据相关权益。数据处理者可以对其依法收集的已经合法公开的数据进行处理，但不得危害国家安全、损害公共利益和他人合法权益。

草案征求意见稿提出，天津市人民政府统筹规划全市公共数据资源管理，建立物理分散、逻辑集中、资源共享、政企互联、安全可靠的公共数据资源管理体系，部署推动全市公共数据资源开发利用工作。市数据主管部门组织全市公共数据资源目录编制工作，制定统一的目录编制标准规范，建立目录动态更新机制。区数据主管部门组织编制本行政区域内的公共数据资源目录。公共管理和服务机构应当依照本部门职责，编制和更新本部门公共数据目录。

草案征求意见稿强调，天津市和区数据主管部门应当按照国家和本市有关规定组织开展本行政区域内公共数据资源授权运营，会同有关部门对公共数据运营机构运营情况实施监督管理。公共数据运营机构按照国家和本市有关规定，在授权范围内开展业务，提供数据产品和服务并获取合理收益，不得泄露、窃取、不当利用公共数据，不得参与已交付公共数据产品和服务的再次开发。纳入授权运营范围的公共数据以及生成的公共数据产品应当按照国家和本市有关规定开展公共数据资源登记；未开展登记的，不得进行流通交易。（来源：天津市数据局）

7. 宁夏回族自治区发展改革委、数据中心印发《公共数据资源目录编制指南》

5 月 25 日，宁夏回族自治区发展改革委、宁夏回族自治区数据中心印发《公共数据资源目录编制指南》，包括公共数据资源目录、编制原则、责任分工、编制流程等内容。

《指南》规定了公共数据资源目录结构、目录分类、目录要素、目录编码，以及公共数据资源目录编制的责任分工、要求和流程等内容。文件适用于指导各地区、各部门开展公共数据资源目录编制和管理工作。公共数据资源目录方面，《指南》提出，公共数据资源目录按照自治区级、地市级、县（区）级三级进行划分，共同构成全区统一的公共数据资源目录体系。自治区级分目录由自治区数据管理部门牵头编制，整合自治区级部门及各地市报送的数据资源形成。地市级目录由地市级数据管理部门编制，整合本级部门及所辖区县报送的数据资源形成。县（区）级目录由县级数据管理部门编制，整合本级部门报送的数据资源形成。各级目录逐级汇聚、上下衔接。（来源：宁夏回族自治区发展和改革委员会）

8. 上海市人大常委会公布关于修改《上海市促进浦东新区运用区块链赋能电子单证应用若干规定》的决定

5 月 27 日，上海市人民代表大会常务委员会公布关于修改《上海市促进浦东新区运用区块链赋能电子单证应用若干规定》的决定，共八条。

其中，《规定》新增以下内容：上海市支持经营主体在依法合规、确保安全的前提下，依托区块链基础设施开发应用智能合约。智能合约在符

合法律法规规定并满足约定的预设条件时，执行电子单证转让、跨境支付及交易结算等事项。上海市保障符合法律、行政法规规定条件的电子运输记录与运输单证具有同等效力；电子运输记录与运输单证完成转换后，原运输单证或者电子运输记录随即失效。（来源：上海人大）

9. 广州互联网法院发布《广州互联网法院加强未成年人网络司法保护的五年规划（2026-2030）》

5 月 28 日，广州互联网法院发布《广州互联网法院加强未成年人网络司法保护的五年规划（2026-2030）》，围绕筑盾工程、育苗工程、共护工程、强基工程提出二十五项措施。

筑盾工程方面，《规划》提出，强化个人信息保护。明晰未成年人个人信息全流程处理规则，探索监护人同意制度，严惩过度索权、大数据杀熟等行为。支持公益诉讼，探索人格权侵害禁令适用标准与信息删除权行使规则，引导企业采用技术手段保护未成年人个人信息安全。

育苗工程方面，《规划》提出，创新“青苗友好型”在线审理模式。对涉未成年人案件专项标识、优先分流，全面推行异步审理。运用虚拟形象、智能变声、背景虚化等技术保护被害人与证人隐私，防止二次伤害。

共护工程方面，《规划》提出，聚数据协同之智赋能科学决策。用司法大数据分析纠纷类型、风险趋势与突出问题，发布白皮书、典型案例与司法建议。精准识别新型风险，为前端治理、政策制定、行业监管提供数据与规则支撑。（来源：广州互联网法院）

境内前沿观察二：治理实践

导读：5 月，公安机关、网信部门、通信管理部门及相关机构围绕个人信息保护、网络谣言治理、AI 应用乱象整治、APP 用户权益保护、数据安全等领域持续推进治理实践。整体看，相关治理工作聚焦移动应用违法违规收集使用个人信息、虚假摆拍和 AI 造谣等突出问题。

公安机关方面，围绕违法违规收集使用个人信息、非法破解无人机飞行控制系统、网络谣言、虚假摆拍、侵犯公民个人信息等问题持续开展执法治理。国家网络与信息安全信息通报中心、公安部计算机信息系统安全产品质量监督检验中心通报多款违法违规收集使用个人信息移动应用，涉及未明示个人信息收集使用规则、未经同意收集使用个人信息、未列明向第三方提供个人信息情况等问题。公安部网安局公布非法破解无人机飞行控制系统、打击整治网络谣言等典型案例，北京、辽宁等地公安机关围绕虚假摆拍、AI 生成谣言、涉企谣言等依法查处相关违法行为。

网信部门方面，围绕“自媒体”信息来源标注、涉企网络环境、AI 应用乱象等开展专项治理。网信部门通报“自媒体”未规范标注信息来源典型案例，重点涉及涉时政信息未标注来源、AI 生成内容未添加标识等问题。中央网信办部署开展“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动，聚焦恶意炒作涉企信息、诋毁抹黑企业等突出问题。

通信管理部门方面，工信部及北京、江苏、浙江等地通信管理部门继续通报侵害用户权益行为 APP、SDK 和小程序，重点涉及违反必要原则收

集个人信息、未明示收集使用个人信息目的方式范围、整改不到位等问题，并要求相关开发运营者限期整改等。

其他部门和司法实践方面，国家计算机病毒应急处理中心发布“银狐”系列木马病毒攻击活动预警。最高人民检察院发布未成年人犯罪预防和治理典型案例，其中包括未成年人帮助信息网络犯罪活动案和非法获取计算机信息系统数据案等。

关键词：个人信息保护；网络谣言治理；AI 应用乱象

（一）公安机关治理实践

1. 国家网络与信息安全信息通报中心等部门通报多款违法违规收集使用个人信息移动应用

5 月，国家网络与信息安全信息通报中心、公安部计算机信息系统安全产品质量监督检验中心通报多款违法违规收集使用个人信息移动应用。

2026 年 2 月 26 日至 2026 年 4 月 16 日期间，国家计算机病毒应急处理中心检测发现 67 款移动应用存在一项或者多项违法违规收集使用个人信息情况。具体违法违规行为包括在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；以默认选择同意隐私政策等非明示方式征求用户同意；隐私政策难以访问；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等。

此外，2026 年 4 月 2 日至 2026 年 4 月 20 日期间，公安部计算机信息系统安全产品质量监督检验中心检测发现 41 款移动应用存在一项或者多项违法违规收集使用个人信息情况。具体违法违规行为包括未公开个人信息收集使用规则、未经用户同意收集使用个人信息、未完整准确告知收集使用个人信息情况，或告知收集使用个人信息目的、方式、范围与实际收集使用情况不一致，未列明向第三方提供个

人信息的种类、目的、方式以及接收方的名称、联系方式等。（来源：公安部网安局）

2. 公安部公布 10 起非法破解无人机飞行控制系统违法犯罪典型案例

5 月 18 日，公安部网安局公布 10 起非法破解无人机飞行控制系统违法犯罪典型案例。

案例一：四川泸州公安机关侦破侯某等人非法破解无人机飞行控制系统案。四川泸州公安机关网安部门查明，2025 年 3 月以来，以侯某（男，29 岁）为首的犯罪团伙利用技术手段篡改某大型无人机出厂载重参数，牟取非法利益。改装后的大型无人机极易引发剐蹭破坏高压电力设施、负重后“炸机”、负重脱落等安全事故，造成高压电线断落引发森林火情、高空坠落导致公共安全案事件等，危害人民群众生命财产安全。2026 年 3 月，四川泸州公安机关将侯某等 5 人抓获，查明其篡改大型农用无人机 30 余台。

案例二：上海奉贤公安机关侦破李某非法破解无人机飞行控制系统案。上海奉贤公安机关网安部门查明，2022 年以来，李某（男，40 岁）制作并出售解除无人机限高等限制的破解软件，并通过电商平台进行兜售，牟取非法利益。2026 年 3 月，上海奉贤公安机关将李某抓获，查明其非法破解无人机 100 余台。

案例三：福建厦门公安机关侦破欧阳某野等人非法破解无人机飞行控制系统案。福建厦门公安机关网安部门查明，2021 年 6 月以来，

欧阳某野（男，29 岁）和陈某（男，38 岁）2 人帮助他人非法破解无人机禁飞区域、限高等限制，牟取非法利益。2026 年 1 月，福建厦门公安机关将欧阳某野和陈某抓获，查明 2 人非法破解无人机 20 余台。

案例四：湖北武汉公安机关侦破解某雄等人非法破解无人机飞行控制系统案。湖北武汉公安机关网安部门查明，2024 年以来，解某雄（男，35 岁）和宋某毅（男，25 岁）2 人为他人提供破解无人机限高、禁飞区域限制服务，牟取非法利益。2026 年 3 月，湖北武汉公安机关将解某雄和宋某毅抓获，查明 2 人非法破解无人机 30 余台。

案例五：浙江衢州公安机关侦破涂某龙非法破解无人机飞行控制系统案。浙江衢州公安机关网安部门查明，2020 年以来，涂某龙（男，25 岁）为他人提供破解无人机限高、禁飞区域限制服务，牟取非法利益。2026 年 1 月，浙江衢州公安机关将涂某龙抓获，查明其非法破解无人机 20 余台。

案例六：湖南张家界公安机关侦破何某乾非法破解无人机飞行控制系统案。湖南张家界公安机关网安部门查明，2025 年 2 月以来，何某乾（男，24 岁）为他人提供破解无人机限高、禁飞区域限制服务，牟取非法利益。2026 年 1 月，湖南张家界公安机关将何某乾抓获，查明其非法破解无人机 20 余台。

案例七：山东青岛公安机关侦破王某雷等人非法破解无人机飞行控制系统案。山东青岛公安机关网安部门查明，2019 年 7 月以来，王某雷（男，39 岁）以青岛某电子科技有限公司为掩护，为他人提

供破解无人机限高、禁飞区域限制服务，牟取非法利益。2026 年 2 月，山东青岛公安机关将王某雷抓获，查明其非法破解无人机 20 余台。

案例八：广东深圳公安机关侦破胡某斌非法破解无人机飞行控制系统案。广东深圳公安机关网安部门查明，2024 年 7 月以来，胡某斌（男，40 岁）为他人提供破解无人机限高、禁飞区域限制服务，并出售破解无人机，牟取非法利益。2025 年 12 月，广东深圳公安机关将胡某斌抓获，查明其非法破解无人机 10 余台。

案例九：重庆两江新区公安机关侦破尹某华非法破解无人机飞行控制系统案。重庆两江新区公安机关网安部门查明，2023 年以来，尹某华（男，43 岁）为他人提供破解无人机限高、禁飞区域限制服务，牟取非法利益。2026 年 3 月，重庆两江新区公安机关将尹某华抓获，查明其非法破解无人机 10 余台。

案例十：甘肃陇南公安机关侦破李某慧非法破解无人机飞行控制系统案。甘肃陇南公安机关网安部门查明，2024 年 3 月以来，李某慧（男，33 岁）为他人提供破解无人机限高、禁飞区域限制服务，牟取非法利益。2026 年 1 月，甘肃陇南公安机关将李某慧抓获，查明其非法破解无人机 10 余台。

以上 10 起案例涉案人员均已被公安机关依法采取刑事强制措施，案件正在进一步办理中。（来源：公安部网安局）

3. 国家网络与信息安全信息通报中心通报，主流 JavaScript 软件包管理平台 npm 遭供应链投毒攻击

5 月 25 日消息，国家网络与信息安全信息通报中心近日监测发现，全球主流 JavaScript 软件包管理平台 npm 遭“沙虫”（Shai-Hulud）供应链投毒攻击。攻击者攻陷了 npm 官方维护者账户，并在短时间内批量投放大量恶意软件包，涉及 300 余个独立程序包的 600 余个恶意版本，影响多个热门开源项目。当开发者安装恶意依赖包后，程序会自动在本地主机、CI/CD 流水线环境执行恶意代码，窃取 GitHub Token、npm Token、云服务密钥、SSH 私钥、Kubernetes 凭据、数据库连接字符串等敏感信息。此次投毒攻击具备极强蠕虫式自我复制与横向传播能力，攻击者可利用窃取的 npm 发布权限篡改和二次发布开发者名下的其他软件包，造成供应链风险持续扩散、危害持续升级。

主要受影响项目包括 echarts-for-react、@antv 系列核心库（@antv/g2、@antv/g6、@antv/x6 等）、TanStack 系列 42 个包、Mistral AI 相关 PyPI 包以及 timeago.js 等社区包。受影响对象主要包括前端开发者、人工智能或机器学习开发者、开源项目维护者及企业研发人员等。由于恶意软件具备蠕虫式传播能力，可自动重新发布受害者维护的其他包，导致共享开发环境的其他用户及依赖同一维护者发布的其他软件包的用户也可能面临间接感染风险。

国家网络与信息安全信息通报中心提出处置建议：一是隔离风险设备。若本地设备近期安装过相关受影响的 npm 依赖，建议暂停项目运行，并断开可疑设备网络连接，防止恶意代码继续外联；二是排

查依赖文件。检查 package.json、package-lock.json、pnpm-lock.yaml、yarn.lock 及 node_modules 目录，核实是否存在异常 preinstall、postinstall 等自动执行脚本；三是清理残留痕迹。排查 Claude Code hooks、VS Code 任务配置等位置，检查是否存在 router_runtime.js、setup.mjs 等可疑文件，避免恶意代码在卸载依赖后继续残留；四是更换敏感凭证。及时更新 GitHub Token、npm Token、云服务密钥、SSH 私钥、数据库密码等各类密钥与令牌，对关联账号执行“退出全部设备”操作；五是提升安全意识。安装 npm 第三方依赖前，应核验项目官方来源、近期发布记录和脚本内容，不盲目安装热门包，优先选用安全稳定的官方版本。（来源：公安部网安局）

4. 公安部网安局公布 5 起打击整治网络谣言典型案例

5 月 26 日，公安部网安局公布 5 起打击整治网络谣言典型案例。

案例一：彭某等人虚假摆拍“绑架”谣言并煽动网友报警案。近日，江西上栗公安网安部门依法查处一起直播间虚假摆拍“绑架”谣言、煽动网友报警的扰乱公共秩序案件。违法行为人彭某、郭某、李某、刘某 4 人已被依法行政拘留。经查，2026 年 4 月 24 日晚，违法行为人彭某为博取流量、吸引关注，伙同郭某、李某、刘某等人编造虚构剧情，在直播间制造虚假警情，并煽动网友报警，导致大量不明真相的网友信以为真，出于善意纷纷向公安机关报警，该行为故意扰乱公共秩序，扰乱公安机关正常工作，造成警力浪费。目前，属地公安机关已依法对上述 4 人作出行政拘留处罚。

案例二：刘某某等人虚假摆拍“将女主播高薪骗至境外挣钱”谣言案。近日，重庆公安网安部门工作发现，有网民在互联网平台发布信息，称“重庆开州一男子骗女主播去境外从事诈骗”，引发舆论关注。经查，此事系刘某某、夏某某、王某等6人为博取流量而策划演绎的虚假信息。刘某某等人通过在互联网平台直播连线的方式，虚构“将女主播高薪诱骗至境外挣钱”“向女主播家人索要30万赎金”“女主播母亲卖房筹款”等情节，引发大量网民关注和讨论。为让谣言信息更具欺骗性，刘某某专程前往外地连线直播，营造其身处境外的假象。目前，属地公安机关已依法对刘某某等6人作出行政拘留处罚。

案例三：“薛某某编造“瑞安某中学5名学生怀孕”谣言案。近日，浙江温州公安网安部门工作发现，一则关于“瑞安某中学5名学生怀孕”的消息，在网络平台传播，引发大量网民关注，造成恶劣影响。经查，网民薛某某为博取关注，编造了涉“瑞安某学校举行体检，5个女孩子怀孕，校长也被叫出去约谈了”等不实信息，并在短视频平台和社交媒体发布，引发大量网民关注和讨论，对学校声誉和正常教学秩序造成恶劣影响。目前，属地公安机关已依法对薛某某作出行政拘留处罚。

案例四：马某某利用AI工具编造“张家界大峡谷玻璃桥坍塌”谣言案。湖南张家界公安网安部门工作发现，“五一”假期前夕，一条“惊悚”的视频在网络平台悄然扩散，视频显示，张家界大峡谷玻璃桥突发坍塌事故，画面中桥头断裂、人群四散奔逃，并配上“没事

就别想着出去玩了，还是家里安全”的煽动性标题，引发了公众的恐慌与关注。经查，网民马某某为博人眼球，吸引流量，利用 AI 工具编造了这场“坍塌事故”，并通过短视频平台发布，马某某为了最大程度收割流量，马某某还特意带上了“张家界天门山”“张家界大峡谷玻璃桥”等热门旅游话题，意图恶意蹭取假期热度。肆意传播的不实信息，不仅严重损害了张家界大峡谷景区的声誉，抹黑了张家界文旅的整体形象，更引发了公众对旅游安全的深度恐慌，严重扰乱公共秩序。目前，属地公安机关已依法对马某某采取刑事强制措施。

案例五：赵某某利用 AI 工具编造“某企业车间爆炸”谣言案。近日，山西大同公安网安部门工作中发现，某企业员工在互联网平台发布信息，谣称“有一车间内发生爆炸，现场有一名工人受伤”，甚至声称“伤者面部烧伤面积 100%”，该谣言引起大量网民关注讨论。经查，该企业未发生此类安全事故，相关内容系该企业员工赵某某通过 AI 工具生成的虚假文案和虚假视频，在互联网平台发布，引发网民关注，造成不良影响。目前，属地公安机关已依法对赵某某作出行政警告。（来源：公安部网安局）

5. 因系统服务器遭木马入侵，某高校被行政处罚

5 月 8 日消息，甘肃兰州网警近日对当地某高校系统服务器开展日常检查时发现系统日志存在异常通联情况。

调查发现，该校对服务器系统未采取有效的防范措施，内部网络未采取横向隔离措施，其服务器已被远程植入挖矿木马恶意程序，并

横向传播至其它办公设备。属地公安机关依据《网络安全法》第二十三条、第六十一条规定，对该校不履行网络安全保护义务的违法行为作出行政处罚，责令该校限期整改。目前，该高校服务器系统被植入的木马程序已被清除，属地网警对黑客攻击开展溯源调查工作。（来源：公安部网安局）

6. 北京网警侦破 2 起有偿删除商品差评案，刑拘 7 人

5 月 14 日消息，北京公安网安部门近日会同经侦部门侦破 2 起有偿删除商品差评案件，打掉 2 个犯罪团伙，抓获涉案人员 7 名。

北京公安网安部门工作中发现，在多个电商平台、短视频评论区内出现“专业删差评”等有偿推广信息，疑似有组织开展有偿删除商品差评违法活动。经查，以郭某、谢某为首的 2 个犯罪团伙以电商服务工作室为掩护，利用商家惧怕“负面评价”影响商品销量的心理，为商家提供有偿删除差评服务。进一步工作发现，2 个犯罪团伙通过伪造材料，向平台申诉删除差评，借机非法牟利。

北京警方分赴外省市成功抓获包括组织者在内的 7 名涉案人员。目前，上述人员均已被公安机关依法采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

7. 北京网警发布 3 起打击虚假摆拍、造谣典型案例

5 月 16 日，北京公安网安部门发布 3 起打击虚假摆拍、造谣典型案例。

案例一：刘某（男，26 岁）和江某某（女，24 岁）为吸粉引流、博取关注、牟取私利，在朝阳区某路旁虚假摆拍“盲人在盲道行走被电动自行车撞击并遭骑车人斥责”内容，并通过短视频平台对外发布，误导大量网民关注和讨论，造成恶劣影响。上述二人被公安机关依法采取刑事强制措施。

案例二：胡某（女，39 岁）和张某某（男，55 岁）为蹭热度、博取关注、牟取私利，虚假摆拍“街头骑电动自行车发生纠纷”的视频，并通过短视频平台对外发布，造成谣言传播扩散，产生不良影响。上述二人被公安机关依法行政处罚。

案例三：杨某（男，25 岁）为吸粉引流、牟取私利，利用 AI 工具生成“北京郊区超万吨垃圾堆放”不实信息并公开发布，造成谣言传播扩散，产生不良影响。杨某被公安机关依法行政处罚。（来源：公安部网安局）

8. 王某利用工作便利买卖公民个人信息被依法采取刑事强制措施

5 月 19 日消息，四川省攀枝花市公安机关网安部门近日破获一起利用工作便利条件，非法买卖公民公积金信息案件，犯罪嫌疑人王某等 10 人因涉嫌侵犯公民个人信息罪被依法采取刑事强制措施。

经查，犯罪嫌疑人王某曾任职于某信息技术公司，利用维护公积金相关系统的便利条件，非法获取一批公民的公积金缴存信息，并通过社交网络向贷款中介、理财公司兜售。经进一步查证，王某等人累

计向他人出售公民公积金信息500余万条。经审讯，王某对其非法获取并出售公民个人信息的犯罪事实供认不讳。

王某等人因非法获取和买卖公民个人信息已被依法采取刑事强制措施。案件正在进一步侦办中。（来源：公安部网安局）

9. 辽宁公安公布五类网络谣言典型案例

5月26日，辽宁公安公布五类网络谣言典型案例。

第一类是利用社会热点炒作，包括李某贵编造“老太太偷樱桃”谣言案、刘某编造“不雅视频”谣言案、李某阁等人编造“外卖骑手上吊自杀”谣言案。

第二类是利用灾情、险情吸引流量，包括巴某编造“交通事故”谣言案、刘某娇编造“燃气爆炸”谣言案、王某凤“暴雨滑坡”谣言案。

第三类是利用警情造谣，包括李某编造虚假警情谣言案、田某编造“婚车使用警车开道”网络谣言案、修某编造“大连王家桥发生割喉事件”网络谣言案。

第四类是侮辱英烈，包括栾某侵害英雄烈士名誉、荣誉案。

第五类是涉企谣言，包括刘某发布不实信息扰乱公共秩序案、李某等8人发布不实信息扰乱公共秩序系列案。（来源：网信辽宁）

10. 四川成都公安网安部门侦破一起侵犯公民个人信息案

5 月 27 日消息，四川成都网安部门近日破获一起特大侵犯公民个人信息案。

2026 年 3 月，四川成都网安民警巡查发现，有人通过网络批量售卖成都各小区业主信息，可精准查询姓名、电话、房产详情。警方立即溯源深挖，锁定一条完整的犯罪链条。

经查，该黑灰产团伙层级清晰、分工明确，形成了“源头窃取、中间倒卖、下游使用”的全链条违法模式：不动产行业“内鬼”何某超、叶某，利用工作职务便利，非法窃取海量不动产及公民个人敏感信息；余某等多名中间商承接泄露数据，通过多层流转、加价倒卖的方式非法牟利；下游大量房产中介、家装行业从业人员批量购买涉案信息，用于商业精准营销活动。该案涉案信息超 130 万条，涉案资金达 160 万元，危害范围广、社会影响恶劣。

2026 年 4 月 8 日，警方开展集中收网，一举抓获违法犯罪人员 56 人。其中，11 名主要涉案人员为信息源头窃取者、信息倒卖中间商，系该案黑灰产链条关键人员，其行为已触犯《刑法》第 253 条之一，涉嫌侵犯公民个人信息罪，警方依法对其采取刑事强制措施；45 名涉案人员为下游非法购买、违规使用公民个人信息的房产中介、家装行业从业者，其行为违反网络安全及个人信息保护相关行政法规，公安机关依法对其作出行政处罚。（来源：公安部网安局）

（二）网信部门治理实践

1. 网信部门通报“自媒体”未规范标注信息来源典型案例

5 月 3 日消息，网信部门近日针对“自媒体”账号发布涉时政等领域信息未标注国内外时事、公共政策、社会事件的信息来源，未标注 AI 生成标识，未标注虚构演绎标签的行为，督促网站平台自查自纠，依法依约处置违规账号 9.8 万余个。其中，涉及四类典型案例。

案例一：抖音“青青国际”“极客科普馆”、快手“名妍”、哔哩哔哩“晋说”“军武-史记”等“自媒体”账号，集纳涉美伊等国际时事信息，未标注信息来源，公众难以溯源信息原始出处，无法辨别信息真伪。涉及的账号已被依法依约处置。

案例二：抖音“小胖农业”“乡村发展”、快手“农民大姐”“清华鱼妈”、哔哩哔哩“商业策略”等“自媒体”账号，发布涉农业农村、教育、养老等领域公共政策相关信息时，未标注信息来源，公众无法获得准确、完整的权威信息，可能会基于碎片化内容对政策作出错误理解。涉及的账号已被依法依约处置。

案例三：抖音“萌萌哒”“用户赵先生”、快手“农村户外小张 1”“玉婷”、微博“金毛治郁系”、哔哩哔哩“哎呦哎呦小然子”等“自媒体”账号，通过人工智能技术，制作并发布金毛抱小孩、大猩猩护崽对峙鳄鱼、老虎和橘猫开车回家探亲、小猫玩游戏眼花后戴眼镜、柴犬厨神做菜等视频，未添加 AI 生成标识，易误导不了解 AI 的网民，难以区分虚拟与现实边界。涉及的账号已被依法依约处置。

案例四：抖音“刘百川商业”“马瑞（在农村）”、快手“玉雕师凤云”、微信视频号“遇见翡翠的夏天”、哔哩哔哩“加油嘉宜”等“自媒体”账号，以剧情摆拍、虚构情节等方式，发布外卖员送餐遭歧视、婆媳冲突、代际冲突、未成年人无人看护、丑化农村等内容，未标注虚构演绎标签，借机博取流量，以负面叙事渲染消极情绪，挑动群体对立。涉及的账号已被依法依约处置。（来源：网信中国）

2. 中央网信办发布《生活服务类平台算法负面清单（试行）》实施成果

5 月 8 日，中央网信办发布《生活服务类平台算法负面清单（试行）》实施成果。

中央网信办前期会同有关部门督促外卖、网约车、货运、网购、在线旅游、票务领域重点平台对照《负面清单》开展自查自纠。美团、淘宝闪购、淘宝天猫、京东、滴滴、高德、T3、百度、满帮、货拉拉、拼多多、抖音、携程、去哪儿网等平台已实施优化改进措施 63 项，承诺遵守算法要求 139 项，限期推进 125 项。上述改进措施涉及优化订单分配算法、时间预估算法、安全保障算法、收入抽成算法、定价算法、申诉处理、提升算法透明度七个方面。（来源：网信中国）

3. 中央网信办发布规范短视频内容标注工作成果

5 月 12 日消息，中央网信办此前针对部分短视频内容来源不清、真假难辨、混淆视听等突出问题，开展规范短视频内容标注工作。2026

年1月以来，指导网站平台深入清理虚假摆拍等违规短视频52万余个，严惩违规账号6.8万余个，发布治理公告54期，并集中曝光典型案例；3月，指导抖音、快手、腾讯、小红书、哔哩哔哩、微博、淘宝、京东、拼多多、支付宝、美团、百度等12家平台先行先试，完善内容标注标签，对内容标注功能进行优化和测试。

中央网信办总结12家平台试行经验，指导各地各网站平台全面推进落实三项工作：一是规范短视频内容标注标签，明确网站平台必须为用户提供6类“必选标签”，并可根据自身实际提供其他“可选标签”。其中，“必选标签”包括“含有虚构演绎内容”“含有AI生成内容”“含有营销信息”“内容为转载”“内容为个人观点”和“无需标注”。真实生活记录类短视频可选择“无需标注”标签，该标签不在短视频页面呈现；二是将内容标注设为短视频发布必经环节，发布者必须从“必选标签”中选择一项，才能发布短视频；三是对新增短视频标注情况加强审核，对存量短视频进行分批回溯，对未规范标注的，进行补标或纠正，并对相关发布者进行教育警示，推动实现短视频内容应标尽标。（来源：网信中国）

4. 中央网信办部署开展“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动

5月26日，中央网信办秘书局发布《关于开展“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动的通知》，部署开展“清

朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动。专项行动聚焦四类突出问题：

一是恶意炒作涉企信息问题，包括在企业上市融资、财务报表公布、新品发布等重要时间节点，炒作涉企负面信息；恶意集纳涉企负面信息，泛化异化炒作企业经营问题或产品质量问题；开展虚假不实测评，恶意炒作商品测评、测试和消费体验信息；通过“付费投流”等方式，对涉企负面信息进行推广，人为制造或放大涉企舆论热点。

二是诋毁抹黑企业问题，包括利用 AI 生成涉企虚假不实信息，恶意抹黑诋毁企业、企业家；雇佣网络水军，散布同质化涉企负面信息，恶意碰瓷、诋毁其他企业和产品；网络名人账号以“喊话”等形式无端质疑、拉踩企业，煽动网民攻击谩骂企业、企业家；对特定品牌用户“贴标签”，进行污名化攻击，煽动消费群体对立。

三是牟取非法利益问题，包括向企业发送“负面信息求证函”“情况核实函”等，胁迫企业开展商业合作；将舆论监督、社会监督与商业合作挂钩，以发布涉企负面信息为手段，向企业施压牟取经济利益；发布涉企负面信息后，向企业索要“删帖费”“撤稿费”；

四是侵犯企业家个人权益问题，包括炒作企业家个人隐私；发布传播侮辱谩骂、造谣诽谤企业家的言论；炒作企业家私生活话题，贬损丑化企业、企业家形象；翻炒企业家旧闻旧事，断章取义、歪曲解读企业家言论。（来源：网信中国）

5. 海南省完成全国首个遥感卫星数据出境安全评估

5 月 18 日消息，海南省委网信办近日指导文昌航天超算智慧科技有限公司顺利完成全国首个遥感卫星数据出境安全评估。

遥感卫星数据既是数字经济发展的重要数据要素，也是关系国家安全的战略性资源。长期以来，受政策多头交叉、敏感程度判定难、申报无先例可循等因素影响，数据合规出境成为制约产业开放发展的关键瓶颈。本次评估的顺利完成，填补了商业遥感数据出境合规工作的空白，为同类企业依法依规开展遥感数据跨境流动提供了可参考、可复制的实践路径，对推动商业航天产业数字化、国际化发展具有积极示范意义。（来源：网信海南）

6. 辽宁省阜新市发布“网络乱象”专项整治典型案例

2026 年，辽宁省阜新市网信、公安等部门深入开展“网络乱象”专项整治行动，依法依规打击处置一批违法人员和平台账号。

案例一：网民通过“12377”平台举报阜新市一网站发布涉某企业创始人成长、发展经历的不实信息，损害当事人及企业品牌声誉。市网信办依据《网络信息内容生态治理规定》等法律法规，约谈该平台负责人，责令删除相关涉企侵权信息。

案例二：巡查发现一域外网民在阜新市某平台发布虚拟货币相关非法金融活动信息。市网信办依据《网络信息内容生态治理规定》等法律法规，向该平台下达《责令立即整改通知书》，关停涉事账号。

案例三：阜新网民李某因怀疑吴某与自己男友有不正当关系，在短视频平台发布诽谤视频，声称吴某患有性病，损害他人名誉。公安机关责令李某删除了短视频，依法对李某批评教育。

案例四：阜新网民许某某为博取流量和关注，录制一段结婚现场燃放鞭炮的视频，配音频称“化工厂爆炸了”发布至短视频平台，造成不良社会影响，其行为涉嫌虚构事实扰乱公共秩序，公安机关依法对许某某作出行政处罚。

案例五：阜新网民刘某某将网上下载的“某次作战牺牲军人姓名”的视频，在未经核实视频真伪的情况下上传至短视频平台，导致部分网民被误导，造成不良社会影响，公安机关依法对刘某某作出行政处罚。

案例六：阜新网民刘某某在短视频平台发布“辽宁某地厨房煤气爆炸，孩子被弹飞”的作品。经查，该事件为虚假信息，刘某某为博眼球赚取流量将事发地改为辽宁某地，造成恶劣社会影响，涉嫌虚构事实扰乱公共秩序，公安机关依法对刘某某作出行政处罚。

案例七：阜新网民曾某某在快手平台发布“某平台外卖员向餐食内撒尿”的视频。经查，该事件为虚假信息，严重侵害企业品牌声誉与外卖骑手合法权益。鉴于曾某某患有智力二级残疾，公安机关依法对其批评教育，责令监护人严加看管。

案例八：阜新网民李某某、姚某某在抖音平台发布视频称，“某平台骑手因差评上吊自杀”。经核实，死者非外卖骑手。公安机关依法对李某某、姚某某作出行政处罚。（来源：网信辽宁）

（三）通信管理部门治理实践

1. 工信部、北京、上海、江苏、安徽、浙江等通信管理部门通报侵害用户权益行为 APP

（1）工信部

5 月 21 日，工信部信息通信管理局通报 2026 年第 3 批，总第 56 批侵害用户权益行为的 APP（SDK）。工信部信息通信管理局近日组织第三方检测机构进行抽查，共发现 31 款 APP 及 SDK 存在侵害用户权益行为。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）北京市

5 月 6 日，北京市通信管理局通报 2026 年第五期问题移动互联网应用程序。北京市通信管理局近日通过抽测发现北京市部分移动互联网应用程序存在“违反必要原则收集个人信息”“未明示收集使用个人信息的目的、方式和范围”等侵害用户权益问题。截至通报，尚有 5 款移动互联网应用程序未整改或整改不到位。

此外，2026 年 4 月 7 日，北京市通信管理局通报北京市部分存在侵害用户权益行为的移动互联网应用程序并要求整改。截至通报，仍有 4 款移动互联网应用程序未整改或整改不到位。

（3）江苏省

5 月 19 日，江苏省通信管理局通报 2026 年第 3 批侵害用户权益行为 APP。江苏省通信管理局近日组织第三方检测机构对省内智慧停

车等类型的APP、小程序进行检测，并通报相关单位限期整改。截至通报，尚有15款APP、小程序未完成整改。相关单位于5月27日前完成整改并反馈，整改落实不到位的，江苏省通信管理局将依法依规组织开展相关处置工作。

（4）浙江省

5月25日，浙江省通信管理局通报2026年第4批侵害用户权益行为的APP（小程序）。浙江省通信管理局近日组织第三方检测机构对群众关注的教育、交通等领域APP、小程序进行检查，书面要求违规APP、小程序开发运营者限期整改。经核查复检，尚有11款APP、小程序未按要求完成整改。上述APP、小程序开发运营者在6月1日前按有关规定进行整改，整改落实不到位的，浙江省通信管理局将依法依规组织开展相关处置工作。（来源：工信微报、北京通信业、江苏通信业、浙江省通信管理局）

2. 上海市通信管理局部署开展“浦江护航”2026年电信和互联网行业数据安全专项行动

5月29日，上海市通信管理局部署开展“浦江护航”2026年电信和互联网行业数据安全专项行动。专项行动适用于上海市电信和互联网行业数据处理者。其中，重点对象为在电信和互联网行业处理重要数据、1000万人以上个人信息或运营重要网络信息系统的电信业务经营者。

专项行动包括八项重点任务，包括赋能行业人工智能数据安全治理、深化行业首席数据官履职效能评估、深入推进重要数据识别认定及目录管理等。

赋能行业人工智能数据安全治理方面，重点防范数据标注、汇聚、训练、合成等环节的数据泄露、篡改、丢失等各类数据安全风险。市通管局组织提供易使用的技术检测工具，协助企业快速识别大模型及智能体相关数据安全风险并提供改进建议；组织专业机构和专家开展人工智能数据安全专项培训并提供实践指导，保障电信和互联网行业人工智能安全有序发展。

深入推进重要数据识别认定及目录管理方面，电信和互联网企业应动态结合国家出台的最新法律法规及其他规范性文件定期进行数据资产梳理，依据《电信领域重要数据识别指南》（YD/T 3867-2024）等相关标准规范开展重要数据及1000万人以上个人信息识别工作，形成并定期更新本单位重要数据目录，在7月31日前向市通管局备案。当重要数据条目数量或者存储总量等变化30%以上，或者其他备案内容发生重大变化时，企业应在3个月内向市通管局更新备案。

强化企业出海数据安全与跨境合规方面，电信和互联网企业应主动应对出海目的地国家及地区数据安全相关监管要求，统筹境内外双重合规义务，防范因法律环境差异引发的经营风险。向境外提供在中华人民共和国境内收集和产生的重要数据或个人信息的，应按照国家法律法规要求，做好数据出境安全保护。市通管局加强企业出海数据安全合规指导，推动编制《上海市电信和互联网行业出海企业数据双

向合规指引》，探索建设企业出海公共服务平台，为企业出海提供数据安全和跨境合规实务支持，护航企业全球化发展。（来源：上海通信圈）

（四）其他部门治理实践

1. 国家计算机病毒应急处理中心发布针对我国用户的“银狐”系列木马病毒攻击活动的预警报告

5 月 22 日消息，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室近日依托国家计算机病毒协同分析平台捕获多个文件名中包含“内部调查结果”“违纪名单”“违纪通报信息”“裁员补偿”等词汇的恶意程序。这些恶意程序表面上伪装成快捷方式、文件夹、文档文件或压缩包文件，实际为针对 Windows 平台用户的远程控制木马病毒。

经分析，这些木马病毒均为针对我国用户的“银狐”（又名“游蛇”“谷堕大盗”“UTG－Q－1000”“Silver Fox”等）木马病毒攻击活动的最新变种。如果用户不慎运行相关恶意程序文件，将被攻击者实施远程控制、窃密等恶意操作，并可能被网络犯罪分子利用充当进一步实施电信网络诈骗活动的“跳板”。

国家计算机病毒应急处理中心建议采取以下综合防范措施：一是在使用即时通讯工具（如：微信、QQ、钉钉、飞书等）或电子邮件处理工作事务期间，警惕新增临时工作群组和电子邮件中传播的“违

纪”“裁员”等相关主题文件，拒绝点击陌生人发送的文件，对本单位或外单位同事发送的相关文件应与其本人或正式渠道核实。

二是用户可将可疑的文档文件、可执行文件、压缩包文件或解压后的可疑文件先行上传至国家计算机病毒协同分析平台（https://virus.cverc.org.cn）进行安全检测，并保持防病毒软件实时监控功能开启，将计算机操作系统和防病毒软件更新到最新版本。

三是一旦发现本人即时通讯工具或电子邮件发生被盗用现象，应立即停止使用可能感染病毒的计算机设备，将其断开网络链接，并向单位网络管理员、相关同事和亲友告知相关情况，在备份重要数据的前提下，对相关计算机设备进行杀毒和安全检查，更换常用口令且应具有较高强度。（来源：公安部网安局）

2. 最高检发布“强化检察监督，促进未成年人犯罪预防和治理”典型案例

5 月 28 日，最高人民检察院发布十起“强化检察监督，促进未成年人犯罪预防和治理”典型案例，其中有两起涉网案件。

案例一：朱某某帮助信息网络犯罪活动案——精准监督，推动加强未成年人银行账户管理

2022 年 8 月，朱某某（男，16 岁）明知他人为转移网络犯罪资金，仍在多家银行办理银行卡 3 张出租给他人使用，上述银行卡单向流水金额合计人民币 55 万余元，查明上游网络犯罪资金人民币 7 万余元，朱某某非法获利人民币 6800 元。2023 年 6 月 26 日，江苏省

徐州市某区人民检察院依法对朱某某作出附条件不起诉决定，考验期为六个月。朱某某在考验期内表现良好，遵守相关规定。同年 12 月 26 日，依法对朱某某予以不起诉。

案例二：刘某某非法获取计算机信息系统数据案——惩教结合挽救少年“黑客”，数智赋能推动网络空间协同治理

2024 年 3 月，国内某互联网公司员工吴某某（另案处理）联系刘某某（男，16 岁），提出有渠道获取某云存储平台的后台存储数据。二人商定，由刘某某招揽“客户”、收取钱款；吴某某采用技术手段，超出公司授权范围，非法获取并提供相应数据。截至案发，二人通过上述手段非法获利人民币 5 万余元。2024 年 9 月，北京市某区人民检察院依法对刘某某提起公诉。同年 12 月，法院以非法获取计算机信息系统数据罪判处其有期徒刑二年六个月，并处罚金人民币三万元，没收全部违法所得。

本案中，检察机关委托司法社工对刘某某开展社会调查，梳理总结其犯罪诱因，并牵头组建帮教小组，制定对刘某某的个性化帮教方案：一方面通过网络犯罪专题辅导提升其道德法律意识，借助黏土雕塑创作引导自我认知重构，开展家庭议事契约模拟改善亲子沟通方式，分阶段达成网络素养提升、自我价值重塑、改善亲子关系等具体目标；另一方面以预防再犯罪为核心，将帮教措施贯穿侦查、审查起诉和判后全流程，帮教小组通过与管教民警持续沟通、与刘某某面对面谈心、查阅日常表现记录等，动态评估帮教成效，适时调整方案，帮助刘某某树立重新回归社会的信心。（来源：最高人民检察院）

3. 北京互联网法院发布《北京互联网法院未成年人网络司法保护白皮书（2021-2026）》

5 月 28 日，北京互联网法院发布《北京互联网法院未成年人网络司法保护白皮书（2021-2026）》。

白皮书指出，2021 年 5 月至 2026 年 5 月，北京互联网法院共受理涉未成年人网络纠纷案件 2581 件，年收案从 2021 年的 50 件升至 2025 年的 997 件，收案数量增长近 20 倍，年均增幅 111.3%。

白皮书指出，从案件整体案由结构来看，主要案件类型为网络服务合同纠纷、网络侵权责任纠纷、信息网络买卖合同纠纷。其中，网络服务合同纠纷 2231 件，占比 86.4%，主要为未成年人游戏充值、直播打赏等非理性消费引发的退款纠纷；网络侵权责任纠纷 275 件，占比 10.7%，包括因未成年人名誉权、肖像权、隐私权及个人信息等人格权益遭受侵害而引发的纠纷，其中网络欺凌、个人信息泄露等问题较为突出；信息网络买卖合同纠纷 75 件，占比 2.9%，主要是未成年人私自大额购物或开设网络店铺未按约发货引发的争议。

白皮书指出，大部分案件是未成年人作为原告的案件，占比 95%，由监护人代理提起诉讼，提出消费退款、侵权赔偿等诉讼请求。被告主要以各类网络服务提供者为主，涵盖网络游戏、网络音视频、网络社交、电子商务等多类平台。同时，网络主播、第三方运营主体等被告逐年增加，主体结构日趋多元。另有部分未成年人因不当网络言行、交易违约等成为侵权纠纷、合同纠纷的被告。从年龄结构来看，8 周岁以下未成年人占比 11%，8 至 16 周岁未成年人群体占比高达 77.3%，

16 周岁以上占比 11.7%，涉案最小当事人仅 4 岁，低龄未成年人网络风险防范能力薄弱问题凸显。（来源：北京互联网法院）

4. 上海法院依法打击新型网络犯罪典型案例

5 月 28 日，上海市高级人民法院举行新闻发布会，通报上海法院依法打击新型网络犯罪典型案例，分别是：

案例一：非法获取网站 token、cookies 的行为定性——李某等非法获取计算机信息系统数据案；

案例二：劫持用户手机强制进行广告推广的行为定性——蔡某非法控制计算机信息系统案；

案例三：为他人提供破解民用无人机禁飞限高服务的行为定性——高某、刘某康提供侵入计算机信息系统程序案；

案例四：利用自动化脚本及模拟器侵入系统解密快递单号非法牟利的行为定性——彭某、郭某烨非法获取计算机信息系统数据案；

案例五：组织他人利用 AI 洗稿并提供有偿发布服务的行为定性——徐某等非法经营案；

案例六：实施网络诋毁进行不正当竞争行为的定性——某科技公司、陈某、周某损害商品声誉案；

案例七：利用平台结算漏洞恶意清零以获取免费流量的行为定性——武某青、武某丹合同诈骗案；

案例八：贩卖数字人民币账户等公民个人信息的行为定性及刑事附带民事诉讼处理——王某等侵犯公民个人信息案。（来源：上海高院）

境内前沿观察三：人工智能安全专题

导读：5 月，我国人工智能政策推进重点聚焦中美人工智能治理对话、智能体规范应用、人工智能计量体系建设、人工智能应用伦理安全、地方“人工智能+”发展等方面。总体看，相关部署继续围绕人工智能创新发展与安全治理协同推进，既注重夯实智能体标准协议、数据资源和应用场景等发展基础，也更加突出分类分级治理、伦理安全原则和跨部门协同监管等配套机制建设。

国际合作方面，中美两国元首就人工智能问题进行建设性交流，并同意开展人工智能政府间对话。

智能体规范应用方面，国家网信办、国家发展改革委、工业和信息化部联合发布《智能体规范应用与创新发展实施意见》。《意见》提出构建智能体标准体系，系统布局关键技术、重要产品、数据交换、应用场景、质量评测、安全保障、可信认证等标准体系，并加强智能体互联协议等关键标准推广应用。

人工智能计量体系建设方面，市场监管总局、国家发展改革委联合印发《人工智能计量体系和能力建设指引（2026 版）》。《指引》聚焦人工智能“测不准”“度量衡”“全产业”赋能和“数据荒”等问题，提出部署 AI 系统内部状态监测与表征等关键技术攻关，推动建立可靠、安全、可信的人工智能计量标准。

地方应用和生态培育方面，湖北省人民政府办公厅印发《湖北省支持人工智能 OPC 发展若干措施（试行）》，围绕构建 OPC 全链条

服务生态、加强 OPC 要素赋能保障等方面提出支持措施。重庆市发展和改革委员会发布《重庆市“十五五”“人工智能+”发展规划（2026—2030 年）（征求意见稿）》，围绕人工智能应用场景体系、产业发展生态、自主创新能力、等提出措施，重点包括加快多模态公共数据归集、推进高质量数据集建设。

人工智能伦理安全方面，全国网络安全标准化技术委员会发布《人工智能应用伦理安全指引 1.0》。《指引》提出人工智能应用可能对人类主导权、公共秩序、个体认知与社会价值等产生影响，并提出增进人类福祉、尊重生命权利、坚持公平公正等伦理安全原则。

智能体安全风险方面，国家信息安全漏洞共享平台通报部分智能体技能包存在隐蔽执行恶意命令、诱导用户执行高危操作等问题。

关键词：智能体规范应用；人工智能计量；“人工智能+”；伦理安全

1. 中美同意开展人工智能政府间对话

5 月 19 日，外交部发言人郭嘉昆在例行记者会上答问时表示，作为两个人工智能大国，中美双方应该携手促进人工智能发展和治理，推动人工智能更好地服务人类文明进步和国际社会共同福祉。美国总统特朗普访华期间，两国元首就人工智能问题进行了建设性交流，同意开展人工智能政府间对话。（来源：新华网）

2. 国家网信办等三部门发布《智能体规范应用与创新发展实施意见》

5 月 8 日，国家网信办、国家发展改革委、工业和信息化部联合发布《智能体规范应用与创新发展实施意见》，围绕夯实发展基础、守牢安全底线、完善治理体系等四个方面，提出三十八项措施。

夯实发展基础方面，《意见》提出构建标准协议，建立智能体标准体系。制定智能体标准化工作指导文件，形成智能体标准框架，系统布局关键技术、重要产品、数据交换、应用场景、质量评测、安全保障、可信认证等标准体系，加快制定智能体与软件工具、应用服务、硬件外设接口等基础标准。加强智能体互联协议（AIP）等智能体互联关键国家标准、行业标准的推广应用。支持医疗、交通、媒体、公共安全等领域制定强制性标准。鼓励企业按照相关标准研发产品服务，提升智能体规范性。积极参与国际标准制定。

守牢安全底线方面，《意见》提出完善治理体系，构建分类分级治理框架。根据应用场景和潜在影响，审慎稳妥开展智能体分级治理。对于敏感领域及重点行业，由网信部门联合行业主管部门确定开放场景，根据相关法律法规、监管要求和安全防护标准，实行备案、检测、问题产品召回等管理措施。对于部分生活娱乐、日常办公等低风险领域，完善智能体评估测试工具，通过合规自测、信息报告、分发平台管理、行业自律等实现高效治理。（来源：网信中国）

3. 市场监管总局、国家发展改革委联合印发《人工智能计量体系和能力建设指引》

5 月 28 日消息，市场监管总局、国家发展改革委近日联合印发《人工智能计量体系和能力建设指引（2026 版）》，系统布局人工智能计量能力建设。《指引》围绕基础支撑、通用技术、核心技术、计量技术规范、计量服务产业、智能赋能计量等六大部分系统布局，打通实验室创新与行业应用“最后一公里”。

聚焦“测不准”难题，让人工智能更可信。针对算法“黑箱”、决策可解释性差等痛点，《指引》部署 AI 系统内部状态监测与表征等关键技术攻关，推动建立人工智能可靠、安全、可信计量标准，实现 AI 技术性能“可测量、可比较、可追溯”。

聚焦“度量衡”基准，让人工智能更精准。《指引》明确提出支持构建国家级计量技术研发应用中心，研制一批具有自主知识产权人

工智能计量标准装置，加快形成覆盖算法模型、算力效率、数据质量全链条计量能力，为人工智能产品提供统一“度量衡”。

聚焦“全产业”赋能，让智能经济更惠民。《指引》推动计量技术深度融入智能制造、智慧医疗、智慧交通等14个重点领域，围绕AI诊断算法可靠性等关键参数开展计量技术研究，助力解决产业数字化转型中质量评估难题，切实增强人民群众对人工智能应用的安全感、获得感。

聚焦“数据荒”难题，让人工智能有“粮”可依。《指引》明确提出构建具有最高计量特性数据集、标准参考数据集和测试数据集，建立基础资源共享机制，打破行业数据壁垒，实现数据安全共享，为人工智能算法训练和评测提供精准“粮草”。（来源：国家市场监督管理总局）

4. 全国网络安全标准化技术委员会发布《人工智能应用伦理安全指引1.0》

5月19日，全国网络安全标准化技术委员会发布《人工智能应用伦理安全指引1.0》。《指引》给出了人工智能应用伦理安全影响，提出了人工智能应用伦理安全理念与原则，规定了人工智能应用开发、服务提供和应用使用等安全指引。《指引》可为组织和个人开展人工智能应用活动提供指导，也可为相关主管部门、行业组织和有关机构推进人工智能伦理安全治理提供参考。《指引》正文包括范围、规范

性引用文件、术语和定义、人工智能应用伦理安全影响、伦理安全理念与原则、伦理安全指引六章。

伦理安全原则方面，《指引》提出九项原则，包括增进人类福祉、尊重生命权利、坚持公平公正、合理控制风险、保持公开透明、保护隐私安全等。例如，坚持公平公正方面，坚持公平包容和机会均等，避免人工智能应用造成不合理差别对待或加剧既有不公。坚持消除技术偏见和歧视，确保人工智能不对特定民族、信仰、国别、性别等群体以及特定组织或服务造成不公正影响。关注特殊群体与弱势群体权益，鼓励人工智能增进公共服务公平性与可及性。

伦理安全指引方面，包括通用指引、应用开发指引、服务提供指引、应用使用指引。例如，通用指引方面，《指引》提出十三项措施，包括：一是在开展人工智能应用活动前，预先评估应用目的及影响，充分保障国家安全、公共利益、组织及个人权益；二是以集体主义、人的全面发展等原则为基础，构建符合中国国情和文化传统的伦理规范体系；三是正确认识人工智能的应用价值、能力边界及潜在影响，避免盲目信赖、片面夸大和过度宣传；四是保留关键环节的人类判断、监督、干预和纠偏，避免人工智能过度替代人类决策等。（来源：网信中国）

5. 湖北省人民政府办公厅印发《湖北省支持人工智能 OPC 发展若干措施（试行）》

5 月 11 日，湖北省人民政府办公厅印发《湖北省支持人工智能 OPC 发展若干措施（试行）》，从构建 OPC 全链条服务生态、加强 OPC 要素赋能保障、强化 OPC 多元资本支撑、推动 OPC 成果转化应用四个方面提出十二项支持措施。

加强 OPC 要素赋能保障方面，《措施》提出深化数据要素流通。依托湖北省公共数据开放网设立 OPC 专区，安全有序供给市场主体、交通、文旅、医疗、教育等公共数据资源。为 OPC 提供定制化高质量数据，助力开展算法训练、模型优化、场景验证和产品创新。完善公共数据开放规则，在确保数据安全的前提下，为 OPC 开放定制化高质量公共数据资源。出台政策支持各级公共数据资源授权运营机构、数据流通服务机构向 OPC 提供免费或优惠的数据产品和服务。引导企业聚焦行业需求，开发市场稀缺、行业急需的高质量语料库，加强语料产品定制开发，丰富 OPC 数据资源供给。

推动 OPC 成果转化应用方面，《措施》提出支持 OPC 参与产业创新发展。支持 OPC 参与“人工智能+”行动，引导 OPC 运用人工智能技术服务实体经济，激活产业创新潜能。引导龙头企业面向社会发布服务需求，鼓励 OPC 主动承接、联合攻关，形成“核心聚焦+细分外包”的协同网络，提升产业发展韧性。支持 OPC 通过调用第三方大模型 API（应用程序编程接口）或者采用本地化部署等方式，开展垂直细分领域应用，各地可根据 API 流量、网关流水等给予适当

补助。支持 OPC 加入省算力产业创新联盟、数商联合会等组织，鼓励相关组织面向 OPC 开展主题培训、场景对接、成果展示、供需撮合、应用推广等常态化服务，帮助 OPC 深度融入产业生态。（来源：湖北省政府）

6. 重庆市发展和改革委员会发布《重庆市“十五五”“人工智能+”发展规划（2026—2030 年）（征求意见稿）》

5 月 12 日，重庆市发展和改革委员会发布《重庆市“十五五”“人工智能+”发展规划（2026—2030 年）（征求意见稿）》，从构建人工智能应用场景体系、构建人工智能产业发展生态、强化人工智能自主创新能力、夯实人工智能基础底座、加速人工智能开放共赢、确保人工智能安全可控六个方面提出措施。

夯实人工智能基础底座方面，征求意见稿提出激活数据要素活力，包括加快数据基础设施建设、强化高质量数据供给、推进数据要素市场化配置改革等。例如，征求意见稿提出加快多模态公共数据归集，依托一体化智能化公共数据平台，围绕人工智能大模型训练需求，推动政府部门、公共企事业单位按需编目归集多源多模态数据资源。分级分类推进高质量数据集建设，完善数据治理、清洗标注、质量核验与评测机制，在政务服务、城市治理等政府侧和智能网联汽车、生物医药、低空经济等产业侧，形成一批覆盖通用大模型预训练、行业大模型微调的行业通识、专识高质量数据集。

确保人工智能安全可控方面，征求意见稿提出构建多元协同治理格局。强化政府统筹协调，建立网信、公安、数据、市场监管等跨部门协同监管机制，联合开展执法检查，形成监管合力。强化行业协同治理，推动人工智能研发应用企业建立健全内部安全管理制度，鼓励行业企业牵头建立自律公约和合规指引，定期发布人工智能治理行业实践案例。畅通社会监督渠道，建立健全人工智能治理听证会机制，鼓励社会公众、媒体组织、行业专家实质性参与规则制定和方案优化。（来源：重庆市发展和改革委员会）

7. 国家信息安全漏洞共享平台（CNVD）通报部分智能体技能包（Skills）存在隐蔽执行恶意命令

5 月 11 日消息，国家信息安全漏洞共享平台（CNVD）近日发现多个智能体技能包（Skills）存在严重安全风险，可在 OpenClaw 等主流智能体系统中被恶意利用以执行未经授权的操作，或通过诱导方式使用户执行高危指令。

上述 Skills 主要涉及两类。一是部分 Skills 隐蔽执行恶意命令。该类 Skills 存在隐蔽命令执行的恶意行为：伪装成正常的办公助手、数据分析等 Skill，实际运行了下载木马等恶意文件的指令。智能体在用户不知情的情况下，根据恶意指令下载并运行木马或其他恶意文件，造成用户隐私和敏感数据泄露等严重后果。

例如，部分 Skills（“yahoofinance”“bybit-trading”等）将恶意插件伪装成“自动交易机器人”“效率辅助脚本”等热门工具，诱导

用户或智能体自动下载。这些带有极强欺骗性的插件暗藏窃密木马，一旦被加载运行，便会直接绕过常规安全防御，在后台窃取用户电脑上的系统密码及核心业务凭证。此类恶意插件累计下载上万次，可能导致大量用户的数字资产和敏感数据遭到窃取，暴露出第三方 AI 工具库存在的严重安全审核盲区。

二是部分 Skills 诱导用户执行高危操作。该类 Skills 存在诱导使用第三方 MCP/插件进行付费、非法交易等操作：如在 Skill 中推荐或内置来源不可信的 MCP 服务或插件程序，诱导用户在不可靠第三方网站注册付费，或者引入包含非法加密货币交易等隐藏恶意功能的插件。看似便捷的“智能助手”，成为数字时代悄然张开的“引流推手”。

例如，Skill“MoltsPay”宣称功能为帮助用户进行钱包管理工作，实则是在本地生成加密货币钱包，并通过“注册领取 333ORA 代币奖励”诱导用户使用加密货币进行交易。此类 Skill 存在三方面风险：一是在我国，虚拟货币（比特币、以太坊等）相关业务活动（如兑换、中介、钱包服务）已被明确禁止；二是 Skill 设置“注册送 333ORA、提现门槛却是 3333ORA”的资金陷阱，用户无法立即取出任何奖励，需绑定 MoltWork 等关联平台持续完成任务才能“积累”差额，诱导用户不断投入却无法提现；三是私钥以明文形式写入本地固定路径，系统一旦被植入恶意模块或文件遭窃取，用户数字资产将面临直接被盗取且无法追回的风险。

国家信息安全漏洞共享平台建议，个人用户应坚持从官方渠道获取 Skills，审慎授予权限并遵循最小化原则，及时回收敏感权限，定

期清理不再使用的 Skills 与敏感对话记录，同时开启多因素认证以保护账户安全；企业层面则需建立 Skills 准入白名单机制，入库前做好安全检查，优先在隔离网络部署智能体，按照数据敏感性对智能体分级管理，并实施数据脱敏与临时授权策略。（来源：CNVD）

8. 上海、重庆网信部门开展“清朗·整治 AI 应用乱象”专项行动

5 月，根据中央网信办统一部署，上海、重庆网信部门结合属地实际，积极组织开展为期 4 个月的“清朗·整治 AI 应用乱象”专项行动。

本次专项行动分两个阶段开展。第一阶段为“清朗·AI 应用服务典型违规问题”专项治理行动，重点整治未按规定履行大模型备案登记义务、安全审核能力不足、大模型训练语料安全、AI 数据投毒、生成合成内容标识落实不到位等问题，强化 AI 技术源头治理。第二阶段为“清朗·整治 AI 信息内容乱象”专项行动，聚焦利用 AI 技术生成“数字泔水”、制作发布虚假信息、散播暴力低俗等不良信息、假冒仿冒他人、侵害未成年人权益、从事网络水军活动等问题，坚决清理违法不良信息，依法处置处罚违规账号、MCN 机构和网站平台。（来源：网信上海、网信重庆）

境外前沿观察：月度速览十则

导读：5 月，境外各国及国际组织围绕智能体人工智能安全、人工智能风险分类与合规评估、云主权、数据保护和平台系统性风险治理等领域持续推进政策法律安排。整体看，相关动向一方面更加突出对人工智能系统全生命周期、智能体工具调用的规则约束，另一方面也进一步强化对公共部门云服务、在线平台和个人信息处理活动的安全治理与合规监管。

人工智能安全治理方面，澳大利亚、美国、加拿大、新西兰、英国网络安全机构联合发布《审慎部署智能体人工智能服务》指南，系统梳理智能体人工智能引入 IT 环境后面临的网络安全挑战、主要风险及安全部署实践。新加坡 IMDA 发布《智能体人工智能治理示范框架》1.5 版，在延续事前评估并限定风险、确保人类有意义地承担责任、实施技术控制和流程、赋能终端用户责任等“四维治理框架”的基础上，进一步将访问控制、护栏和持续监测等纳入智能体核心组成部分。七国集团和欧盟联合发布《人工智能软件物料清单最低要素》指南，围绕元数据、系统级属性等最低要素集群，推动提升人工智能系统组成、依赖、数据来源、漏洞和安全措施的透明度。

人工智能规则实施与应用治理方面，越南细化《人工智能法》实施规则，建立高风险、中风险、低风险人工智能系统风险分类机制。欧盟推迟《人工智能法》部分高风险人工智能系统义务和人工智能生成内容水印义务适用时间。欧盟委员会还发布更新版《欧洲研究区关

于在研究中负责任使用生成式人工智能》动态指南，要求研究人员、研究机构和科研资助机构关注生成式人工智能在会议记录、讨论总结等场景中的保密、数据保护、知识产权和科研诚信风险，并强调人工智能系统不能作为作者或共同作者。

数据保护、平台治理和数字基础设施方面，葡萄牙批准《国家主权云计划》，通过公共行政部门业务流程及其支撑数据、系统分级认定，设定主权、安全和韧性要求。加拿大发布对 OpenAI 旗下 ChatGPT 的联合调查结果，认为 OpenAI 初期训练 ChatGPT 的方式存在过度收集个人信息、未取得有效同意、透明度不足、个人访问更正删除机制不足和问责不足等问题。欧盟委员会依据《数字服务法》对 Temu（拼多多海外版）处以 2 亿欧元罚款，认为其未能充分识别、分析和评估平台非法商品流通所带来的系统性风险。法国国家信息与自由委员会因 IQVIA 在健康数据仓库管理中存在个人信息告知、权利行使和数据安全等方面违规，对其处以 500 万欧元罚款。

关键词：智能体人工智能；人工智能风险分类；人工智能软件物料清单；数据保护；主权云

1. 五国网络安全机构联合发布《审慎部署智能体人工智能服务》指南

5 月 1 日，澳大利亚、美国、加拿大、新西兰、英国的网络安全机构联合发布《审慎部署智能体人工智能服务》指南。该指南聚焦基于大语言模型的智能体人工智能系统，面向政府、关键基础设施运营者和行业组织，系统梳理智能体人工智能引入 IT 环境后面临的网络安全挑战、主要风险及安全部署实践。

指南指出，智能体人工智能不同于一般生成式人工智能，其能够与外部工具、数据源、记忆模块和规划工作流深度集成，具备一定自主规划和执行能力，因此在提升自动化效率的同时，也会放大传统网络安全风险和大模型固有风险。指南建议，各组织应将智能体人工智能安全纳入既有网络安全框架，而非作为独立议题处理；在采用智能体人工智能时，应优先用于低风险、非敏感任务，绝不应授予其广泛或无限制访问权限，尤其不得使其直接接触敏感数据或关键系统。

在治理建议方面，指南提出覆盖设计、开发、部署和运行全生命周期的安全实践，包括落实最小权限、强身份管理、可信注册表、纵深防御、输入验证、红队测试、第三方组件管理、人在回路审批等措施。指南还强调，未来应加强智能体人工智能威胁情报共享，开展面向智能体系统的专项安全评估。（来源：美国 CISA）

2. 越南细化人工智能法实施规则，建立人工智能系统风险分类与合规评估机制

5 月 1 日，越南第 142/2026/ND-CP 号法令生效，对越南《人工智能法》的若干条款和实施措施作出细化规定。该法令确立了人工智能系统风险分类和合规评估的基本规则，要求人工智能系统分类应当依据《人工智能法》和该法令规定的风险等级进行。

法令将人工智能系统划分为高风险、中风险、低风险三个等级。其中，高风险人工智能系统原则上以总理发布的高风险人工智能系统目录为准；影响程度、使用领域、用户范围和影响规模等，是制定该目录的判断标准。根据法令，人工智能系统提供者应当在系统投入使用前完成风险分类，并对分类结果的准确性、真实性承担法律责任。部署方修改、集成、变更系统功能或者使用目的，导致出现新的风险或者更高风险时，应当与提供者协同重新审查并调整风险分类。

在合规评估方面，法令要求提供者和部署方对高风险人工智能系统开展符合性评估。对于嵌入产品、货物或者服务中的人工智能系统，如其已受行业法律、标准技术规范或者产品质量法律调整，相关主体仍应遵守相应行业规则，同时履行人工智能组件特有风险管理要求。法令还强调，不应在分类、合规评估和检查环节造成重复监管等。（来源：越南政府）

3. 欧洲议会与欧盟理事会就简化《人工智能法》部分规则达成临时协议

5 月 7 日，欧洲议会与欧盟理事会谈判代表就数字综合简化方案中有关修改欧盟《人工智能法》部分规则的内容达成临时协议，旨在降低人工智能系统提供者的合规负担，同时保留《人工智能法》的核心规定和基于风险的监管方法。

协议对部分规则适用期限作出延期调整。其一，针对基于使用场景认定的高风险人工智能系统，包括生物识别、关键基础设施、教育、就业、执法、移民、庇护和边境管理等领域的人工智能系统，相关义务由原定 2026 年 8 月 2 日适用，推迟至 2027 年 12 月 2 日适用。其二，针对作为产品或产品安全组件，并受欧盟特定产品领域安全与市场监管规则约束的高风险人工智能系统，相关义务由原定 2027 年 8 月 2 日适用，推迟至 2028 年 8 月 2 日适用。其三，针对人工智能生成内容的水印义务，其适用时间由《人工智能法》原定 2026 年 8 月 2 日推迟至 2026 年 12 月 2 日。

协议还新增针对“脱衣”类人工智能应用的禁止性规定。欧洲议会和欧盟理事会同意，禁止用于生成儿童性虐待材料，或者在未经本人同意的情况下描绘可识别个人私密部位、露骨性行为的人工智能系统，相关内容包括图像、视频或音频。该禁令适用于以下情形：（1）以生成此类内容为目的，将人工智能系统投放欧盟市场；（2）在未采取合理安全措施防止生成此类内容的情况下，将相关人工智能系统

投放欧盟市场；（3）部署者以生成此类内容为目的使用这些系统。企业须在 2026 年 12 月 2 日前完成合规调整等。（来源：欧盟委员会）

4. 欧盟委员会发布更新版《欧洲研究区关于在研究中负责任使用生成式人工智能》动态指南

5 月 8 日，欧盟委员会发布更新版《欧洲研究区关于在研究中负责任使用生成式人工智能》动态指南，旨在为研究人员、研究机构和科研资助机构提供简明、可操作的建议，推动生成式人工智能在科研活动中的负责任应用。

本次更新新增或强化了若干具体建议，包括：研究人员和研究机构应关注第三方在会议记录、讨论总结、文件概览等场景中使用生成式人工智能可能带来的保密、数据保护和知识产权风险；在与第三方互动时，应说明自身是否使用相关人工智能工具以及如何保护被收集信息。指南还特别提示机构关注“隐藏提示词”风险，即嵌入人工智能系统、但不易被人类监督发现的指令。

在科研诚信方面，指南强调研究人员仍应对科研产出承担最终责任，应批判性看待生成式人工智能输出，注意偏见、幻觉和不准确内容；人工智能系统不能作为作者或共同作者，因为作者身份意味着主体能动性和责任承担。指南还要求研究人员遵守适用的国家、欧盟和国际法律，特别是知识产权和个人数据保护规则。（来源：欧盟委员会）

5. 七国集团和欧盟联合发布《人工智能软件物料清单最低要素》指南

5 月 12 日，七国集团和欧盟联合发布《人工智能软件物料清单最低要素》指南。

指南提出，人工智能软件物料清单应包含以下几类最低要素集群：一是元数据集群，用于记录与人工智能软件物料清单本身相关的信息，而非人工智能系统中的单个组件或子要素；二是系统级属性集群，用于记录人工智能系统整体层面的信息，包括由分类器、大型语言模型或 AI 智能体等多个人工智能要素组成的系统内部运作信息，并涵盖系统所使用的软件依赖项和框架，以及系统组件如何交互、如何处理用户数据等内容；三是模型集群，用于识别人工智能系统所使用的模型，说明每个模型权重的生成方式，并概述模型属性及已知限制；四是数据集属性集群，用于记录模型全生命周期中所使用的数据集信息，包括能够说明数据身份和来源的核心内容；五是基础设施集群，用于记录支撑人工智能系统正常运行和维护所需的物理及虚拟基础设施，包括基础设施软件和基础设施硬件；六是安全属性集群，聚焦适用于人工智能模型和系统的网络安全措施，包括安全控制、安全合规、网络安全政策信息，以及与系统组件相关的已知漏洞编号、漏洞数据库记录和安全公告等信息；七是关键绩效指标集群，用于记录人工智能系统及其组件，包括集成于系统内的人工智能模型在生命周期阶段中的相关指标，主要包括安全指标和运行性能指标等。（来源：德国联邦信息安全办公室）

6. 新加坡 IMDA 发布更新版《智能体人工智能治理示范框架》

5 月 20 日，新加坡资讯通信媒体发展局（IMDA）发布《智能体人工智能治理示范框架》1.5 版。该版本在 2026 年 1 月发布的 1.0 版基础上修订形成，吸收了 60 余家企业的反馈意见，进一步完善智能体人工智能的风险识别、责任分配、技术控制和用户责任等治理要求。

更新版延续原有“四维治理框架”，即事前评估并限定风险、确保人类有意义地承担责任、实施技术控制和流程、赋能终端用户责任，但进一步增强了实践操作性。一是在智能体组成部分方面，将访问控制、护栏、人类审批、日志记录和持续监测等安全可靠性组件纳入智能体核心组成部分，强调智能体治理不应仅关注模型、工具和协议，也应关注运行时控制与可追责机制；二是在协议部分，补充了智能体商业领域的新型协议，反映出智能体正从信息处理、工具调用进一步进入支付、交易和商业履约等高风险场景；三是在风险部分，新增系统性与多智能体风险，重点关注智能体高速、大规模行动可能带来的实时监督困难、错误级联放大、智能体蔓延、协作失败、目标冲突、潜在合谋以及跨系统、跨组织交互带来的不可预测性等。（来源：新加坡资讯通信媒体发展局）

7. 葡萄牙批准《国家主权云计划》

5 月 27 日，葡萄牙部长理事会通过第 102/2026 号决议，批准《国家主权云计划》，并将其纳入《葡萄牙数字战略》2026—2027 年行动计划框架。该计划旨在推动公共行政部门安全采用云计算服务，强

化国家数字主权、安全性和韧性，保障公共服务连续性，并促进公共行政体系现代化转型。

该计划主要通过三个维度实施：一是对公共行政部门业务流程及其支撑数据、系统进行分级认定，依据敏感性、关键性和保密性确定相应主权水平和安全要求；二是针对不同分级水平设定具体主权、安全和韧性要求，明确国家所使用数字基础设施和云服务应满足的技术与运营条件；三是建设主权数字基础设施，根据业务流程的主权要求确定优先顺序，并制定分阶段采用主权云解决方案的行动计划。

该计划强调，其目标并非单纯建设云基础设施，而是为市场运行创造条件，确保公共行政部门内部供给和市场供给均符合主权与安全要求。计划还提出发展主权人工智能能力，包括建立统一云服务目录、制定部门性云服务采用计划、完善云计算服务框架协议等。同时，葡萄牙还将加强公共行政部门在云计算和数字主权方面的能力建设，对信息技术专家、管理人员和项目负责人开展培训，并简化云服务采购流程。（来源：葡萄牙部长会议）

8. 加拿大 OPC 发布对 OpenAI 旗下 ChatGPT 的联合调查结果

5 月 6 日，加拿大隐私专员办公室（OPC）联合魁北克、卑诗省和阿尔伯塔省隐私监管机构，发布对 OpenAI 旗下 ChatGPT 的联合调查结果。调查重点审查 OpenAI 在开发和部署 ChatGPT 过程中，收集、

使用和披露加拿大个人信息的做法是否符合联邦及省级私营部门隐私法律。

调查认为，OpenAI 初期训练 ChatGPT 的方式不符合加拿大相关隐私法律要求。监管机构指出，相关问题主要包括：过度收集个人信息、未取得有效同意，透明度不足，ChatGPT 输出中涉及个人信息的事实错误和“幻觉”问题，个人访问、更正和删除权机制不足，以及对其控制下个人信息的问责不足。

OpenAI 已采取或承诺采取多项整改措施，包括大幅限制用于训练新模型的个人信息和敏感信息，使用过滤工具识别并对训练数据中的姓名、电话号码等个人信息进行脱敏处理，并制定个人信息保存和删除政策等。（来源：加拿大隐私专员办公室）

9. 因未充分评估非法商品系统性风险，欧盟委员会对 Temu 处以 2 亿欧元罚款

5 月 28 日，欧盟委员会宣布，依据《数字服务法》（DSA）对电商平台 Temu 处以 2 亿欧元罚款，理由是 Temu（拼多多海外版）未能审慎识别、分析和评估其平台上非法商品流通所带来的系统性风险，以及由此可能对欧盟消费者造成的损害。

欧盟委员会表示，其掌握的证据显示，欧盟消费者在 Temu 平台上很可能接触到非法商品，而 Temu 提交的 2024 年风险评估未达到 DSA 规定的标准。欧盟委员会指出，Temu 的风险评估主要依据整个电子商务行业的一般性风险信息，而非围绕 Temu 自身服务形成的公

开报告和测试结果等具体证据；同时，Temu 严重低估了欧盟消费者接触非法商品的可能性。欧盟委员会调查中纳入的一项“神秘购物”测试显示，被抽检充电器中有很高比例未能通过基本安全测试，被检测婴幼儿玩具中也有相当比例存在中高程度安全风险，包括化学物质超过法定安全限值，或因可拆卸零部件造成窒息风险等。此外，Temu 也未能对其推荐系统以及相关商品推广计划的服务设计是否可能放大非法商品传播风险进行充分评估。

下一步，Temu 须在 2026 年 8 月 28 日前依据 DSA 第 75 条向欧盟委员会提交行动计划，说明其拟采取何种措施纠正风险评估义务违反问题。（来源：欧盟委员会）

10. 因健康数据仓库管理违规，法国国家信息与自由委员会对 IQVIA 处以 500 万欧元罚款

5 月 28 日，法国国家信息与自由委员会发布消息称，其于 5 月 26 日对 IQVIA OPERATIONS FRANCE 处以 500 万欧元罚款，原因是该公司在健康数据仓库管理中未遵守旨在限制个人风险的保障措施，并在信息告知、权利行使和数据安全等方面存在违规。

IQVIA OPERATIONS FRANCE 是 IQVIA 集团子公司，主要开展咨询和研究服务，可为自身或制药实验室开展疾病和治疗相关研究。为实施相关研究，该公司依托两个经委员会授权设立的健康数据仓库：一是 2018 年获批、由约 1.4 万家药房提供数据的 LRX 数据仓库；二是 2021 年获批、由数千名医生提供数据的 EMR 数据仓库。委员会

表示，健康数据属于高度敏感数据，在其处理健康领域授权申请时，通常要求采取多项保障措施，以限制对个人的风险并确保相关权利得到尊重。

委员会收到个人和协会投诉对IQVIA及合作药房开展多次检查，并认定该公司未遵守此前授权条件，违规内容涉及个人信息告知、权利行使和数据安全。委员会指出，涉案数据仓库涉及数千万人员的健康数据，且IQVIA在相关市场中具有重要地位并具备相应财务能力，因此决定作出500万欧元罚款并公开该决定。（来源：法国国家信息与自由委员会）

行业前沿观察：各地协会动态

各地协会、单位立足本职服务大局，紧扣行业发展需求，广泛开展行业交流、安全科普、人才培养、标准建设及社会服务等活动。苏州市互联网协会协办的网络安全专家讲师赋能 AI 办公 助力社会组织实战营圆满结营；甘肃省商用密码行业协会召开二届四次理事会暨 2026 年第二次会长办公会；肇庆市计算机学会成功举办科技赋能成长 创新点亮未来——人工智能科普进校园主题活动；北京网络空间安全协会在港成功举办“第二届京港澳博士后青年人才发展交流大会”；湖南省网络空间安全协会等保专委会召开 2026 年第一次工作会议；上海市信息安全行业协会成功举办心肺复苏（CPR+AED）专项急救技能专场培训；金华市网商协会主办的金华网商绿色直播为民行动之“云享兰溪枇杷”顺利开播；南昌市网络信息安全协会承办的 2026 网民网络安全感满意度调查活动江西省动员宣讲会顺利召开；东莞市信息技术联合会教育行业交流研讨会顺利举行；安徽省网络安全协会顺利召开 2025 年度安徽省网络安全等级保护测评机构通报会；东莞市信息与网络安全协会赴佛山开展走访交流活动；南通市信息网络安全协会召开第五次会员代表大会及第五届理事会第一次会议；广州网络空间安全协会网络安全公益大讲堂走进广东工贸职业技术学院；陕西省信息网络安全协会主办的 2026 第十届丝绸之路网络安全论坛在西安圆满成功举办；西藏自治区互联网协会成功举办公文智能化应用培训；武汉市网络安全协会承办的 2026 年“黄鹤杯”网络安全人才创新

大赛启幕；上海市信息网络安全管理协会聚焦 AI 安全共治，赋能行业合规发展，共探人工智能安全与发展。

关键词：行业交流、标准建设、人才培育、安全科普、社会服务、产教融合、国际交流、组织建设

1. 苏州市互联网协会协办的网络安全专家讲师赋能 AI 办公 助力社会组织实战营圆满结营

5 月 6 日，由苏州市社会组织总会主办，苏州市人工智能行业协会、苏州市互联网协会协办的苏州市社会组织 AI 办公应用实战营顺利结营，网络安全专家讲师现场授课赋能，提升社会组织从业人员数字办公素养与安全履职能力，30 余名社会组织从业人员参与学习与实操演练，成效显著。

2. 甘肃省商用密码行业协会召开二届四次理事会暨 2026 年第二次会长办公会

2026 年 5 月 9 日，甘肃省商用密码行业协会二届四次理事会暨 2026 年第二次会长办公会在甘肃省密码与信创产教融合发展中心（筹）召开。协会会长、副会长、理事及会员代表等共 50 余人参会，省国家密码管理局相关处室人员列席。会议由协会会长主持。会议传达学习了省委组织部、省委社会工作部、省民政厅等部门近期出台的关于加强社会组织建设系列文件精神。研究审议了协会法人调整、副会长调整事宜，审议通过了新增入会和退会单位名单，以及《甘肃省商用密码行业协会助学行动实施办法（修订稿）》和《甘肃省商用密码行业协会“密码技术应用员”职业技能等级认定资质申请工作方案》。

3. 肇庆市计算机学会成功举办科技赋能成长 创新点亮未来——人工智能科普进校园主题活动

为普及人工智能科学知识，激发学生科学探索热情，提升科学素养与创新思维，营造爱科学、学科学、用科学的校园氛围，2026 年 5 月 9 日下午，肇庆市人工智能科普进校园主题活动在肇庆市第十一小学书香厅顺利举行。

本次活动由肇庆市技师学院、肇庆市教师发展中心、肇庆市端州区科学技术协会指导，肇庆市计算机学会、肇庆市信息协会主办，肇庆市第十一小学承办。端州区科学技术协会副主席梁伟宇，肇庆市第十一小学党支部书记、校长黎结宁，副校长陈丽珊，肇庆市计算机学会副理事长兼秘书长、学校科学副校长梁永志，肇庆市技师学院信息工程系副主任梁思勤，武当武术广东肇庆推广中心主任何霞，肇庆麦芽联城口腔医院总监江义波等嘉宾出席活动。

4. 北京网络空间安全协会在港成功举办“第二届京港澳博士后青年人才发展交流大会”

为深入贯彻落实习近平总书记关于加快建设世界重要人才中心和创新高地的指示精神，全面服务新时代人才强国战略，深化京港澳三地青年科技人才交流合作，推动博士后等高水平人才融合发展，“第二届京港澳博士后青年人才发展交流大会”于 2026 年 5 月 11 日至 13 日在香港成功举办。

大会以“智汇京港澳·科创耀未来”为主题，由北京市人力资源和社会保障局主办，香港特别行政区政府创新科技及工业局、澳门特别行政区政府教育及青年发展局、港澳各有关高校支持，北京网络空间安全协会、北京继续教育协会、国际高端人才交流联盟、香港网络空间安全协会承办，北京北控京泰投资管理有限公司联合承办，香港国际人才交流中心、网安联（北京）国际人才交流中心协办。

5. 湖南省网络空间安全协会等保专委会召开 2026 年第一次工作会议

为进一步规范全省网络安全等级保护测评工作管理，健全专家队伍体系，完善行业自律与评价机制，全面提升等保测评服务质效，在主管单位湖南省公安厅指导下，湖南省网络空间安全协会网络安全等级保护专委会于 5 月 13 日组织召开 2026 年第一次工作会议。省公安厅网技总队翟凌杰莅临会议指导，等保专委会主任及副主任单位、22 家成员单位代表参会，共商全省等保行业规范建设、专家队伍管理、行业自律发展等年度重点工作。

6. 上海市信息安全行业协会成功举办心肺复苏（CPR+AED）专项急救技能专场培训

为进一步提升会员单位从业人员的安全防范意识与突发事件应急处置能力，切实保障员工生命健康安全，2026 年 5 月 16 日（周六），上海市信息安全行业协会秘书处特别对接市级急救专业机构，成功举

办了“心肺复苏与 AED 使用急救技能”内部定制专场培训。本次培训分设上午、下午两个批次，来自协会副会长、理事、会员单位的近 50 名企业负责人及网络安全负责人参与。

7. 金华市网商协会主办的“云享兰溪枇杷”助农直播活动顺利开展

5 月 16 日上午，由金华市市场监督管理局、金华市农业农村局、金华市商务局指导，金华市网商协会、金华市网络界人士联谊会主办，九三学社金华农业支社、金华市商业联合会、金华市广告协会、上海财经大学浙江学院商学院、博瑞会展、乡野直播协办，乐农直播共富工坊、兰溪市黄店镇鸡啼坞家庭农场承办的“云享兰溪枇杷”助农直播活动，在兰溪鸡啼坞枇杷园及乐农直播共富工坊，通过多平台同步直播方式顺利开展。

8. 南昌市网络信息安全协会承办的 2026 网民网络安全感满意度调查活动江西省动员宣讲会顺利召开

5 月 16 日上午，2026 网民网络安全感满意度调查活动江西省动员宣讲会在南昌隆重举行。宣讲会由 2026 年网民网络安全感满意度调查活动组委会主办，南昌市网络信息安全协会承办，旨在深入贯彻“网络安全为人民，网络安全靠人民”理念，全面部署我省 2026 年网民网络安全感满意度调查工作，凝聚社会各界合力，筑牢赣鄱大地网络安全防线。宣讲会得到省内外各界高度关注，网络安全领域专家学

者、社会组织负责人、企业代表、志愿服务团队及新媒体从业人员等140余人齐聚一堂，共商调查推进大计，共绘江西网络安全建设蓝图。

9. 东莞市信息技术联合会教育行业交流研讨会顺利举行

2026年5月18日，由东莞市信息技术联合会与中国计算机学会（CCF）东莞会员活动中心联合主办，“融党建初心 筑科技根基——教育行业交流研讨会”顺利举办。我会会长魏文红先生、秘书长温婷婷女士，CCF东莞分部秘书长余梓彤先生代表出席会议并作开场发言。

10. 安徽省网络安全协会顺利召开2025年度安徽省网络安全等级保护测评机构通报会

2026年5月19日上午，“2025年度安徽省网络安全等级保护测评机构通报会”在安徽省网络安全协会2号会议室召开。来自在皖开展业务的省内外网络安全测评机构代表齐聚一堂，围绕2025年度工作成效、质量状况及未来发展进行了全面总结与交流。

11. 东莞市信息与网络安全协会赴佛山开展走访交流活动

为加强行业协会间经验互通，助力区域数字化建设与网络安全防护体系高质量发展，2026年5月21日，东莞市信息与网络安全协会组织赴佛山市开展走访交流活动，先后走访佛山市网络安全和信息化协会、新明珠集团。广东唯一网络科技有限公司、北京江南天安科技

有限公司、广东数标检测认证中心有限公司等企业代表一同参与了此次走访交流活动。

12. 南通市信息网络安全协会召开第五次会员代表大会及第五届理事会第一次会议

2026 年 5 月 26 日下午，南通市信息网络安全协会第五次会员代表大会在张謇企业家学院謇业楼 103 教室顺利召开。118 名协会会员代表、友好协会——南通市互联网协会、南通市电脑商会的嘉宾，以及业务主管单位市公安局相关部门的负责人参加了本次会议。

13. 广州网络空间安全协会网络安全公益大讲堂走进广东工贸职业技术学院

为助力网络安全人才培养，促进产教融合，5 月 26 日，网络安全公益大讲堂走进广东工贸职业技术学院，面向学院网络工程系三个专业的师生开展了一场网络安全专题宣讲，50 余名学生积极参与，现场气氛热烈。广东工贸职业技术学院对本次活动高度重视，副院长黄培泉、系主任高学勤、办公室主任袁佳、专业带头人吴倩等领导出席。活动由高学勤主任主持。

14. 陕西省信息网络安全协会主办的2026第十届丝绸之路网络安全论坛在西安圆满成功举办

5月28日，2026第十届丝绸之路网络安全论坛在陕西宾馆成功举办，本届论坛由陕西省信息网络安全协会主办，得到了北京网络空间安全协会网安联发展工作委员会的支持和华为技术有限公司、杭州安恒信息技术股份有限公司、杭州宏杉科技股份有限公司协办。

本次论坛以“共筑网络安全，共享数智文明”为主题，汇聚行业顶尖智慧，深入探讨AI在网络安全领域的创新应用、风险防控与治理路径，助力构建安全可信，有韧性的数字生态。来自省内外400余名专家、各省区网安协会代表、行业从业人员、企事业单位相关负责人参加本次大会。

15. 西藏自治区互联网协会成功举办公文智能化应用培训

为深入贯彻落实习近平总书记关于网络强国的重要思想，推动人工智能技术在政务办公中的普及应用，助力提升全区公文处理智能化水平，5月28日下午，由西藏自治区互联网协会主办的公文智能化应用培训在柳梧城投大厦B座3楼成功举办。来自自治区党政机关、企事业单位等20余家单位的100余名干部职工参加培训。

16. 武汉市网络安全协会承办的 2026 年“黄鹤杯”网络安全人才创新大赛启幕

5 月 29 日，2026 年“黄鹤杯”网络安全人才创新大赛在国家网络安全人才与创新基地正式启动。大赛以“人机共战砺网安精兵产才融合筑产业高地”为主题，由武汉市委网信办、武汉市总工会、网络空间安全学院、国家网络安全人才与创新基地联合主办，武汉市网络安全协会、国家网络安全人才与创新基地产业联盟承办，东风汽车集团研发总院、小米安全中心、湖北省汽车信息安全技术创新中心、智能网联汽车网络安全湖北省工程研究中心提供支持，全国相关高校院所和领军企业的学者、专家、负责人与参赛代表共同见证赛事启幕。

17. 上海市信息网络安全管理协会聚焦 AI 安全共治，赋能行业合规发展，共探人工智能安全与发展

人工智能技术高速迭代，安全可控、合规发展、责任共治已然成为人工智能产业高质量发展的核心底色。为搭建多方交流平台，凝聚行业发展共识，由上海市信息网络安全管理协会主办的人工智能安全与发展沙龙，于 2026 年 6 月 5 日在创智天地 6 号楼 V 聚场正式举办。 上海市公安局网络安全保卫总队总队长季增令、上海市公安局杨浦分局常务副局长朱荣、中共上海市委网络安全和信息化委员会办公室网络技术处副处长郑森峰、上海市高级人民法院研究室副主任、三级高级法官高佳运等多位领导莅临现场指导。