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7月第7期（总第36期）

2026年7月10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 7 月第 7 期（总第 36 期）

2026 年 7 月 10 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：6 月，国家数据局、国家网信办、国家能源局等部门围绕数据开发和利用、数据分类分级、数据安全、分布式数字身份互通互认等方面发布相关规定。地方层面，江西、浙江、北京、上海等地围绕公共数据授权运营和开发利用、行政裁量等作出制度安排。

部委层面，国家数据局印发《关于推进行业高质量数据集建设行动的实施方案》，这是国家层面首次对数据赋能人工智能发展作出的系统性部署。行业领域的数据分类分级规则加快落实，《金融信息服务数据分类分级指南》《能源行业数据分类分级指南（2026 年版）》相继发布，明确金融信息服务数据、能源行业数据的分类分级、重要数据识别规则等内容。《实施网络安全标识的产品目录（第一批）》及相关实施规则发布，第一批产品目录仅包括消费类网联摄像头一类产品。国家互联网信息办公室发布《促进分布式数字身份互通互认应用规定（征求意见稿）》，明确相关主体可自愿通过身份链注册分布式数字身份，经权威身份认证机构核验后，签发分布式数字身份标识符和实名身份凭证。三部门联合公布《网络数据安全风险评估办法》，提出在国家数据安全工作协调机制指导下，国家网信部门会同国务院电信、公安等有关部门建立网络数据安全风险评估专项工作机制，指导、监督风险评估工作。

地方层面，江西省发展和改革委员会、江西省政务服务办印发《江西省省级公共数据资源整体授权运营实施方案》《江西省交通运输领域省级

公共数据资源授权运营实施方案》。《江西省省级公共数据资源整体授权运营实施方案》从实施背景、运营机构遴选、数据供给、授权运营实施、收费定价与收益分配、安全保障及组织保障等方面作出系统部署。《江西省交通运输领域省级公共数据资源授权运营实施方案》是整体方案框架下的首个分领域实施方案，明确交通运输领域授权运营方案。陕西省委办公厅、省政府办公厅发布《关于加快公共数据资源开发利用的实施意见》，围绕扩大数据资源供给、加强授权运营监管、释放公共数据价值等五个方面提出十三项措施。浙江省科学技术厅、浙江省数据局发布《浙江省科学数据汇交与共享管理办法（试行）》，加强和规范浙江省科学数据资源管理，加快建设具有国际影响力的科学数据库和人工智能就绪高质量科学数据集，推动科学数据价值挖掘和高效利用，赋能“人工智能+科学”创新体系建设。北京市经济和信息化局印发《北京市经济和信息化领域行政处罚裁量基准》，要求应当按照违法行为的性质、情节、社会危害性等情况划分不同裁量阶次，各裁量阶次按照违法情节由轻到重、处罚阶次由低到高列明。

关键词：电子认证服务；高质量数据集；数据分类分级；分布式数字身份；行政裁量基准

（一）部委层面动向

1. 国家密码管理局修订发布《电子认证服务使用密码管理办法》

5 月 30 日，国家密码管理局发布修订后的《电子认证服务使用密码管理办法》。

《办法》共 25 条，主要修订内容如下：关于适用范围，《办法》明确，在中华人民共和国境内的电子认证服务使用密码及其监督管理，适用本办法。关于管理体制，根据新修订的《商用密码管理条例》有关规定，《办法》明确国家密码管理局和地方各级密码管理部门对电子认证服务使用密码行为实施监督管理。关于许可证办理，《办法》增设了电子认证服务使用密码许可证办理条件，规范了许可证办理的申请材料和申请受理程序，完善了审查审批程序、技术评审措施和许可证件内容，明确了许可事项变更和期满延续办理要求。

此外，关于运行规范，根据国家有关加强事中事后监管要求和实际监管需求，《办法》对获得《电子认证服务使用密码许可证》的机构提出了安全管理、密钥服务、运行维护、合规性评估和人员培训等规范管理要求，以保障电子认证服务系统安全可靠运行和密码使用安全。关于监督管理和法律责任，《办法》进一步明确了密码管理部门监管职责、监督检查方式、监督检查措施及相关实施要求，明确了违反有关要求所应承担的法律责任，以及对从事电子认证服务使用密码监督管理工作人员的监管责任。

6 月 29 日，国家密码管理局发布《关于做好〈电子认证服务使用密码管理办法〉实施工作的公告》。公告指出，按照《办法》第六条、第七条有关规定，现委托各省、自治区、直辖市密码管理部门，新疆生产建设兵团密码管理部门负责受理本行政区域的电子认证服务使用密码许可申请，对申请材料进行形式审查，出具受理通知书或者不予受理通知书。自 2026 年 7 月 1 日起，申请人可以向住所地省级密码管理部门提出许可申请。2026 年 7 月 1 日前已获得《电子认证服务使用密码许可证》的单位，应当对照《办法》规定的条件和要求开展电子认证服务使用密码合规性评估，对评估中发现的问题及时进行整改，并于 2026 年 9 月 30 日前向住所地省级密码管理部门报送电子认证服务使用密码合规性评估报告。（来源：国家密码管理局）

2. 国家数据局印发《关于推进行业高质量数据集建设行动的实施方案》

6 月 3 日，国家数据局印发《关于推进行业高质量数据集建设行动的实施方案》，这是国家层面首次对数据赋能人工智能发展作出的系统性部署。《方案》提出实施强基扩容行动、实施标注攻坚行动、实施提质增效行动等六项措施。

实施强基扩容行动方面，《方案》提出面向人工智能应用需求丰富行业高质量数据集建设形态。持续推进文本、代码、图像、音频、视频、点云、时序数据、科学数据等多模态高质量数据集建设，赋能人工智能预训练、指令微调、强化学习、测评等各阶段。加强知识库、知识图谱、本体

等数据集建设，加快复杂任务规划、长程推理、人机交互、决策执行等数据集建设，赋能智能体等新型智能应用形态。加快重点场景物理交互、环境感知、运动控制等真机交互数据集建设，积极应用仿真模拟与合成技术扩大数据供给，赋能具身智能发展。积极面向世界模型等前沿方向，推进数据集建设。

实施标注攻坚行动方面，《方案》提出推动数据标注转型升级。加强数据标注领域科技创新，强化自动化工具和平台的研发与应用，发展“模型预标注+人工校准”“人工标注+模型检验”“模型预标注+模型检验”等智能化标注服务，全面提升数据标注水平。发展专家型数据标注服务，建立行业专家认证机制，推动专家深度参与指令微调、强化学习等阶段所需的专业知识标注，生产领域知识、逻辑推理等高质量数据集，提高数据集的知识密度与专业价值。（来源：国家数据局）

3. 国家网信办、市场监管总局联合印发《网络测评活动规范》

6 月 8 日消息，国家网信办、市场监管总局近日联合印发《网络测评活动规范》，共十二条。

《规范》提出，“网络测评活动”是指测评主体通过开展测试、对比分析数据、引用专业检测结果或者表达使用感受等方式，对产品质量、功能、性价比等进行评价，并在互联网上以图文、视频、直播等形式发布测试过程与评价结果的行为。消费者针对特定产品发布消费体验信息，不属于本规范所称的网络测评活动。

《规范》强调，从事网络测评活动，涉及对产品功能、性能等项目测试，应当委托具有法定检验检测资质许可的检验检测机构按照相关标准以及技术规范开展测试，并明示测试依据的标准以及技术规范，按照规定保留测试样本以及测试数据、图片、视频等记录，确保测试数据、结果可以追溯。国家对测试依据的标准以及技术规范有强制性规定的，应当遵守其规定。相关测试项目已有国家标准、行业标准的，应当优先采用国家标准、行业标准。确需采用其他标准或者非标方法进行测试的，应当说明其与国家标准、行业标准的异同；采用非标方法的，还应当事先进行方法论证。对食品开展检验检测的，测试方应当具备相应的资质，不得使用非标方法，不得测评无国家标准检验方法的项目。（来源：网信中国）

4. 六部门联合印发《金融信息服务数据分类分级指南》

6 月 13 日，国家网信办、中国人民银行、国家金融监督管理总局等六部门联合印发《金融信息服务数据分类分级指南》，规定了金融信息服务数据分类分级规则，适用于在境内从事金融信息服务的金融信息服务提供者开展数据分类分级和重要数据识别工作，不适用于涉及国家秘密的数据和军事数据。

《指南》提出，金融信息服务数据可按照业务属性进行分类。一级分类分为业务数据、用户数据和企业数据三类，进一步细分为二级分类九类、三级分类六十七类。数据分类分级规则方面，《指南》明确数据分级框架、分级要素、影响对象、影响程度、综合确定级别以及级别动态更新。例如，数据分级框架方面，《指南》提出根据金融信息服务数据在经济社会发展

中的重要程度和敏感程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为四级，分别为核心数据、重要数据、敏感一般数据、常规一般数据。

数据分类分级流程方面，《指南》提出：一是数据资源梳理，包括对组织的数据资源进行全面梳理，明确数据资源基本信息、描述对象、业务属性等，形成数据资源清单；二是数据分类，包括根据数据所描述的对象，确定一级类别，根据数据所属的业务领域、数据主体等，确定二级类别；三是根据数据所涉及的行业条线、关键业务、管理和用途等，确定三级类别；四是数据分级，包括通过对分级要素进行识别分析，综合研判数据对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益的影响，对数据进行分级；五是形成数据分类分级清单，包括审核确定数据分类分级结果，形成数据分类分级清单和重要数据目录；六是报送重要数据目录，按照要求的频度和格式向主管部门报送重要数据目录；七是动态更新管理，定期复核数据资源和数据分类分级情况，及时更新数据分类分级清单和重要数据目录。当核心数据和重要数据发生重大变化（如重要数据条目数量、存储总量等变化30%以上，或其他重要内容发生变化），应当及时重新报送重要数据目录。（来源：网信中国）

5. 三部门联合发布《实施网络安全标识的产品目录（第一批）》及相关实施规则

6 月 15 日，国家互联网信息办公室、工业和信息化部、公安部联合发布《实施网络安全标识的产品目录（第一批）》及《消费类网联摄像头网络安全标识实施规则》。

第一批产品目录仅包括一类产品，即消费类网联摄像头。具体指的是适用于消费者个人或组织购买、使用，为个人或组织提供音视频信息采集和处理服务、具有互联网联网功能的独立摄像头。不适用于公共安全领域的摄像头。在网络安全能力等级方面，消费类网联摄像头的网络安全标识对应的网络安全能力由低到高依次为基础级、增强级、领先级三个级别，相应的标识等级分别用一星、二星、三星表示。网络安全能力应依据《网络安全标准实践指南——网络安全标识 消费类网联摄像头安全要求》（TC260-PG-20265A）进行检测，确定物理与硬件安全、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、安全保障等单项网络安全能力等级。满足同一等级的所有单项要求，方可获得该网络安全能力等级。（来源：网信中国）

6. 国家网信办发布《促进分布式数字身份互通互认应用规定（征求意见稿）》

6 月 18 日，国家互联网信息办公室发布《促进分布式数字身份互通互认应用规定（征求意见稿）》，旨在深入推进网络强国、数字中国战略实施，促进分布式数字身份创新发展和互通互认应用，建立健全分布式数字

身份公共服务体系，夯实网络空间可信身份认证基础，支撑国家区块链网络基础共性服务能力建设，推动国民经济和社会发展各领域数字身份跨平台互通互认。

征求意见稿共八章四十三条，包括分布式数字身份的注册与互通互认、可验证凭证的签发与验证、分布式数字身份的管理等内容。征求意见稿明确了一系列定义。其中，分布式数字身份是指基于区块链等分布式技术，支持用户自主管理身份信息的新型数字身份，由标识符、密钥、可验证凭证和可验证声明构成，可用于数字账户管理、登录认证、数据授权等场景，旨在解决跨地域、跨行业、跨平台身份互通互认问题。分布式数字身份链是指由国家网信部门授权单位运营，与权威身份认证机构、分布式数字身份应用服务机构、可验证凭证签发机构、可验证凭证应用机构等协作，通过区块链技术实现多方共识，基于国家区块链网络建设的可信分布式数字身份公共服务基础底座。

征求意见稿规定，相关主体可自愿通过身份链注册分布式数字身份，经权威身份认证机构核验后，签发分布式数字身份标识符和实名身份凭证。实名身份凭证分为境内实名身份凭证和境外实名身份凭证。其中，境内方面，实名身份凭证依照其身份类别按照以下方式自愿申请和签发：个人用户由国务院公安部门核验身份后，通过身份链签发身份凭证；机关事业单位用户向中央机构编制部门申请身份数据核验，通过身份链签发身份凭证；法人及其他组织机构用户向统一社会信用代码管理部门申请身份数据核验，通过身份链签发身份凭证；工业设备及物品由国务院工业和信息化部门依

托工业互联网标识解析体系负责注册、核验身份数据，通过身份链签发身份凭证。（来源：网信中国）

7. 三部门联合公布《网络数据安全风险评估办法》

6 月 18 日，国家互联网信息办公室、工业和信息化部、公安部联合公布《网络数据安全风险评估办法》，共二十五条，自 2026 年 8 月 20 日起施行。

《办法》指出，在国家数据安全工作协调机制指导下，国家网信部门会同国务院电信、公安等有关部门建立网络数据安全风险评估专项工作机制，指导、监督风险评估工作。有关主管部门应当按照谁管业务、谁管业务数据、谁管数据安全的原则，定期组织开展本行业、本领域风险评估，根据工作需要对本行业、本领域的重要数据处理者开展风险评估情况进行检查，并于每年 1 月底前将年度风险评估检查计划报送国家网信部门。国家网信部门通过国家数据安全工作协调机制将计划与国务院电信、公安、国家安全等有关部门共享并进行协调，避免不必要的检查和交叉重复检查。

《办法》规定，重要数据处理者应当每年度开展风险评估。重要数据安全状态发生重大变化，可能对数据安全造成不利影响的，应当及时对发生变化及其影响的部分开展风险评估。网络数据处理者可以自行或者委托第三方评估机构开展风险评估。网络数据处理者自行开展风险评估，应当指定专人负责。网络数据处理者委托评估机构开展风险评估，应当通过订立合同或者其他具有法律效力的文件等方式明确双方的权利、义务等。（来源：网信中国）

8. 中央网信办发布《政务移动互联网应用程序管理要求》强制性国家标准（征求意见稿）

6 月 26 日，中央网络安全和信息化委员会办公室发布强制性国家标准《政务移动互联网应用程序管理要求》（征求意见稿）。

该标准对政务移动互联网应用程序功能建设、备案管理、使用管理、安全保密等方面提出系统性管理要求，适用于各级行政机关、群团组织、事业单位及行政机关以外的其他国家机关开展政务移动互联网应用程序管理。标准所称政务移动互联网应用程序，是指各级行政机关、群团组织、事业单位开发建设或依托各类互联网平台搭建、运行于移动智能终端上、为内部工作人员办公、管理、学习提供支撑服务的应用软件，包括移动客户端（APP）、小程序、快应用等，不包括政务公众账号和工作群组。

在使用管理方面，标准提出多项禁止性要求：不应随意或重复要求基层填表报数交材料；不应将应用程序的登录及使用频次和时间、下载率、安装使用率等信息作为通报排名、考核评价、评比评选的依据；不应通过应用程序上传不必要的工作照片、截图、视频、轨迹等；不应简单以工作场景截图或视频代替实际工作成效评价；不应将阅读量、关注数、评论量、点赞数、转发量、网络投票数、学习时长等作为考评依据；不应将积分排名、在线时长等数据用于通报排名和考评；不应使用政务移动互联网应用程序从事经营性活动等。（来源：网信中国）

9. 国家能源局发布《能源行业数据分类分级指南（2026 年版）》

6 月 30 日，国家能源局发布《能源行业数据分类分级指南（2026 年版）》，自 2026 年 7 月 1 日起施行。《指南》共四章十五条，包括能源行业数据分类分级规则、能源行业重要数据、核心数据识别规则等。

能源行业数据分类分级规则方面，《指南》提出，能源行业数据分类维度包括但不限于能源品种、能源活动等。按能源品种，能源行业数据一级分类包括：煤炭、石油、天然气、核能、水能、风能、太阳能、生物质能、地热能、海洋能、电力、氢能等；按能源活动，能源行业数据二级分类包括：规划、设计、建设、生产、储运、消费、科研等。能源行业数据处理者可按数据内容和特点，进行三级和四级分类。

《指南》提出，根据数据重要性、精度、规模、安全风险等因素，能源行业数据分为一般、重要、核心三个等级。能源行业重要数据、核心数据经过统计、关联、挖掘或聚合等加工活动产生的衍生数据，如能恢复、还原为重要数据、核心数据，原则上按原等级管理。能源行业重要数据、核心数据经过脱敏处理后，无法恢复、还原为重要数据、核心数据的，核心数据可以降级为重要数据或一般数据，重要数据可降级为一般数据。（来源：国家能源局）

（二）地方层面动向

1. 江西省发改委等部门印发《江西省省级公共数据资源整体授权运营实施方案》《江西省交通运输领域省级公共数据资源授权运营实施方案》

6 月 3 日，江西省发展和改革委员会、江西省政务服务办印发《江西省省级公共数据资源整体授权运营实施方案》《江西省交通运输领域省级公共数据资源授权运营实施方案》，自 2026 年 7 月 4 日起施行。

《江西省省级公共数据资源整体授权运营实施方案》从实施背景、运营机构遴选、数据供给、授权运营实施、收费定价与收益分配、安全保障及组织保障等方面作出系统部署。方案明确，省大数据中心作为省级公共数据资源整体授权运营实施机构，须按照公开招标、邀请招标、谈判等公平竞争方式遴选运营机构。运营机构须具备独立法人资格、良好财务状况和信用记录、专业技术能力、数据运营能力、成熟安全保障能力及专业数据技术团队等条件。在数据供给方面，省直相关单位依法合规持有的公共数据资源应纳入省级授权运营范围。省级层面整体授权运营第一批公共数据资源目录清单共 440 项数据，主要涵盖金融、公安、人社、住建、交通、农业、文旅、林业等行业。

《江西省交通运输领域省级公共数据资源授权运营实施方案》是整体方案框架下的首个分领域实施方案。运营机构除满足整体方案基本条件外，还须具备交通运输行业项目实施经验、行业数据管理能力、行业数据运营经验及熟悉交通运输业务的专业技术队伍。在数据供给方面，交通运输领

域第一批授权运营公共数据资源目录共35项，涵盖公路服务设施、高速通行、水路运输、道路运输、交通事件、行政处罚、信用管理等业务领域。（来源：江西省发改委）

2. 陕西省两部门公布《关于加快公共数据资源开发利用的实施意见》

6月4日，陕西省委办公厅、省政府办公厅发布《关于加快公共数据资源开发利用的实施意见》，围绕扩大数据资源供给、加强授权运营监管、释放公共数据价值等五个方面提出十三项措施。

扩大数据资源供给方面，《意见》提出推进政务数据汇聚共享。认真贯彻执行《政务数据共享条例》，压实政务数据共享主体责任，明确共享工作机构，制定共享工作制度，依照部门职责全量编制政务数据目录，按需共享政务数据，持续做好“一数一源一标准”治理。省数据管理部门统筹建立全省一体化政务数据平台体系，健全政务数据异议处理和常态化供需对接机制，持续更新高频数据共享责任清单，组织全省人口、法人、自然资源和空间地理、宏观经济和电子证照等基础数据库建设。省市政务数据全量向本级已有政务数据平台汇聚，除法律、行政法规另有规定外，原则上不得通过新建政务数据共享交换系统开展跨层级、跨地域、跨系统、跨部门、跨业务的政务数据共享工作。

释放公共数据价值方面，《意见》提出加强公共数据资产管理。落实对数据资源、数据产品等各类形态数据的持有权、使用权、经营权等分置的产权运行机制，依法依规维护数据资源资产权益，有序探索将授权运营

形成的公共数据产品和服务纳入公共数据资产管理范畴。（来源：中共陕西省委办公厅、陕西省人民政府办公厅）

3. 上海市浦东新区数据局发布《浦东新区数据产业高质量发展三年行动方案（2026—2028 年）》（草案）

6 月 8 日，上海市浦东新区数据局公开征求《浦东新区数据产业高质量发展三年行动方案（2026—2028 年）》（草案）意见。草案围绕完善制度政策体系、优化空间布局、打造数字引擎等六个方面提出十八项措施。

完善制度政策体系方面，草案提出推动新区科学数据、健康医疗数据开发利用等制度突破，重点突破数据资源评估定价、数据要素收益分配等关键制度瓶颈。以数据价值创造和价值实现为导向，建立数据要素收益分配机制，为数据要素的生成、确权、开发和运营提供制度保障，营造长期稳定、可预期的数据产业法治化营商环境。

打造数字引擎方面，草案提出建设高标准检测认证基础设施，打造基于国际密码检测标准的商用密码检测服务能力。全面提升新区政务信息系统安全管理能力，强化系统安全防护与风险防控水平，构建网络数据安全防护力量。研究数字运营中心新型安全管理能力建设，完善平台安全监管能力，加强关键信息基础设施安全保障。（来源：上海市浦东新区数据局）

4. 上海市通信管理局印发《上海市电信领域数据安全事件应急预案（试行）》

6 月 17 日，上海市通信管理局印发《上海市电信领域数据安全事件应急预案（试行）》，适用于在上海市内发生的电信领域数据安全事件应急处置活动。文件自印发之日起实施。

在事件分级方面，预案根据数据安全事件对国家安全、企业网络设施和信息系统、生产运营、经济运行等造成的影响范围和危害程度，将数据安全事件分为特别重大、重大、较大和一般四个级别。工作原则是坚持统一领导、分级负责，统一指挥、密切协同、快速反应、科学处置，落实“谁管业务、谁管业务数据、谁管数据安全”的数据处理者数据安全主体责任。

在监测与预警方面，数据处理者和数据安全应急支撑机构应当按照相关规定加强电信领域数据安全风险监测、研判和上报。数据安全风险预警等级分为四级，由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般数据安全事件。在事件响应方面，数据安全事件应急响应分为四级：I 级、II 级、III 级、IV 级，分别对应发生特别重大、重大、较大、一般数据安全事件。（来源：上海通信管理局）

5. 浙江省科学技术厅、浙江省数据局发布《浙江省科学数据汇交与共享管理办法（试行）》

6 月 18 日，浙江省科学技术厅、浙江省数据局发布《浙江省科学数据汇交与共享管理办法（试行）》，自 2026 年 7 月 15 日起施行。《办法》共七章三十三条，包括职责分工、汇交与管理、共享与使用等内容。

《办法》指出，科学数据是指利用省级政府预算资金支持产生的，可用于支撑科学发现、技术创新以及人工智能大模型训练与推理等活动的数据，具体包括原始数据、衍生数据、关联数据。

《办法》强调，浙江省级政府预算资金资助形成的科学数据应当按照开放为常态、不开放为例外的原则，分级分类进行开放共享。根据数据级别制定差异化的共享策略，明确科学数据共享条件和共享对象。科学数据中心发布科学数据目录，分级分类提供数据在线检索、使用申请、下载及调用等服务。数据使用方通过科学数据中心提交使用申请，通过审核后可使用所申请的数据。（来源：浙江省科学技术厅、浙江省数据局）

6. 北京市经济和信息化局印发《北京市经济和信息化领域行政处罚裁量基准》

6 月 26 日，北京市经济和信息化局印发《北京市经济和信息化领域行政处罚裁量基准》，共十一条，自印发之日起施行。

《基准》提出，实施行政处罚应当坚持处罚与教育相结合的原则，综合考虑法律依据、违法事实等相关因素，还应当判定是否具有依法不予处罚、从轻、减轻、从重等情形，综合判断后确定行政处罚的种类和幅度，作出相应的处理决定。《基准》规定，对同一类违法主体实施的性质相同、情节相近或者相似、危害后果基本相当的违法行为，适用的法律依据、处罚种类应当基本一致，处罚幅度应当基本相同。《基准》强调，对当事人的违法行为依法不予行政处罚的，应当通过说服教育、警示告诫、指导约

谈等措施教育、引导、督促当事人依法依规开展相关活动。（来源：北京市经济和信息化局）

境内前沿观察二：治理实践

导读：6 月，各部门围绕个人信息保护、网络谣言治理、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，相关治理工作进一步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，围绕仿冒假冒网站、网络谣言、“银狐”木马病毒、网络诈骗、网络暴力、侵犯公民个人信息等违法犯罪行为持续开展执法行动。公安部网安局发布五起“银狐”木马网络犯罪典型案例，包括吉林公安网安部门侦破陈某等人制作“银狐”木马病毒案。湖南公安网安部门依法查处网暴抗洪救灾村干部的网民，云南昆明公安机关依法办理黎某某公然侮辱张桂梅校长案，广东网警侦破仿冒教育考试类官网并为他人“伪造成绩”非法牟利案。

网信部门方面，中央网信办召开全国网络生态治理工作会议，强调加强网络生态治理是服务党和国家工作大局的必然要求，是坚定不移推进网络强国建设的重要举措，是贯彻以人民为中心的发展思想的内在体现，是促进平台经济健康发展的基础保障。中央网信办部署开展“清朗·整治账号名称信息乱象”专项行动，针对名称冒充、身份伪装、夹带违规信息、名称信息黑灰产四个方面的问题开展治理。国家互联网信息办公室发布《中国个人信息保护报告（2025 年）》，是国家网信办首次就个人信息保护工

作发布综合性年度报告。广东省委网信办组织全省网信系统启动为期2个月的“清朗·优化营商网络环境整治恶意炒作涉企信息”专项行动。上海市委网信办会同多部门启动规范汽车行业网上信息传播秩序专项整治行动。上海市网信办针对上海携程商务有限公司未落实数据出境安全评估要求、违法出境个人信息等行为，依据《个人信息保护法》罚款1000万元。爱特思亚太企业管理有限公司收到上海市数据出境负面清单管理办法及配套文件落地实施后，全市首张数据出境负面清单备案结果通知书。

通信管理部门方面，工信部通信管理局针对部分APP在开屏和弹出的信息窗口中，采用违规方式诱导用户点击，或通过高灵敏度“摇一摇”等方式误导触发跳转的问题，指导督促相关互联网平台和智能终端企业，强化APP信息窗口呈现方式的规范管理，严禁违规呈现信息窗口。

其他部门和司法实践方面，最高人民检察院发布《未成年人检察工作白皮书（2025）》，2025年检察机关受理审查起诉未成年人犯罪和起诉侵害未成年人犯罪近五年首次实现“双下降”，未成年人犯罪防治工作取得阶段性成效。国家数据局发布《数字中国发展报告（2025年）》，数字中国发展指数达到170.1，较2024年增长12.99%。

关键词：个人信息保护；网络生态治理；AI应用乱象；数据出境

（一）公安机关治理实践

1. 公安部网安局公布 5 起打击仿冒假冒网站典型案例

6 月 5 日，公安部网安局公布 5 起打击仿冒假冒网站典型案例。

一是甘肃武威公安机关侦破赵某等人非法利用信息网络案。甘肃武威公安机关网安部门查明，赵某（男，26 岁）委托卢某（男，38 岁）设立仿冒学历学位认证类网站，为虚假学历证书提供在线查验服务牟利。2026 年 3 月，甘肃武威公安机关将赵某、卢某 2 人抓获，查明其设立、运营仿冒网站 18 个，制作仿冒学位证、毕业证等 2406 份。

二是河北石家庄公安机关侦破张某等人非法利用信息网络案。河北石家庄公安机关网安部门查明，张某（男，32 岁）伙同他人设立仿冒某部委人事考试网，制售虚假职业资格证书牟利。2026 年 3 月，河北石家庄公安机关将张某等 4 人抓获，查明其设立、运营仿冒网站 1 个，制作仿冒职业资格证书 256 份。

三是山西临汾公安机关侦破崔某非法利用信息网络案。山西临汾公安机关网安部门查明，崔某（男，33 岁）设立假冒民办教育网站，为虚假学历证书提供在线查验服务牟利。2026 年 3 月，山西临汾公安机关将崔某抓获，查明其设立、运营仿冒网站 1 个，制作仿冒学历证书 72 份。

四是甘肃临夏公安机关侦破袁某等人非法利用信息网络案。甘肃临夏公安机关网安部门查明，以袁某（男，45 岁）为首的犯罪团伙

设立假冒教育培训网站，制售虚假学历、学位证书牟利。2026 年 3 月，甘肃临夏公安机关将袁某等 4 人抓获，查明其制作仿冒学历证书 4125 份、伪造印章 5976 枚。

五是福建厦门公安机关侦破陈某非法利用信息网络案。福建厦门公安机关网安部门查明，陈某（男，35 岁）在明知他人实施涉税违法行为的情况下，仍为其搭建仿冒税务机关网站。2026 年 5 月，福建厦门公安机关将陈某抓获，查明其设立、运营的仿冒网站 1 个。

以上 5 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）

2. 公安部网安局公布 10 起涉高考网络谣言典型案例

6 月 8 日，公安部网安局公布 10 起涉高考网络谣言典型案例。

案例一：2026 年 6 月 7 日，广东省潮州市网民沈某宏为博取关注、吸粉引流，使用 AI 工具生成了一张“坐在 2026 年高考考场并使用手机拍摄考场”的虚假图片，并配文“带都带了，那发个抖音吧”后发布，误导大量网民，并引发关注和讨论，造成不良社会影响。目前，属地公安机关已依法对沈某宏作出行政处罚。

案例二：2026 年 6 月 7 日，河南省驻马店市网民吴某帅为博取关注、吸粉引流，使用 AI 工具生成了一张虚假的“2026 年普通高等学校招生全国统一考试语文试卷”图片，并在互联网平台发布，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对吴某帅作出行政处罚。

案例三：2026 年 6 月 4 日，湖南省郴州市网民李某怡为博取关注、吸粉引流，在互联网平台编造并发布了虚假高考答案信息及教唆高考带手机舞弊的不当内容，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对李某怡作出行政处罚。

案例四：2026 年 6 月 4 日，湖南省耒阳市网民刘某涛在互联网平台谎称自己有“高考答案”出售，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对刘某涛作出行政处罚。

案例五：2026 年 6 月 6 日，湖南省邵阳市网民钱某兰为博取关注、吸粉引流，在互联网平台编造并发布了“高考压力大，又死人了”的谣言信息，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对钱某兰作出行政处罚。

案例六：2026 年 6 月 3 日，山东省聊城市网民夏某硕为博取关注、吸粉引流，在互联网平台发布信息，谎称自己“买到 2026 年高考答案”，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对夏某硕作出行政处罚。

案例七：2026 年 6 月 5 日，山东省菏泽市网民张某为博取关注、吸粉引流，在互联网平台发布所谓“2026 年高考答案”的谣言信息，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对张某作出行政处罚。

案例八：2026 年 6 月 4 日，山东省菏泽市网民张某轩为博取关注、吸粉引流，在互联网平台发布信息，谎称自己有“2026 年高考

答案”，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对张某轩作出行政处罚。

案例九：2026 年 5 月 21 日，广西壮族自治区南宁市网民曾某津为博取关注、吸粉引流，在互联网平台发布信息，谎称自己有“2026 年高考答案”，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对曾某津作出行政处罚。

案例十：2026 年 4 月 12 日，河北省衡水市网民袁某为博取关注、吸粉引流，通过某短视频平台发布信息，谎称自己有“高考试题”，误导大量网民关注和讨论，造成不良社会影响。目前，属地公安机关已依法对袁某作出行政处罚。（来源：公安部网安局）

3. 公安部通报电信网络诈骗最新形势与特点，刷单返利发案最高，虚假投资理财损失最大

6 月 12 日，公安部召开新闻发布会，通报当前电信网络诈骗犯罪的最新形势、特点，提示防范要点。

发布会指出，2025 年以来，各地各部门综合采取侦查打击、行业治理、技术反制、宣防劝阻、国际合作等措施，依法开展打击治理工作。自 2025 年 10 月以来，全国电诈案件发案已连续 8 个月同比下降。公安机关与相关国家开展国际执法合作，先后铲除位于缅甸缅北、妙瓦底和柬埔寨的规模化赌诈园区，成功缉捕陈志、佘智江、李雄等重大跨境赌诈犯罪集团头目。当前案件仍多发高发，最高发的诈骗类型共 10 类，占全部电诈案件的 85%。其中，刷单返利诈骗发案最高，

占 25%；虚假网络投资理财诈骗损失最高，约占全部损失的 40%，损失百万、千万以上的案件大多属此类型。

据介绍，近期出现的电诈犯罪新特点和新手法主要包括以下四点：特点一，犯罪分子主要通过网络平台寻找作案目标，在社交聊天、短视频直播、电商购物等平台通过发布信息、评论互动、私信聊天、扫码入群等方式引流，占比高达 66%；特点二，犯罪分子大量使用小众通联软件对被害人进行深度洗脑，诱导被害人下载和使用用户数量少、关注度低的非主流通信软件，以规避预警发现；特点三，犯罪分子使用具有屏幕共享、呼叫转移功能的专门诈骗 App 实施远程盗刷，一旦安装即等于交出手机最高权限，可远程获取银行卡账号、密码和验证码；特点四，犯罪分子大量利用现金或黄金等贵重物品获取和转移涉诈资金，以逃避资金管控和追查拦截。（来源：公安部刑侦局）

4. 公安部网安局公布 5 起打击“银狐”木马病毒典型案例

6 月 16 日，公安部网安局发布五起“银狐”木马网络犯罪典型案例。

一是吉林公安网安部门侦破陈某等人制作“银狐”木马病毒案。吉林公安网安部门查明，以陈某为首的犯罪团伙开发“银狐”木马病毒变种，通过技术手段对抗安全检测，批量发送钓鱼邮件，窃取企业数据、搭建诈骗场景实施犯罪，涉案金额 700 余万元。目前，属地公安机关已对陈某等 27 名犯罪嫌疑人依法采取刑事强制措施。

二是浙江杭州公安网安部门侦破纪某飞等人制作并贩卖“银狐”木马病毒案。浙江杭州公安网安部门查明，以纪某飞为首的犯罪团伙制作并贩卖“银狐”木马病毒，非法控制他人计算机信息系统，盗取网络资产，涉案金额300余万元。目前，属地公安机关已对纪某飞等5名犯罪嫌疑人依法采取刑事强制措施。

三是山东公安网安部门侦破杨某等人非法控制他人计算机信息系统案。山东公安网安部门查明，以杨某为首的犯罪团伙搭建多个钓鱼网站，诱导用户下载捆绑“银狐”木马病毒的软件安装包，非法控制他人计算机信息系统，盗取网络资产，涉案金额300余万元。目前，属地公安机关已对杨某等15名犯罪嫌疑人依法采取刑事强制措施。

四是广东公安网安部门侦破李某等人非法控制他人计算机信息系统案。广东公安网安部门查明，以李某为首的犯罪团伙在网络上投放“银狐”木马病毒，非法控制他人计算机信息系统，盗取网络资产，涉案金额20余万元。目前，属地公安机关已对李某等13名犯罪嫌疑人依法采取刑事强制措施。

五是浙江嘉兴公安网安部门侦破周某等人非法控制他人计算机信息系统案。浙江嘉兴公安网安部门查明，以周某为首的犯罪团伙在正规社交软件安装包中捆绑“银狐”木马病毒，并搭建仿冒的官方下载网站，诱导大量网民下载携带“银狐”木马病毒的软件，非法控制他人计算机信息系统，盗取网络资产，涉案金额20余万元。目前，属地公安机关已对周某等3名犯罪嫌疑人依法采取刑事强制措施。

（来源：公安部网安局）

5. 公安部公布 5 起依法联合惩戒电信网络诈骗及其关联违法犯罪典型案例

6 月 18 日，公安部发布消息称，自《电信网络诈骗及其关联违法犯罪联合惩戒办法》正式施行以来，公安机关在依法开展刑事打击和行政处罚的同时，会同有关部门对 2 万余名涉电信网络诈骗及其关联违法犯罪的人员采取金融惩戒、电信网络惩戒、信用惩戒措施，切实维护了人民群众的合法权益。公安部同日公布 5 起依法联合惩戒电信网络诈骗及其关联违法犯罪的典型案例。

案例 1：出借银行卡帮助诈骗团伙转移涉诈资金。何某将本人名下的一张银行卡提供给诈骗分子接收涉诈资金 49985 元，随后帮助诈骗分子提现 49700 元并从中获利。经公安机关调查，其在明知收取到的是涉诈资金的情况下，仍帮助取现并送给犯罪团伙成员。何某因帮助信息网络犯罪活动罪被法院判处拘役四个月。同时，何某被公安机关列为惩戒对象，3 年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；在信用方面，将其纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例 2：利用微信、支付宝等帮助诈骗团伙转移涉诈资金。仇某将本人实名认证的微信账户提供给诈骗分子，转移涉诈资金 56900 元，从中获利 4000 元；高某将本人实名认证的支付宝账户提供给诈骗分

子，转移涉诈资金 135842 元，从中获利 6000 元。仇某、高某被公安机关列为惩戒对象，3 年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；在信用方面，将其纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例 3：架设手机口为诈骗分子提供通讯支持。康某伙同侯某在明知诈骗分子正在实施电诈犯罪活动的情况下，仍通过搭建“手机口”的方式为其提供通讯传输，关联全国 3 起电信网络诈骗案件，两人非法获利共计 59338 元，构成帮助信息网络犯罪活动罪被法院分别判处有期徒刑十一个月和有期徒刑九个月。同时，两人被公安机关列为惩戒对象，3 年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；在信用方面，将其纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例 4：使用互联网社交 App 为诈骗团伙引流。陈某、李某、赵某等 7 人为非法获利，将邵某拉入介绍跨境电商项目的投资理财微信群中，帮助境外诈骗分子与邵某建立联系，最终造成邵某被骗。经查，陈某等 7 人每组建一个群聊即可获利 4 至 6 元，共计获利 4 万余元。

陈某等 7 人在明知他人实施电信网络诈骗犯罪的情况下仍积极参与，因涉嫌诈骗罪已被公安机关采取刑事强制措施。同时，上述人员均被公安机关列为惩戒对象。3 年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；在信用方面，将其纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例 5：利用自己及家人支付宝账户帮助诈骗团伙实施诈骗。受电信网络诈骗团伙的指使，在 2026 年 4 月 9 日至 15 日期间，麦某怀伙同弟弟麦某一起使用两人名下的支付宝账户，并借用其父亲和妹妹的支付宝账户，在刷单返利骗局中给予被害人小额返利进而帮助诈骗分子实施犯罪，每天接单 400 起左右，共计获利 1400 元人民币。麦某怀因向电信网络诈骗活动提供帮助被处以行政拘留 5 日、罚款 1000 元的行政处罚，并被公安机关列为惩戒对象，2 年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能。（来源：公安部）

6. 国家网络与信息安全信息通报中心：防范假冒公安机关恶意应用程序攻击

6 月 18 日，据国家网络与信息安全信息通报中心通报，监测发现，近日一款伪装成中国公安机关对外提供服务的“公安一网通办”恶意 APP 在互联网上传播，下载地址为 110GongAn.com，IP 地址为 207.56.30.188。

通报指出，该 APP 安装包内置木马程序，通过社会工程学手段诱导用户下载，实现支付信息窃取和远程控制等恶意行为。用户一旦通过移动终端下载安装该 APP，攻击者可控制用户终端设备、获取对应访问权限，实施窃密等攻击行为。

通报建议广大用户做好以下安全防范：一是认准正规下载渠道。仅通过公安部“互联网+政府服务”平台、手机官方应用商店等正规发布渠道获取应用，切勿通过陌生短信链接、微信群转发链接、非正规二维码、小众网盘等途径下载安装自称政务服务类应用；二是严格审核应用真伪。下载应用前核对应用名称、图标、开发者主体信息（“公安一网通办”APP 开发者为公安部信息通信中心）。对名称相近、图标粗糙、主体不明的应用，一律不予安装；三是审慎开放手机权限。安装移动应用时，仅授予业务应用所需必要权限，不在来源不明的应用内填写身份证、银行卡、支付密码、短信验证码等敏感信息，避免个人隐私信息泄露；四是及时处置异常情况。如不慎安装虚假政务应用，请立即卸载并开展设备安全查杀；若已发生信息泄露或资金异常，

第一时间修改账户密码、冻结支付渠道，并向公安机关报案。（来源：国家网络与信息安全信息通报中心）

7. 国家网络与信息安全信息通报中心通报违法违规收集使用个人信息的移动应用

6 月，国家网络与信息安全信息通报中心发布消息，通报国家计算机病毒应急处理中心、公安部计算机信息系统安全产品质量监督检验中心发现的多款违法违规收集使用个人信息移动应用。

2026 年 4 月 16 日至 2026 年 5 月 20 日期间，国家计算机病毒应急处理中心检测发现 71 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。

2026 年 5 月 6 日至 2026 年 5 月 27 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 40 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处理不满十四周岁未成年人个人信息；未制定专门的个人信息处理规则，未取得未成年人父母或其他监护人的同意；未经用户同意收集使用个人信息等。（来源：公安部网安局）

8. 网警依法查处网暴抗洪救灾村干部的网民

6月2日消息，公安网安部门近日依法查处网暴抗洪救灾村干部的网民。湖南省石门县遭遇强降雨，一村干部连续多日坚守抗洪救灾一线，上门叫应、通知转移、安置群众、运送物资等，令无数网友动容。然而，有极个别网民因其接受采访时的配饰，而对其进行无端指责，揣测“耳环有二两重”，并发布“普通农村妇女可戴不起金耳环”“把耳环捐了更感动”等贬低嘲讽类言论，干扰抗洪救灾工作，影响恶劣。对此，公安网安部门迅速行动，依法查处网暴行为15起，对秦某某（男，44岁）、未某某（男，45岁）等依法行政处罚。（来源：公安部网安局）

9. 广东网警侦破仿冒教育考试类官网并为他人“伪造成绩”非法牟利案

6月6日，广东公安网安部门近日在工作中发现，网上有多条涉仿冒教育考试类官网“假查分、伪造成绩”帖文，引发网民关注和讨论。经查，违法行为人罗某于2026年1月开始，仿照“中国教育考试网”等教育考试相关官方站点，搭建虚假教育考试网站，并通过社交平台进行非法引流，以提供“定制版成绩查询页面”“定制版成绩查询截图”等虚假成绩为名，收取费用、非法牟利，其行为严重扰乱招生考试秩序。目前，属地公安机关已对罗某依法采取刑事强制措施，相关虚假网站、引流账号均被关停清理。（来源：公安部网安局）

10. 浙江网警发布六起侵犯公民个人信息违法犯罪案件

6 月 11 日，浙江宁波公安网安部门发布 6 起侵犯公民个人信息违法犯罪案。

案例一：陈某等人侵犯公民个人信息案。2025 年 10 月，宁波海曙区公安机关在工作中发现，辖区工业园区内有人以借兼职的名义，诱骗兼职人员下载注册各类 APP 软件网络账号并完成实名认证。经查，陈某等人在宁波某创业园区设立“充场工作室”，组织中介姜某等人以招聘日结兼职的名义，诱骗兼职人员完成各类社交网络账号和虚拟号的实名认证，后高价转售给李某等上游号商以非法牟利。2025 年 11 月至 2026 年 4 月，海曙公安在全国多地抓获陈某等犯罪嫌疑人 14 名。目前，以上人员均已被采取刑事强制措施。

案例二：张某等人侵犯公民个人信息案。宁波慈溪市公安机关工作发现，2025 年 4 月至 8 月，犯罪嫌疑人张某伙同赵某等人，以高薪招聘吸引日结兼职人员入职私人工作室，并以兼职登记为由让日结兼职人员提供身份证、人脸等信息配合工作，在对方不知情的情况下开通实名手机号、虚拟号，并实名注册多个社交 APP 账号，同时设置统一密码后出售给上家用于电信网络诈骗、刷单炒信等黑灰业务，该团伙非法牟取利益合计 30 余万元，出售手机号、APP 账号合计 2 万余个。犯罪嫌疑人张某等人已于 2025 年 12 月被判处有期徒刑 3 年 2 个月至 1 年 2 个月不等。

案例三：王某等人侵犯公民个人信息案。2025 年 1 月，宁波余姚市公安机关在工作中发现，辖区某电商科技公司因未做好数据安全

保护工作，导致后台客户身份数据被泄露，并被中间商转卖至贷款引流、催收等环节。同年1月至7月，余姚公安在内蒙古通辽、江苏泰州、山东泰安等地抓获犯罪嫌疑人12名。经查，王某等人在内蒙古通辽某创业园区设立“信息工作室”，利用黑客技术手段爬取宁波余姚等地电商平台数据，后高价转售给李某、刘某等下游号商以非法牟利。2025年8月，以上人员分别被判处有期徒刑1年2个月至3年2个月，并处罚金2万至16万元不等。同时该电商公司被依法处以行政处罚。

案例四：葛某等人侵犯公民个人信息罪案。2026年4月16日，宁波宁海县公安机关在工作中发现，辖区内有人收售商品房业主信息。经查，2025年以来，宁海某装饰公司业务经理葛某（男，33岁，浙江宁海人）从宁海某房地产企业公共账号非法获取多个在售商品房小区业主信息后，并出售给行业相关人员。对此，宁海网安组织警力开展多次集中收网，抓获葛某等犯罪嫌疑人17名，查获公民个人信息2.9万余条。目前，以上人员均已被采取刑事强制措施。

案例五：杨某等人侵犯公民个人信息案。2026年1月，宁波奉化区公安机关在工作中发现，辖区内有一团伙利用工作之便，非法获取、出售辖区各个楼盘小区业主个人信息。2026年1月至3月，奉化公安抓获杨某等犯罪嫌疑人20名。经查，杨某等人为宁波装潢公司员工，长期利用工作之便，收集各个楼盘小区业主信息，并通过线下上门售卖的方式将数据出售给装修、家居等相关行业公司以非法牟利。目前，以上人员均已被采取刑事强制措施。

案例六：任某等人侵犯公民个人信息案。2025 年 11 月，宁波北仑区公安机关在侦查一起诈骗案件过程中发现，宁波一信息科技公司非法获取公民个人信息用于推广业务。经查，任某、刘某、荆某合伙经营该信息科技有限公司，任某等人向他人购买个人信息几十万条，派发给员工进行电话营销。当月，北仑公安成功抓获公司股东任某、刘某等犯罪嫌疑人 15 名，现场查获手机 41 部、电脑 6 台，查获非法获取的个人信息 40 余万条。目前，以上人员均已被采取刑事强制措施。（来源：公安部网安局）

11. 福建、湖南网警办理多起涉停车管理系统管理单位未履行个人信息保护义务案

6 月 12 日消息，福建泉州公安网安部门近日办理了一起某单位停车管理系统未履行个人信息保护义务案。涉事单位作为个人信息处理者，既未制定内部管理制度和操作规程，也未采取相应的加密、去标识化等安全技术措施，致使系统中的个人信息存在被非法窃取、泄露的安全风险，侵害了公民在网络空间的合法权益。属地公安机关依照《个人信息保护法》对该单位依法予以行政处罚。

湖南郴州公安机关近期也对辖区内不履行个人信息保护义务的停车场管理系统运营单位进行依法查处。2026 年 5 月，郴州市公安局北湖分局网安大队对辖区内某停车管理公司开展网络安全检查发现，该公司开发使用的停车系统，管理了郴州近 200 个停车场的车辆用户数据，但该公司未制定个人信息内部管理制度和操作规程，对用

户数据未采取相应的加密、去标识化等安全技术措施，公司多名员工系统账号均能随意导出用户数据。郴州市公安局北湖分局对该公司不履行个人信息保护义务的情形依法处以行政处罚、责令限期改正。（来源：公安部网安局、湖南网警）

12. 四川峨眉山破获倒卖学生信息案，封存信息 90 余万条

6 月 12 日消息，四川峨眉山公安局近日成功破获一起横跨全省 17 个市州的特大侵犯公民个人信息案，并联动德阳、眉山、成都等多地警方，全链条摧毁“学院高层—校内管理员—中间商—校外招生团队”的四级黑色产业网络，抓获涉案人员 5 名，封存涉案学生公民信息 90 余万条。

2026 年 4 月，峨眉山市公安局接到群众举报，辖区校外招生团队涉嫌非法持有学生信息、开展违规招生扰民活动。民警快速出击，突击清查涉案办公点位，现场查获纸质学生信息资料 300 余份。

经审讯查明，该招生团伙全部数据均从德阳某校工作人员处非法获得。随后，四川省公安厅迅速组建跨市专案工作组，统筹调度德阳、眉山、成都警方，全线开展溯源打击，成功抓获涉案中间商黄某某，查实黄某某的上线为德阳某校招生办主任吴某某，完整固定犯罪嫌疑人吴某某的作案证据，形成闭环证据链。省、市、县三级公安机关同步配合，成功斩断一条由高校管理层人员外泄数据、校内人员中转分享、校外招生团队落地牟利的完整涉学生信息黑色产业链。

目前，该案3名主要犯罪嫌疑人已依法批准逮捕，2名涉案人员被刑事拘留，案件后续深挖扩线、溯源治理工作正在有序开展中。（来源：新华社）

13. 在网上公然侮辱张桂梅校长，黎某某被行拘

6月26日消息，云南昆明公安机关近日依法查处一起在互联网平台发布违法言论的案件。

经查，违法行为人黎某某在其个人微博账号连续发布大量不当言论，公然侮辱张桂梅校长，恶意挑起地域歧视并制造男女对立情绪。相关不实及有害信息阅读量共计1989次，造成了恶劣的社会影响。接报后，公安机关第一时间组织警力对涉案账号内容进行固定取证，迅速锁定账号持有人黎某某身份，并将其抓获归案。依据《治安管理处罚法》相关规定，公安机关依法对其作出行政拘留10日的处罚。（来源：云南网警）

14. 因未履行网络安全保护义务，湖南长沙网警对一运维单位处以罚款

6月26日消息，湖南长沙公安网安部门近日对辖区内不履行网络安全保护义务的信息技术服务单位及个人依法进行查处。

某通信设备股份有限公司工作人员在对客户单位话务系统运维期间，违规操作停用了话务系统IP访问识别防护机制，导致犯罪分子利用上述漏洞侵入系统实施违法犯罪活动，造成了严重危害。长沙

市公安局天心分局依照《网络安全法》对该公司不履行网络安全保护义务的情形处以罚款6万元,对直接责任的主管人员处以罚款1万元。（来源：湖南网警）

15. 湖南衡山网警侦破一起利用 AI 伪造证据诈骗案，累犯恶意索赔获刑一年

6 月 27 日，湖南衡山县公安局近日成功侦破县首例利用 AI 技术实施电商恶意诈骗案。

犯罪嫌疑人谭某钻平台网络规则漏洞，通过批量操作账号、伪造售后问题等方式，多次恶意申请生鲜商品全额退款，同时转卖货品非法获利，累计涉案 1.6 万余元。其个人恶意索赔行为，直接导致衡山县被多家电商平台列为高风险区域，生鲜商品受限发货，全县群众正常网购权益受到普遍影响，社会危害突出。多家电商平台整理固定电子证据，向衡山县公安机关报案。

衡山县公安局网安大队依托电子数据勘验、IP 轨迹追踪、数据交叉比对进行线索排查，店门派出所同步开展线下走访摸排，精准锁定嫌疑人身份。2026 年 1 月 26 日，民警抓获谭某，现场查获作案手机、涉案生鲜若干，在其住所查获 75 部涉案手机，完整提取 AI 造假、资金流转记录，形成完整证据链条。经审讯，谭某对全部犯罪事实供认不讳。

衡山县人民法院审理认为，谭某系多次犯罪的累犯，主观恶性大、社会影响恶劣。最终，人民法院以诈骗罪依法对其从重判处有期徒刑一年，并处罚金，违法所得全部追缴。（来源：湖南网警）

16. 广西玉林、浙江绍兴网警侦破两起涉世界杯网络赌博推广引流案

6 月，广西玉林、浙江绍兴网警侦破两起涉世界杯网络赌博推广引流案。

广西玉林公安网安部门工作中发现，2026 年 5 月以来，多个互联网社交平台出现大量图文、视频形式的涉赌推广引流广告，诱导网民进入赌博网站参赌。经查，犯罪嫌疑人陈某某纠集陈某、刘某某等人设立工作室，专门为赌博网站提供引流推广和运维保障，牟取非法利益，该行为严重扰乱网络空间秩序。目前，陈某某等人已被属地公安机关依法刑事拘留，案件正在进一步侦办中。

浙江绍兴公安网安部门近日也侦破一起涉世界杯网络赌博推广引流和赌资结算的案件，成功抓获涉案人 6 名（刑事拘留 2 名），查获涉案手机 19 台，涉案电脑 3 台。经查，涉案人陶某某、胡某等人，为牟取非法利益，为某赌球平台进行推广引流服务，同时，开设大批支付账号，使用第三方支付平台提供赌资结算服务，非法获利 10 万余元。目前，主要犯罪嫌疑人陶某某、胡某已被属地公安机关依法刑事拘留，案件正在进一步侦办中。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办召开全国网络生态治理工作会议

6 月 10 日，中央网信办召开全国网络生态治理工作会议。会议强调，加强网络生态治理，是服务党和国家工作大局的必然要求，是坚定不移推进网络强国建设的重要举措，是贯彻以人民为中心的发展思想的内在体现，是促进平台经济健康发展的基础保障，要提高政治站位、深化思想认识，进一步增强做好网络生态治理工作的责任感使命感紧迫感。要明确目标任务、聚焦工作重点，持续提升网络生态治理能力水平。在强化标本兼治上下功夫，提升专项行动质效，完善长效治理机制，抓好制度措施落实。在强化基础管理上下功夫，把好互联网入口关，把好重要流量入口关，把好新业态新应用入口关。在强化平台履责上下功夫，加强平台规则治理，提升账号管理效能，强化平台运营管理，规范和管理未成年人使用网络。在强化技术赋能上下功夫，兴利除弊发展新兴技术，与时俱进丰富技术手段，前瞻布局推动技术向善。（来源：网信中国）

2. 中央网信办、上海网信办通报多款 App 个人信息收集使用问题

6 月 11 日消息，中央网信办近日组织对 App（含小程序）收集使用个人信息行为进行检测，通报 30 款 App 个人信息收集使用问题：一是锐新教育、趣学车等 7 款 App 未公开个人信息收集使用规则；

二是蓝猫云商、大象优品等 4 款 App 频繁索要非必要权限；三是中旅旅行、东融等 5 款 App 未完整准确列明 SDK 收集使用个人信息情况；四是匠者、句苗岛等 14 款 App 未提供有效账号注销功能。相关 App 运营者应当于本通报发布之日起的 15 个工作日内完成整改，并将整改情况报中央网信办。中央网信办将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。

6 月 25 日，上海市网信办通报 2026 年第三批八款交通出行 App 个人信息收集使用问题，包括享道出行、随申行、Metro 大都会等。相关运营者应当于本通报发布之日起的 15 个工作日内完成整改，并将整改情况报上海市网信办。上海市网信办将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。上期通报的上海市网信办关于属地 App 个人信息收集使用问题的通报（2026 年第二批—消费零售专项），经复测，相关运营者均已完成问题整改。（来源：网信中国、网信上海）

3. 国家互联网信息办公室发布《中国个人信息保护报告（2025 年）》

6 月 12 日，国家互联网信息办公室发布《中国个人信息保护报告（2025 年）》，这是国家网信办首次就个人信息保护工作发布综合性年度报告。《报告》分为正文和附录两大部分。正文共有七个部分，开篇系统概述 2025 年我国个人信息保护取得的积极进展，主体部分围绕加强顶层设计、强化监管治理、推动社会共治、深化宣传教

育、对外交流合作等全面总结工作成效，最后对2026年工作进行展望。附录部分对个人信息保护法律法规规章、国家标准、典型司法案例等作了集纳。

在制度完善方面，《报告》指出，2025年我国持续健全以《个人信息保护法》为核心的法规体系，相继生效实施《网络数据安全管理条例》，并出台《个人信息保护合规审计管理办法》等重要规范性文件，进一步夯实了依法治理的制度基础。同时，相关部门不断加强监管执法力度，全年累计通报违规移动应用程序（App）和软件开发工具包（SDK）共计1100余款，排查超过8万个使用人脸识别技术的场所和14万余个线下消费场景，发现并处置违法违规问题8300余个，有效震慑了各类侵害个人信息权益的行为。

2026年是“十五五”规划开局之年，也是我国个人信息保护向纵深推进、迈向新台阶的关键之年。《报告》提出将坚持系统思维、问题导向、依法治理、多元共治、以人为本、合作共赢。具体来说，将健全个人信息保护体制机制，强化各地区、各部门协同联动，建设完善政府监管、企业履责、行业自律、公众监督的个人信息保护综合治理格局；加快制定大型个人信息处理者、小型个人信息处理者个人信息保护相关规章，持续完善个人信息保护法规体系；深入开展个人信息保护系列专项行动，强化执法监管，加强司法保护，加大个人信息违法犯罪打击力度；持续推广个人信息保护认证、合规审计等服务，加快推动国家网络身份认证公共服务在政务、教育、文旅等场景下的部署应用。（来源：网信中国）

4. 中央网信办部署开展“清朗·整治账号名称信息乱象”专项行动

6月13日，中央网信办秘书局印发通知，按照2026年“清朗”系列专项行动总体安排，开展为期3个月的“清朗·整治账号名称信息乱象”专项行动。专项行动重点整治4类突出问题：

一、名称冒充问题。一是假冒仿冒官方机构账号。在账号名称、简介中嵌入党政军机关等官方机构信息，使用相同或相似名称、标识，恶意误导公众。使用、关联县级以上行政区划地名，使用“某某政事”等组合表述，易被误认为官方账号，使公众产生错误认知。使用“某某办事大厅”“某某服务中心”等官方服务通道表述，假冒本地官方生活服务账号。二是假冒仿冒媒体账号。在名称、简介中嵌入新闻单位信息，或使用“新闻”“报道”“发布”等具有新闻媒体属性表述，营造权威信息假象。三是假冒仿冒名人账号。直接冒用名人姓名，或未经授权大量发布名人相关内容，使用相关联的名称、头像、声音、形象等元素，伪装成名人账号或名人的矩阵账号。

二、身份伪装问题。一是未经认证加注头衔。从事证券期货、教育、医疗卫生、司法等专业领域信息内容生产账号，未进行资质认证，在名称、简介中添加“知名经济学家”“首席规划师”“资深法律顾问”“专业健康导师”等专业身份词汇，仿造权威专业形象，违规发布专业领域信息内容。二是伪装特定职业人员。在头像、简介、主页背景中展示穿着军服、警服、医用工作服等职业形象，虚构个人经历，假冒仿冒特定职业人员。三是蹭炒热点事件。冒充热点事件当事人或

其亲友、相关人员等，发布所谓“内情”“细节”信息，借机恶意博取流量或获取粉丝关注。四是“影子账号”骗捐。抄袭病患本人或家属账号信息，批量复制搬运患者治病视频，假借患者或家属名义，骗取爱心捐款。

三、夹带违规信息问题。一是夹带违规外链。在头像、名称、简介中，嵌入违规外链，如二维码、网址、手机号等，引流跳转至色情、赌博、山寨等违法违规网站。二是暗含不良信息。在头像、名称、简介中，发布色情、赌博、迷信等暗示性信息内容，使用谐音、隐晦词、表情符号等方式恶意调侃或侮辱谩骂他人。三是账号违规复出。被处置的账号主体违规注册复出，并在名称、简介等环节中暗示、关联与原账号关系，恶意吸粉引流。

四、名称信息黑灰产问题。一是伪造虚假数据。通过刷量软件、群控系统、黑灰产渠道伪造粉丝数、点赞数等，营造虚假人气。二是虚假“大Ⅴ”问题。售卖“认证”“加Ⅴ”类商品，利用虚假材料申请平台认证“加Ⅴ”或获取“大Ⅴ”身份，欺骗公众。三是“僵尸”账号问题。篡改“僵尸”账号名称、简介、头像等，发布违规信息或冒充他人。（来源：网信中国）

5. 广东网信部门开展整治恶意炒作涉企信息专项行动

6月5日消息，广东省委网信办近日根据中央网信办统一部署，组织全省网信系统启动为期2个月的“清朗·优化营商网络环境整治

恶意炒作涉企信息”专项行动，集中整治恶意炒作涉企侵权信息乱象，积极护航企业健康发展。

专项行动聚焦恶意炒作涉企信息、诋毁抹黑企业、牟取非法利益、侵犯企业家个人权益等 4 类 15 项问题，从严从快清理处置涉企侵权信息、账号，督促网站平台扎实履行主体责任，健全涉企信息内容管理机制，加大涉企侵权信息处置力度，进一步优化营商网络环境。（来源：网信广东）

6. 广东网信部门严厉打击网络暴力，公布一批典型案例

6 月 9 日消息，广东省委网信办近日组织全省网信系统深入整治网络暴力问题，督促网站平台依法依约处置违法违规信息和账号，严厉打击网络暴力行为。

广东省委网信办同步通报部分典型案例。一是“默*”等账号煽动人身攻击。“默*”“雨**”等账号多次发布不实短视频及评论信息，对某明星及粉丝群体打负面标签，进行污名化攻击。相关平台已依法依约对上述账号采取禁言、关闭、暂停营利权限等处置措施；二是“乐**娱”等账号编造谣言信息。“乐**娱”“**谈娱”“**队长”“星***”等账号捏造传播涉某运动员谣言，侵犯他人网络合法权益，无底线博取流量。相关平台已依法依约对上述账号采取禁言、关闭等处置措施；三是“郑**”等账号挑动拉踩互撕。“郑**”“冲*”“二***球”等账号挑动不同明星、运动员粉丝群体互撕谩骂，鼓动“捧

一踩一”。相关平台已依法依约对上述账号采取禁言、关闭等处置措施。（来源：网信广东）

7. 江西南昌县区网信、公安联合处置两起网站被植入后门网络安全事件

6 月 10 日消息，接上级部门转办网络安全通报线索，反映南昌属地两家网站被植入后门程序，存在高危网络安全风险，南昌市网信办近日指导相关县区网信部门联合公安机关开展核查处置，督促相关单位落实主体责任、限期整改到位。

案例一：某医院官网被植入恶意后门文件。根据上级部门通报线索，青云谱辖区某医院官方网站存在被植入恶意后门文件的安全问题。接通报后，青云谱区网信办联合区网安大队，对辖区某医院开展网络安全专项核查。经查，该单位在官方网站日常运维管理过程中，未严格落实网络安全主体责任，存在安全风险意识淡薄、日常运维管理制度不健全、安全防护措施落实不到位等突出问题。因长期存在管理漏洞、防护短板，该医院官网被不法分子成功植入后门程序，导致网站系统管理员权限被非法窃取，网站控制权面临失控风险。上述行为违反《网络安全法》中关于履行网络安全保护义务的相关规定。针对隐患问题，联合工作组依法对涉事医院相关负责人进行约谈警示，现场下达《网络安全整改提示函》，明确整改要求、时限，责令其全面排查系统漏洞、彻底清除安全隐患、健全长效运维机制。目前，该医院已完成全部整改工作。

案例二：某公司网站被植入恶意后门文件。根据上级部门通报线索，青山湖辖区某公司官方网站存在被植入恶意后门文件的安全问题。接通报后，区网信办第一时间联动区网安大队开展专项核查与应急处置工作。经查，该公司网站静态上传目录遭非法植入恶意后门程序，该程序可实现远程命令执行、窃取服务器核心权限等高危操作。若被不法分子利用，极易造成用户信息数据泄露、服务器被非法操控、网站正常业务瘫痪等严重后果，存在高危网络安全风险。针对此次安全隐患问题，区网信办联合区公安分局依法对该网站负责人进行约谈警示，现场下达《网络安全整改提示函》，责令其全方位排查网站系统安全漏洞，彻底清理各类恶意程序、根除安全隐患，同时健全网站日常运维、安全巡检、风险防控长效管理机制。目前，该公司已严格按照整改要求完成全部整改工作。（来源：网信南昌）

8. 上海市网信办依法严肃查处携程违法出境个人信息问题

6 月 13 日消息，在国家网信办指导下，上海市网信办近日针对属地部分企业网络数据安全主体责任履行不到位、安全管理防护措施缺失、后端处理数据合规能力不足、数据出境合规审计不严等问题办理了一批执法案件。

其中，针对上海携程商务有限公司未落实数据出境安全评估要求、违法出境个人信息等行为，依据《个人信息保护法》，予以罚款 1000 万元的行政处罚，并责令企业限期改正。企业受处罚后积极配合，全面落实有关整改要求。（来源：网信上海）

9. 广东网信部门开展整治账号名称信息乱象专项行动

6 月 23 日消息，为进一步规范互联网用户账号名称信息注册、使用和变更等行为，集中整治账号名称信息问题乱象，广东省委网信办近日根据中央网信办统一部署，组织全省网信系统启动为期 3 个月的“清朗·整治账号名称信息乱象”专项行动。

专项行动重点整治账号名称信息存在的 4 类突出问题：一是假冒仿冒官方机构账号、媒体账号、名人账号等名称冒充问题；二是未经认证加注头衔、伪装特定职业人员、蹭炒热点事件、“影子账号”骗捐等身份伪装问题；三是嵌入违规外链、暗含不良信息、账号违规复出等夹带违规信息问题；四是伪造虚假数据、虚假“大 V”、“僵尸”账号等名称信息黑灰产问题。（来源：网信广东）

10. 上海启动规范汽车行业网上信息传播秩序专项整治行动

6 月 26 日，结合 2026 年“清朗·优化营商网络环境整治恶意炒作涉企信息”专项行动要求，上海市委网信办近日会同市经信委、市公安局网安总队等部门，启动规范汽车行业网上信息传播秩序专项整治行动。

专项行动重点整治网上汽车交易不实信息、汽车价格虚假信息，以及恶意唱衰车市、煽动非理性维权等违法违规内容，严防“自媒体”和 MCN 机构借助网络编造虚假车价，误导消费者预期，扰乱汽车市场正常秩序。各部门将坚持线上线下一体治理，通过开展专项整治，督促车企加强行业自律，主动抵制低俗、虚假、夸大宣传等不良网络

营销行为;压实平台主体责任,健全完善汽车领域内容审核发布规则,为汽车行业健康发展营造客观理性、清朗有序的网络环境。

2026 年以来，上海市委网信办持续紧盯汽车领域虚假宣传、恶意炒作等网络突出问题，指导小红书、哔哩哔哩、虎扑等属地重点平台深入开展自查自纠,集中清理涉汽车领域违法和不良信息 10273 条,处置违规汽车类“自媒体”账号 123 个，持续整治虚假车价、恶意炒作、违规引流、教唆恶意投诉等问题。（来源：网信上海）

11. 上海市首个数据出境负面清单备案落地

6 月 26 日，爱特思亚太企业管理有限公司在静安区数据跨境服务中心指导下，通过上海市网信办、上海市数据局数据出境负面清单备案审核,收到上海市数据出境负面清单管理办法及配套文件落地实施后，全市首张数据出境负面清单备案结果通知书。

据介绍，爱特思亚太在日常运营中涉及大量跨国订单处理、客户沟通及供应链协同等数据交互需求,其会员信息出境原本需要申报数据出境安全评估。但根据负面清单新规要求，仅需完成个人信息出境标准合同备案即可，合规门槛明显降低。（来源：网信上海）

12. 上海启动 2026 年未成年人网络环境整治专项行动

6 月 29 日消息，为切实加强未成年人网络保护，营造更加健康安全的网络环境，按照中央网信办 2026 年“清朗”系列专项行动统一部署和市委网信办“清朗浦江”五大重点专项行动安排，7 月 1 日

起至 10 月 31 日，上海市委网信办联合市教卫工作党委、市教委、市“扫黄打非”办、市检察院、市高院、团市委、市公安局网安总队、市文旅局执法总队等市未成年人网络保护专项机制成员单位开展“清朗守护·为你而来”2026 年未成年人网络环境整治专项行动。

专项行动重点部署五大任务：一是政策落地精准化，锚定新规细化全链条治理标准。紧扣《可能影响未成年人身心健康的网络信息分类办法》，开展靶向治理，聚焦平台发布、互动、交易三大核心环节，加大对不良行为、不良价值导向、不当使用未成年人形象以及侵犯未成年人隐私等信息的治理力度；二是 AI+算法双维度管控，新技术筑牢未成年人防护屏障。推动更多 AI 大模型平台建立健全未成年人保护模式，优化时长管控、内容过滤、家长监护功能，丰富正向科普、文化专属内容资源池；严格规范文娱内容算法分发逻辑，要求 AI 生成涉未成年人内容添加标识；三是重点平台全覆盖监管，社交、短视频、电商平台分类施策。整治刻意诱导未成年人盲目追星、集资打榜、拉踩互撕、群体网暴、极端应援等饭圈乱象；整治炒作儿童 CP、打造“网红儿童”博取流量牟利行为；整治绕过网络游戏防沉迷系统售卖游戏账号；四是紧盯新型隐蔽风险，破解未成年人网络治理新难题。严查依托动漫、同人二创、卡牌周边包装美化不良亚文化、鼓吹扭曲价值观内容；联合打击以“谷子”周边、定制图片、学习搭子等名义诱导未成年人大额消费、网络借贷、私下交易等涉诈问题；五是创新 IP 融合线下宣传，打造多场景沉浸式清朗阵地。持续完善未成年人网络素养课程，发挥小红书、哔哩哔哩、米哈游、七猫、稀宇等“未成

年人网络素养提升实践平台”作用，创新开展未成年人 AI 数字素养科普，打造书展、校园、高铁站等多场景线下清朗主题宣传阵地。（来源：网信上海）

（三）通信管理部门治理实践

1. 工信部指导规范 APP 信息窗口跳转行为

6 月 9 日消息，针对部分 APP 在开屏和弹出的信息窗口中，采用违规方式诱导用户点击，或通过高灵敏度“摇一摇”等方式误导触发跳转的问题，工业和信息化部信息通信管理局近日组织召开专题会议，指导督促相关互联网平台和智能终端企业，强化 APP 信息窗口呈现方式的规范管理，严禁违规呈现信息窗口。

会议通报在日常巡查中发现的相关问题线索，要求各相关企业立即开展自查整改，对已上线或即将上线的各类信息窗口样式进行全面审核。建立完善在线巡查机制，及时下线违规信息窗口样式。坚持严守合规边界，完善内部审核和合规管理机制，规范服务行为，优化用户体验，有效杜绝违规行为的发生，切实保护用户合法权益。（来源：工信微报）

2. 上海、北京、浙江等省市通信管理局发布侵害用户权益的 APP（SDK）

（1）北京市

6 月 1 日，北京市通信管理局通报 2026 年第六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。截至目前，尚有 6 款移动互联网应用程序未整改或整改不到位。

5 月 6 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。截至目前，仍有 4 款移动互联网应用程序未整改或整改不到位。

（2）安徽省

6 月 1 日，安徽省通信管理局通报 2026 年第 3 批侵害用户权益 APP。安徽省通信管理局近日对省内 APP 进行拨测检查，发现 27 款 APP 存在违法违规收集使用个人信息的问题。4 月 13 日，安徽省通信管理局对上述违规 APP 企业下达责令改正通知书，要求限期完成整改工作。截至通报，尚有 14 款 APP 未完成问题整改，相关 APP 企业应在 2026 年 6 月 5 日前落实整改要求。逾期不整改的，安徽省通信管理局将依法依规组织开展相关处置工作。

（3）广东省

6 月 3 日，广东省通信管理局公开通报 5 款未按要求完成整改 APP。广东省通信管理局持续开展移动应用程序专项治理工作，发出《APP 整改通知书》责令 APP 运营者限期整改，并通知相关应用商店协助督促 APP 运营者整改。截至通报，有 5 款 APP 未完成整改。

被通报的APP主办者应在6月9日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施，切实维护APP用户合法权益和网络安全秩序。

（4）山东省

6月16日，山东省通信管理局通报2026年第1批不合格APP整改情况。

截至6月16日，有12款存在问题并被山东省通信管理局通知限期整改的APP未按要求在限期内完成整改反馈。6月24日前，上述12款APP开发运营者务必完成整改与情况反馈工作。如再次逾期仍未整改到位，山东省通信管理局将视情采取下架等措施。

截至6月16日，有1款存在问题的APP经书面要求整改、通报再次要求整改后，仍未在规定时限内完成整改反馈，现予以下架。相关应用商店应立即对有关APP进行下架处理，并举一反三，排查反复出现问题的APP开发运营者，严格落实分发平台主体责任，把好上架审核关。山东省通信管理局将对下架情况进行持续跟踪。

（5）浙江省

6月23日，浙江省通信管理局通报2026年第5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住建、教育等领域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8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7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。

（6）上海市

6 月 24 日，上海市通信管理局通报下架 46 款侵害用户权益行为 APP（SDK）。2026 年 6 月，上海市通信管理局向社会公示一批存在侵害用户权益行为的 APP（SDK）。在规定的整改期限内，经核查复检，尚有 46 款 APP（SDK）未按照要求落实整改。上海市通信管理局将对上述 APP（SDK）持续跟踪，视情况进一步采取停止接入、行政处罚、纳入电信业务经营不良名单等处理措施。

6 月 29 日消息，上海市通信管理局近日组织第三方检测机构对上海市 APP（SDK）进行抽查，共发现 76 款 APP（SDK）存在侵害用户权益行为。上述 APP（SDK）应对存在的问题立即整改，并对该 APP（SDK）个人信息和用户权益保护工作开展全面自评估，自通报之日起 5 个工作日内将书面整改报告和自评估报告报送上海市通信管理局。对未能在限期内完成整改并提交报告的，上海市通信管理局将依法依规予以处理。（来源：北京市、安徽省、广东省、山东省、浙江省、上海市通信管理局）

3. 上海市车联网网络安全实战攻防活动成功举办

6 月 23 日至 27 日，上海市通信管理局联合市委网信办、市经信委、市交通委、市公安局、嘉定区人民政府共同主办的“铸盾 2026”上海市车联网网络安全实战攻防活动成功举办。

活动聚焦车辆网络安全、数据安全、AI 安全三大核心维度开展全流程模拟攻击与专项安全测试。本届活动汇聚来自全国各车联网企业、机构和高校组成的共 29 支红方队伍、24 家蓝方智能网联汽车生产和运营企业参与。

相较往届，本次攻防演练还有两大创新：一是聚焦车载 AI，增设 AI 专项测试，针对车载大模型、自动驾驶算法研判智能化新风险；二是多元参赛、深耕人才培养，汇聚企业、高校及产业链企业的队伍，培育车联网复合型安全人才。（来源：上海市通信管理局）

（四）其他部门治理实践

1. 最高检发布《未成年人检察工作白皮书（2025）》，未成年人犯罪与侵害未成年人犯罪近五年首次“双下降”

6 月 1 日，最高人民检察院发布《未成年人检察工作白皮书（2025）》。白皮书显示，2025 年检察机关受理审查起诉未成年人犯罪和起诉侵害未成年人犯罪近五年首次实现“双下降”，未成年人犯罪防治工作取得阶段性成效。

在未成年人犯罪基本情况方面，2025 年检察机关受理审查逮捕未成年犯罪嫌疑人 63215 人，同比下降 3%；批准逮捕 35139 人，同比上升 2.4%。受理审查起诉未成年犯罪嫌疑人 91573 人，同比下降 9.8%，系 2021 年以来首次下降。在侵害未成年人犯罪方面，2025 年检察机关批准逮捕侵害未成年人犯罪 56338 人，同比下降 1.4%；起诉 72807 人，同比下降 2.2%。起诉侵害不满 14 周岁未成年人犯罪

38384 人，同比下降 6%，系近五年首次下降。起诉成年人利用电信网络实施侵害未成年人犯罪 2565 人，同比下降 23.4%。

促推未成年人“六大保护”融通发力方面，检察机关立足职能，进一步增强预防就是保护、惩治也是挽救的意识，促推家庭、学校、社会、网络、政府、司法“六大保护”协同发力，经过各方持续努力，2025 年检察机关受理审查起诉未成年人犯罪人数同比下降 9.8%。其中，网络保护方面，检察机关高度重视涉未成年人网络生态治理，持续加强与网信等部门的协作配合，依法从严惩处利用未成年人实施电信网络诈骗犯罪，严厉打击网络欺凌、隔空猥亵等犯罪。关注未成年人网络领域民事权益保护，通过专题座谈、法律咨询、支持起诉、磋商协调等方式，优化未成年人网络环境。认真落实《未成年人网络保护条例》，配合开展未成年人网络环境整治工作，压实网络平台主体责任。最高人民检察院部署开展“依法全面履行检察职能 强化协同履职促进网络治理”专项工作。最高人民检察院未成年人检察厅围绕未成年人利用电信网络实施犯罪等问题开展调研，组织召开预防未成年人参与“人肉开盒”新型网络暴力座谈会，提出预防和治理举措。云南省检察院对 2023 年以来办理的因网络隐患问题导致的涉未成年人案件进行逐案核查，专题报告省委政法委，推进网络空间安全隐患清理整治。山西省检察院会同省委政法委、省委宣传部、省委网信办等 12 个单位印发《全省未成年人网络保护专项行动工作方案》，以打击整治利用网络社交、网络游戏、网络直播、网络音视频等平台侵害未成年人违法犯罪为重点，部署开展为期一年的未成年人网络保护

专项行动。针对直播领域侵害未成年人现象频发等问题，上海市检察院向市电子商务行业协会制发检察建议，促推直播行业规范发展，强化未成年人保护。（来源：最高人民检察院）

2. 国家数据局发布《数字中国发展报告（2025 年）》，我国数智化发展水平跃上新台阶

6 月 8 日，国家数据局发布《数字中国发展报告（2025 年）》。报告指出，2025 年是“十四五”收官之年，数字中国发展指数达到 170.1，较 2024 年增长 12.99%。截至 2025 年底，“十四五”规划中与数字中国相关的目标任务圆满完成，我国数智化发展水平跃上新台阶。

报告从发展基础、赋能效应、发展环境三方面系统总结了 2025 年数字中国建设的主要进展。其中，数智技术创新成果加速涌现。我国已成为全球人工智能专利最大拥有国，占比达 60%。截至 2025 年底，国家互联网信息办公室已完成 748 款生成式人工智能服务备案，2025 年新增 446 款。数据要素潜力加快释放。2025 年全国数据生产量达 52.26 泽字节(ZB)，同比增长 27.28%，占全球数据总量约 27.44%。全国 25 个省（自治区、直辖市）实质性开展公共数据授权运营。数字安全保障能力快速提升。2025 年“清朗”系列专项行动累计清理违法和不良信息 1401 万条，处置账号、群组 59 万个，关闭下架网站平台超 3900 家。个人信息保护系列专项行动累计公开通报 1100 余款违法违规 APP、SDK。

报告展望2026年，提出智能经济新形态将加快形成，数智技术赋能服务业进一步扩能提质，算力资源部署实现规模化、集约化、绿色化发展，数智领域国际合作跃上新台阶。我国将发挥数字基础设施、丰富应用场景、优质数字人才等独特优势，推动实体经济与数字经济加速融合。（来源：国家数据局）

3. 广州互联网法院发布一起涉及未成年个人信息保护公益诉讼

6月1日，广州互联网法院发布第一批未成年人网络司法保护典型案例，案例一为广州市黄埔区人民检察院与被告刘某、倪某、和某、黄某、温某个人信息保护民事公益诉讼案

刘某在从事招录学生的中介事务过程中，通过QQ群及互联网等途径获取了共计502183条学生信息，其中包含大量未成年人的姓名、所在学校、联系电话等内容。其后，刘某将其中部分信息转卖给倪某、和某、黄某、温某，用于招生牟利，导致相关信息被传播和使用。广州市黄埔区人民检察院据此向广州互联网法院提起个人信息保护民事公益诉讼，请求判令刘某、倪某、和某、黄某、温某彻底删除相关学生信息、公开赔礼道歉，并赔偿公益损害赔偿金64493元。

案件审理中，检察机关委托司法鉴定机构对五被告的电子设备进行核查，确认所有涉案个人信息已清理未留存。五名被告均当庭确认侵权事实，并主动提出愿意接受调解、承担全部侵权责任。经广州互联网法院主持调解，检察机关与五名被告达成调解协议。五被告同意

公开赔礼道歉和赔偿损失 64493 元，并作出书面承诺表示，如仍持有非法获取的个人信息，自愿承担公益损害赔偿金 2 倍的惩罚性赔偿金。广州互联网法院对该协议予以确认。五被告在生效调解书确定的期限内已履行完全部法定义务。（来源：广州互联网法院）

4. 因违反网络安全、数据安全等规定，苏州银行股份有限公司被处以 721.02 万元罚款

6 月 10 日，中国人民银行江苏省分行对苏州银行股份有限公司处以警告、通报批评，没收违法所得 399480.86 元，罚款 721.02 万元，合计罚没超 760 万元。行政处罚公告显示，苏州银行涉及违反网络安全管理规定、违反数据安全管理规定等 11 项违法行为类型。（来源：中国人民银行江苏省分行）

5. 因违反数据安全管理等规定，中国银行宁波市分行被处以警告并罚款 436.09 万元

6 月 30 日，中国人民银行宁波市分行发布的行政处罚决定信息（甬银罚决字〔2026〕5 号）显示，中国银行宁波市分行因违反金融统计管理规定、违反数据安全管理规定、违反人民币流通管理规定、违反反假货币业务管理规定、占压财政存款或者资金、违反信用信息采集、提供、查询及相关管理规定等 6 项违法行为，被警告并罚款 436.09 万元。（来源：中国人民银行宁波市分行）

境内前沿观察三：人工智能安全专题

导读：6 月，国务院总理李强主持召开国务院常务会议，听取人工智能发展情况汇报。会议指出，要深刻把握人工智能演进趋势，完善支持政策和治理体系，牢牢掌握发展主动权。工业和信息化部印发《“人工智能+信息通信”创新发展实施意见（2026—2028 年）》，围绕推动信息通信行业智能化升级、夯实人工智能发展底座、深化融合应用创新推广、增强信息通信行业治理能力提出十七项措施。国家金融监管总局发布《关于银行业保险业人工智能安全开发应用的指导意见》，围绕完善人工智能治理架构、推进高水平人工智能开发应用、提升数据治理能力等方面，提出三十二项措施。

执法方面，中央网信办发布利用 AI 制作生成涉军虚假信息典型案例。上海深入开展“清朗·整治 AI 应用乱象”专项行动第一阶段工作，指导 17 家重点网站平台深入开展自查自纠，累计清理拦截违法违规信息 487 万余条，处置违规账号 1.8 万余个，下架违规智能体 1.4 万余个。

关键词：人工智能开发应用；涉军虚假信息；利用 AI 编造谣言；整治 AI 应用乱象

1. 李强主持召开国务院常务会议，听取人工智能发展情况汇报等

6 月 29 日，国务院总理李强主持召开国务院常务会议，听取人工智能发展情况汇报。会议指出，要深刻把握人工智能演进趋势，完善支持政策和治理体系，牢牢掌握发展主动权。要加力推进人工智能创新突破，加快关键技术攻关和超大规模智算集群建设，强化高质量数据供给，加强人才、资金等要素保障，支持企业开展基础研究和前沿探索。要深入实施“人工智能+”行动，发挥我国产业体系完备、应用场景丰富等优势，促进智能产品和服务加快规模化商业应用。要守牢人工智能安全底线，完善科技伦理、测试认证等制度规则，构建动态适应、分级分类的安全监管体系，加强国际人工智能治理合作。（来源：中国政府网）

2. 工信部印发《“人工智能+信息通信”创新发展实施意见（2026—2028 年）》

6 月 3 日，工业和信息化部印发《“人工智能+信息通信”创新发展实施意见（2026—2028 年）》。《实施意见》围绕推动信息通信行业智能化升级、夯实人工智能发展底座、深化融合应用创新推广、增强信息通信行业治理能力提出十七项措施。

推动信息通信行业智能化升级方面，《实施意见》提出加强网络智能体创新发展与应用。支持研发专业性高、落地性强的网络大模型

和智能体，突破大小模型协同、多智能体协同、智能体通信等技术。打造自主智能体通信协议，深化网络领域的适配与应用，鼓励探索基于智能体的新型电信业务形态，构建网络智能体自主产业生态。面向信息通信领域模型训练和应用需求，在重点场景打造一批信息通信行业高质量数据集。

夯实人工智能发展底座方面，《实施意见》提出优化算力设施部署。构建“枢纽一区域一边缘”三级节点协同的算力设施体系，加快算力大通道建设，支撑人工智能和信息通信融合创新。建立完善国家和区域算力平台，强化算力统筹监测和供需对接，促进算力、模型、应用一体化协同创新，提升信息通信业数据资源利用率。形成统一算力标识体系，加快构建全国一体化、集约化、市场化的算力服务体系，加速信息通信业数字化、智能化转型升级。（来源：工信部）

3. 国家金融监管总局发布《关于银行业保险业人工智能安全开发应用的指导意见》

6 月 18 日，国家金融监管总局发布《关于银行业保险业人工智能安全开发应用的指导意见》，围绕完善人工智能治理架构、推进高水平人工智能开发应用、提升数据治理能力等方面，提出三十二项措施。

完善人工智能治理架构方面，《意见》提出，加强人工智能安全开发应用治理。开发应用人工智能的银行业保险业金融机构，董（理）事会应指定专门委员会对人工智能开发应用管理负责，统筹制定发展

规划，推进能力体系建设，制定制度规范，明确牵头部门和跨业务、科技、数据职能部门的协同机制，加强人才队伍建设，遵循技术发展客观规律，确保人工智能应用与金融机构风险管理能力相匹配。

推进高水平人工智能开发应用，《意见》提出，建设人工智能高质量数据集。金融机构应针对人工智能业务场景持续推进高质量数据集建设，确立数据质量标准，建立高效的质量检控机制，确保数据准确性、相关性、一致性、完整性和无偏见。探索运用人工智能技术强化实时数据、非结构化数据的动态感知、智能提取和解析处理。持续监测数据分布漂移，确保数据集及时更新。（来源：国家金融监管总局）

4. 中央网信办发布利用 AI 制作生成涉军虚假信息典型案例

6 月 9 日，中央网信办发布利用 AI 制作生成涉军虚假信息典型案例。

案例一：利用 AI 编造虚假涉军故事。网络账号“楚晴”“黄仙 1000 芬挑战”AI 生成“孕妇哭诉丈夫执行军事任务牺牲，求点赞转发”故事引流起号。网络账号“大龙麻麻”“艳子”AI 生成“孩子吃了补品后个头长高了，如愿以偿考上军校”故事，编造涉军噱头为增高保健品广告营销。

案例二：利用 AI 合成涉军庸俗视频。网络账号“厚积薄发”AI 制作着军装视频，发布“持枪瞄准拍摄者并威胁开枪”“军人抱着立

功证书热舞”等内容。网络账号“糖糖百货铺”AI 制作“中国战地记者在前线报道，求点赞”视频，误导网民认知。

案例三：利用 AI 丑化涉军公众人物。网络账号“洺锋”、网络账号“疯惨”AI 制作国防部新闻发言人、“最美女飞行员”等军队人员的恶搞视频吸粉引流，损害军队军人形象。（来源：网信中国）

5. 国家发展改革委：中国正加紧筹建世界人工智能合作组织

6 月 17 日，国新办举行《构建更加公正合理的全球治理体系：中国的理念、倡议与行动》白皮书新闻发布会。记者从会上获悉，中国正在加紧筹建世界人工智能合作组织，欢迎各方加入，共促智能向善。

国家发展改革委副主任周海兵介绍，人工智能治理攸关全人类命运，是世界各国面临的共同课题。中国秉持多边主义和开放包容理念，积极推动人工智能全球治理和国际合作，持续为智能时代全球发展贡献中国方案。

在治理实践方面，中国率先发布了《全球人工智能治理倡议》，确立了智能向善、安全可控、普惠公平的治理导向，为人工智能全球治理提供了系统、务实、可落地的行动指引。中国支持联合国发挥人工智能全球治理主渠道作用，推动联合国大会通过人工智能能力建设国际合作决议，提出《人工智能能力建设普惠计划》，常态化开展国际交流培训，助力广大发展中国家弥补技术、人才、治理短板，切实弥合全球智能发展鸿沟。

在国际合作方面，中国依托上海合作组织、金砖国家合作机制等多边平台，持续深化人工智能务实合作。大力发展开源开放生态，推动技术成果、应用经验全球共享，坚决摒弃封闭排他、技术垄断的发展模式，着力构建开放包容、互利共赢的国际合作格局。中国连续8年举办世界人工智能大会，倡议成立世界人工智能合作组织。今年7月，中国将在上海举办2026世界人工智能大会暨人工智能全球治理高级别会议，期待以本次大会为契机，同各方进一步加强国际人工智能合作。

周海兵表示，下一步，中国将坚持统筹发展和安全，积极践行多边主义，秉持“以人为本、智能向善”的理念，推动人工智能始终朝着有益、安全、公平方向发展。同时，履行大国责任，管控风险、强化预防，探索开展人工智能监管合作，共同防范人工智能安全风险。（来源：新华社）

6. 江苏省工业和信息化厅印发《江苏省“人工智能+制造”实施方案》

6月3日，江苏省工业和信息化厅印发《江苏省“人工智能+制造”实施方案》。《方案》围绕推进人工智能在制造业各环节深入应用、加快工业人工智能模型和软件产品供给、提升关键硬件和装备产品供给能力等五个方面提出二十二项措施。

加快工业人工智能模型和软件产品供给方面，《方案》提出推动建设行业高质量数据集。推动企业设立首席数据官，持续推进数据管

理能力成熟度国家标准贯标，夯实企业数据治理基础。开展全省工业和信息化领域行业高质量数据集建设先行先试，推动企事业单位、行业协会、研究机构、集群促进机构等将数据资源转化为高质量数据集，打造行业数据资源库、行业数据技术库、行业数据标准库、行业高质量数据集库，建设行业数智服务平台，完善“4 库 1 平台”行业高质量数据治理体系。实施“模数共振”行动，基于行业数智服务平台开展“以模引数”“用数赋模”，加快形成“数据驱动—模型迭代—场景落地”闭环。

优化制造业人工智能赋能发展生态，《方案》提出加快工业人工智能应用引导和标准制定。结合江苏省制造业领域人工智能技术应用、数据治理、安全防护工作参考指引，加快上线人工智能场景应用等级、数据治理能力、安全防护自评测系统。研制出台全国首个制造业人工智能技术应用场景等级水平建设评价标准。编制基于智能工厂梯度培育的人工智能技术应用典型案例集。（来源：江苏省工信厅）

7. 湖南网警依法查处 2 起利用 AI 工具编造涉张家界景区的谣言案

6 月 17 日消息，湖南公安网安部门依法查处 2 起利用 AI 工具编造涉张家界景区的谣言案。

4 月 26 日，一则“湖南张家界大峡谷玻璃桥断裂垮塌”的视频在网上流传，视频画面显示：张家界大峡谷玻璃桥登桥平台与玻璃桥面衔接的地方发生断裂，大量游客四处奔跑避险，有数名游客从桥面

坠落，并配文：没事就别总想着出去玩了，还是家里安全，并加上了有关张家界的话题词。视频发出后，引发大量网民关注和讨论，当时正值“五一”假期前夕，造成部分游客恐慌，还有不少市民和游客向张家界大峡谷景区拨打电话咨询玻璃桥是否发生垮塌事故。后查明，嫌疑人马某某为博取关注、吸粉引流，使用 AI 工具生成了该谣言视频，并在互联网平台发布，目前，马某某已被公安机关依法采取刑事强制措施。

然而，网民朱某某并未引以为戒，仍然使用 AI 工具制作并发布涉张家界旅游景区的谣言：5 月 23 日，一篇题为《湖南张家界百龙天梯故障频发,游客被困百米高空一小时》的文章在网络上大肆扩散：文章绘声绘色地描述电梯故障、游客被困等惊险场景，引发大量网民关注，造成公众对景区安全管理状况的担忧。公安网安部门迅速开展工作，经核实，百龙天梯并未发生任何故障或游客被困事件，文章内容纯属凭空捏造。经查，朱某某为吸粉引流、提升账号商业价值，使用 AI 生成了谣言信息，并在互联网平台发布。目前，属地公安机关已依法对朱某某作出行政拘留的处罚。（来源：公安部网安局）

8. 上海深入开展“清朗·整治 AI 应用乱象”专项行动第一阶段工作，下架违规智能体 1.4 万余个

6 月 26 日，上海市网信办发布“清朗 • 整治 AI 应用乱象”专项行动第一阶段工作成果。

4 月下旬以来，上海市委网信办聚焦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、滥用 AI 技术开展违法违规活动、开源模型安全管理不到位 7 类突出问题，扎实推进专项行动。

5 月 13 日，上海市委网信办召开重点平台专项行动推进会，向属地 AI 平台、互联网内容平台、电商平台、应用商店、开源社区等五类 17 家重点网站平台部署具体要求，指导平台升级安全与举报机制、接受社会监督。5 月 15 日，指导稀宇、千问、小红书、哔哩哔哩、拼多多等重点平台公开发布专项治理公告，形成监管与平台治理合力。同期，上海举报中心官网开设专项举报渠道，迄今受理涉 AI 类违法不良信息举报及 12345 市民反映相关线索 20 余件。

上海市委网信办指导 17 家重点网站平台深入开展自查自纠，累计清理拦截去 AI 标识的工具和教程、数据投毒、未经授权“换脸拟声”、AI 制谣传谣、AI 低俗内容等违法违规信息 487 万余条，处置违规账号 1.8 万余个，下架违规智能体 1.4 万余个，处置违规商品 1300 余个，并对多次违规的账号实施阶梯式约束与封禁。各网站平台积极履行主体责任，深化治理成效。稀宇持续下架“一键脱衣”、赌球博彩等违规智能体，打击利用 AI 编写病毒、钓鱼软件等恶意行为；小红书打击 AI 托管运营账号，禁售去 AI 标识商品，积极推进与各大制作平台隐式标识互认；哔哩哔哩在内容发布页强化提示，将“AI 生成”列为必选标签，引导创作者规范发布；魔搭社区全面清理下架涉低俗等违规数据集，强化开源模型的审核与管理。

为确保治理常态化，上海市委网信办组织3家专业机构，对用户量大、影响力高的32款AI产品开展了专项巡查测试，并赴4家企业进行现场检查。通过督导企业举一反三，重点整改AI标识落实不到位、平台安全和审核能力不足等问题，进一步提升技术防范能力，完善长效治理机制。（来源：网信上海）

境外前沿观察：月度速览十则

导读：6月，美国、加拿大、欧盟、澳大利亚、西班牙发布网络安全、人工智能相关政策报告，强化网络和人工智能治理，推进人工智能安全发展。

网络安全方面，美国白宫发布总统备忘录《针对国家安全系统的网络安全国家政策》，通过明确权力结构、角色分工和问责机制，强化国家安全系统治理。美国还发布《国家韧性战略》，提出“风险优先、系统现代化、通过联邦制分配责任、简化治理”四项转型支柱，并将其应用于国家安全、经济、公共卫生与安全、国家基础设施四大核心韧性领域。

人工智能安全和发展方面，美国总统特朗普签署行政令《推动先进人工智能创新与安全》，在维持美国人工智能创新优势的同时，强化网络安全、关键基础设施保护和前沿模型安全部署。加拿大总理发布国家人工智能战略《全民人工智能》，推动人工智能以负责任、可信赖且服务全体加拿大公民的方式落地，在增强公众信任、扩大发展机遇的同时维护国家主权。欧盟委员会发布《人工智能生成内容透明度行为守则》，围绕《人工智能法》建立的透明度义务，对相关人工智能系统提供者和部署者提出操作性规则。五国网络安全机构发布联合声明《人工智能推动网络风险变化：为何领导者必须立即行动》，指出人工智能对网络安全的威胁，要求各类组织应立即采取应对措施。西班牙国家密码中心计算机应急响应中心发布《应对攻击型人工智能

模型最佳实践指南》，旨在帮助公共和私营组织理解人工智能对网络安全威胁格局的影响，并提升面对新型攻击场景的准备能力。此外，美国对 Anthropic Claude Fable 5 和 Mythos 5 采取出口管制措施,但于月底接触禁令。

关键词：网络安全韧性；人工智能；出口管制；勒索软件

1. 美国总统签署《推动先进人工智能创新与安全》行政令

6 月 2 日，美国总统特朗普签署第 14409 号行政令《推动先进人工智能创新与安全》，旨在通过政府与私营部门合作，在维持美国人工智能创新优势的同时，强化网络安全、关键基础设施保护和前沿模型安全部署。行政令确立三项目标：推进政府及私营部门信息系统现代化，提升抵御外部威胁的能力；保护美国创造力和知识产权免遭对手窃取利用；培育美国先进人工智能赋能能力。

在网络安全和系统防御方面，行政令要求相关联邦机构优先加强国家安全系统、国防信息系统和联邦民用政府信息系统的网络防御，扩充人工智能赋能防御工具项目，并推动相关工具和服务应用于联邦机构、州和地方政府等关键基础设施运营者。同时，行政令要求扩大网络安全专员招聘通道，并排查可用于人工智能漏洞检测的联邦拨款资源。

在前沿模型安全部署和执法打击方面，行政令要求建立“人工智能网络安全信息交换中心”，统筹软件漏洞扫描、发现验证、修复优先级协调和补丁分发，并建立保密基准评估流程和自愿性政府接触框架，使开发者可在模型向可信伙伴发布前最多提前 30 天向联邦政府提供安全早期访问。行政令同时强调，该机制不得被解释为对新人工智能模型开发、发布或分发设立强制许可、预先审查或审批要求。司法部长还应优先适用相关联邦刑事法律，打击利用人工智能非法访问、损害计算机系统，或者在非法访问过程中进一步实施其他犯罪的行为，

包括使用人工智能智能体非法获取数据并用于犯罪或违法目的的情形。（来源：美国白宫）

2. 加拿大总理发布国家人工智能战略《全民人工智能》

6 月 4 日，加拿大总理发布国家人工智能战略《全民人工智能》。该战略为期五年，旨在通过新的立法、投资和项目安排，推动人工智能以负责任、可信赖且服务全体加拿大公民的方式落地，在增强公众信任、扩大发展机遇的同时维护国家主权。

战略围绕以下支柱提出系统行动：一是保护加拿大公民、捍卫民主，通过完善现代化隐私与在线安全立法、提升国家人工智能安全保障能力、保障政府系统安全，筑牢公众信任基础；二是赋能加拿大公民，推动加拿大成为“人工智能技能国家”，扩大人工智能培训与教育，并体现加拿大多元声音、语言和文化；三是推动人工智能应用，在全经济范围内推广亲劳动者的产业级人工智能技术，重点支持中小企业应用，并改进公共服务交付等。（来源：加拿大政府）

3. 美国白宫发布总统备忘录《国家安全体系中的人工智能》

6 月 5 日，美国白宫发布总统备忘录《国家安全体系中的人工智能》，建立新的国家安全人工智能框架，旨在加快将先进、安全、可靠的人工智能系统提供给美国作战人员和情报专业人员使用，同时确保其负责任使用。

备忘录确立“采用、适配、保障、问责”四项支柱：要求国家安全体系识别人工智能能够提升作战效能的任务领域，消除快速部署中的不必要障碍，主动接入商业、开源或定制化人工智能技术；同时开展测试、评估、验证与确认工作，确保相关系统具备可靠性、稳健性、可引导性和可控制性，并维护系统机密性、完整性、可靠性、可用性和互操作性。备忘录还明确，国家安全体系不得使用人工智能审查言论自由、嵌入意识形态偏见，或实施未经授权、违法的监控活动，并要求各级指挥官、主管和机构负责人承担相应责任。

在具体措施方面，备忘录要求更新国防部关于武器系统自主性的相关指令，审查并优化采购流程，确保国家安全人员能够快速接入多个供应商提供的最先进人工智能模型；同时制定路线图，保障国家安全体系获得先进算力，建设高安全人工智能计算设施和国家安全场景测试靶场。备忘录还要求通过人工智能安全中心与自愿参与的私营部门企业合作，保护美国前沿人工智能技术，防范恶意蒸馏攻击，并开展威胁情报共享、联合红队测试、人员审查协助、联合安全研发以及强化数据中心实体安全和网络安全等活动。（来源：美国白宫）

4. 欧盟委员会发布《人工智能生成内容透明度行为守则》

6 月 10 日，欧盟委员会发布《人工智能生成内容透明度行为守则》，围绕《人工智能法》第五十条建立的透明度义务，对相关人工智能系统提供者和部署者提出操作性规则。

在系统提供者义务方面，守则要求，对于生成或操纵音频、图像、视频、文本内容的人工智能系统，提供者应确保输出内容以机器可读格式标识，并能够被检测为人工智能生成或操纵内容。相关技术方案应在技术可行范围内具备有效性、互操作性、稳健性和可靠性。对于可在线传播的音频、图像、视频以及能够附加元数据的文档化文本内容，原则上应采取多层标识方式，至少包括两层机器可读标识。守则还要求在支持元数据的内容格式中记录内容是否由人工智能生成或操纵，并进行数字签名和时间戳处理；同时嵌入不可感知水印，极短文本除外，自由文本超过 200 个 token 的仍需适用水印。检测方案应支持部署者、用户、监管执法机关、媒体、事实核查机构、研究者和社会组织等验证内容来源，并以清晰、可理解、无障碍的方式呈现检测结果。

在系统部署者义务方面，守则要求，对于人工智能生成或操纵、足以构成深度伪造的图像、音频、视频内容，以及用于向公众说明公共利益事项但未经人工审查或编辑控制的人工智能生成或操纵文本，部署者应清晰披露其人工智能生成或操纵属性。依法用于侦查、预防、调查或追诉犯罪的情形，以及已经经过人工审查或编辑控制并由自然人或法人承担编辑责任的公开文本，不适用相应披露义务。守则还要求标签或等效标识应在自然人首次接触相关内容时清晰、可区分、可感知，并符合无障碍要求。（来源：欧盟委员会）

5. 美国 NIST 发布《勒索软件风险管理：网络安全框架 2.0 社区方案》

6 月 11 日，美国国家标准与技术研究院（NIST）下属国家网络安全卓越中心（NCCoE）发布《勒索软件风险管理：网络安全框架 2.0 社区方案》最终版本。该文件与 NIST《网络安全框架》2.0 保持一致，旨在为各类组织管理和缓解勒索软件风险提供实用指引。

该文件以 CSF 2.0 的六大核心职能为框架，梳理与勒索软件风险防范密切相关的成果类别。其中，“治理”强调将网络安全纳入企业整体风险管理并明确政策和责任；“识别”要求掌握组织资产、供应商及相关风险；“保护”侧重身份管理、认证访问控制、意识培训、数据安全和平台安全；“检测”用于及时发现异常和入侵指标；“响应”涵盖遏制、分析、缓解和报告；“恢复”则要求及时恢复受影响资产和运营。文件通过表格列明各职能下与勒索软件风险相关的类别和子类别，供组织评估现状、设定目标状态并识别差距。

文件还提出组织可立即采取的基础防护措施，包括制定勒索软件事件应对计划，明确决策者和网络安全角色职责，厘清法律法规及合同要求；通过钓鱼和社交媒体演练提升员工安全意识；及时修补系统漏洞，在联网系统中运用零信任原则，仅允许安装和运行经授权的应用；部署恶意软件检测工具，持续监测目录服务；推广多因素认证和最小权限原则；制定并演练事件响应与恢复计划，并可结合实际考虑投保网络保险。（来源：美国国家标准与技术研究院）

6. 美国白宫发布总统备忘录《针对国家安全系统的网络安全国家政策》

6 月 12 日，美国白宫发布总统备忘录《针对国家安全系统的网络安全国家政策》，旨在为美国国家安全系统确立新的网络安全治理架构。备忘录提出，美国政府将构建主动、适应性强且具有韧性的国家安全系统网络安全生态，以应对复杂对手持续带来的网络威胁，并通过明确权力结构、角色分工和问责机制，强化国家安全系统治理。

在治理架构方面，备忘录重新设立国家安全系统委员会，由总统国家安全委员会工作人员担任主席，成员包括战争部首席信息官、国家情报总监办公室首席信息官、行政管理和预算局局长以及国家安全局局长等。该委员会负责制定国家安全系统基线网络安全要求，对系统所有者和运营者进行问责，并代表国家安全系统生态提出政策和资源需求。备忘录同时确立国家安全局局长的国家管理者角色，赋予其识别新兴威胁、提出政策建议、发布紧急指令、制定密码学和密码系统最低要求、评估国家安全系统网络安全态势以及开展国际密码学和网络安全联络等职责。

在技术标准和实施要求方面，备忘录规定国家安全系统原则上须达到或超过美国国家标准与技术研究院发布的网络安全标准保护水平，并要求委员会和国家安全局局长限期发布政策路线图、审查现有政策指令、制定安全事件报告标准，建立政府范围内的事件感知机制。各机构须维护并年度更新其国家安全系统清单，并按要求报告安全事件。备忘录还要求推进国家安全系统云安全治理，提出不同密级云能

力配置报告和安全配置基线建议，并研究安全、可互操作的非密语音和视频通信能力。（来源：美国白宫）

7. 澳大利亚等五国网络安全机构发布联合声明，警示人工智能正在加速网络风险变化

6 月 22 日，澳大利亚、加拿大、新西兰、英国、美国的网络安全机构发布联合声明《人工智能推动网络风险变化：为何领导者必须立即行动》，警示人工智能正在迅速改变网络风险格局，使网络威胁的速度、规模和复杂性持续上升。

声明强调，网络风险已不再是单纯技术问题，而是核心业务风险和领导层责任。董事会和高级管理人员应确认网络韧性已经建立并能在真实压力下发挥作用，重新评估效率、成本与安全之间的取舍，并有意识地使用人工智能强化防御，而不能仅将其作为提升效率的工具。声明要求领导层重点做好风险评估、准备状态和问责安排，优先落实基础性网络安全控制措施，赋予网络安全负责人必要权限和资源，并随着威胁和指导意见变化保持持续参与。

在具体安全措施方面，声明提出减少攻击面、加快补丁流程、处理遗留系统、强化身份和访问控制、提前做好事件响应准备等要求，包括限制不必要访问和外部连接、隔离无需暴露的系统、执行强身份认证、定期审查权限、测试响应计划并加强团队训练。声明还强调，防御方应主动将人工智能工具纳入安全运营，用于更早发现漏洞、提

升软件质量、监测异常行为和加快事件响应，以降低网络安全事件的成本和影响。（来源：美国网络安全和基础设施安全局）

8. 美国白宫发布《国家韧性战略》，强化关键系统网络韧性与可信人工智能

6 月 23 日，美国白宫发布《国家韧性战略》，提出“风险优先、系统现代化、通过联邦制分配责任、简化治理”四项转型支柱，并将其应用于国家安全、经济、公共卫生与安全、国家基础设施四大核心韧性领域。

在网络和数据安全方面，战略强调，应在大规模范围内设计和实施具有互操作性、安全性的网络与物理架构，保障关键服务可靠运行，并推动包括可信赖美国人工智能能力在内的先进技术安全整合，以巩固美国技术主导地位。在国家安全领域，战略提出通过现代化地面和天基物理及数字基础设施，限制对手入侵、扰乱或操纵美国决策优势和关键系统的能力；在经济领域，则要求现代化金融和信息技术系统，提升其抵御网络攻击能力，保障支付、流动性和可信赖信息流动，并防止对手获取美国新兴和先进技术核心能力。

战略还明确美国公民、产业界、州和地方政府以及联邦政府在国家韧性建设中的不同角色，强调将更多权责从联邦层面下放至州和地方，同时通过简化治理和责任分配提升整体应对能力。整体来看，该战略将网络韧性、关键基础设施安全、先进技术保护和可信人工智能

应用纳入国家韧性建设框架，体现出美国以系统现代化支撑国家安全和经济安全的政策取向。（来源：美国白宫）

9. 西班牙国家密码中心计算机应急响应中心发布《应对攻击型人工智能模型最佳实践指南》

6 月 25 日，西班牙国家密码中心计算机应急响应中心（CCN-CERT）发布《应对攻击型人工智能模型最佳实践指南》，旨在帮助公共和私营组织理解人工智能对网络安全威胁格局的影响，并提升面对新型攻击场景的准备能力。

指南重点提示以下几类风险：攻击自动化、合成式社会工程、针对人工智能系统的攻击、人工智能供应链风险以及自主智能体滥用，涉及大规模侦察、深度伪造、提示词注入、数据泄露、工具滥用、RAG 流程操纵、插件和 MCP 等第三方依赖风险，以及 API 调用、系统变更和数据提取等未经充分控制的行为。对应防护措施包括基于行为的检测、输入输出校验、隔离、审计、人工智能资产清单、第三方评估、最小权限、人工监督和熔断机制等。指南强调，应对攻击型人工智能不能仅依赖采购新工具，而应重构组织安全模型，强化身份管理、网络分段、持续监测、访问控制、关键资产保护、漏洞管理和补丁流程，并在严格控制、人工监督和可追溯要求下，将人工智能用于防御性检测和自动化响应。

指南特别关注 AI 智能体安全。指南认为其可能带来操作执行失控、提示词注入、数据外泄、错误链式放大、外部 API 滥用、凭证管

理和可追溯性不足等风险，建议通过身份与访问管理、隔离环境、输入清洗、系统指令与用户上下文分离、DLP、内容过滤、API 网关等措施加以治理。（来源：西班牙国家密码中心计算机应急响应中心）

10. 美国商务部对 Anthropic Fable 5 和 Mythos 5 模型施加出口管制，并于同月底解禁

6 月 9 日，美国人工智能公司 Anthropic 发布 Claude Fable 5 和 Mythos 5，称其具备强大的网络安全技术能力。为防止安全能力被不受限制的广泛使用、滥用，正式发布的 Fable 5 设置了安全防护对相关能力进行限制，而 Mythos 5 则仅通过“玻璃翼计划”与美国政府合作向少数网络防御者和关键基础设施提供商开放部署。两款模型发布后，亚马逊研究人员报告了一种可绕过 Fable 5 安全防护的方法（即“越狱”），美国政府认为这可能导致其网络安全能力被不当获取。

6 月 12 日，美国政府根据国家安全授权发布出口管制指令，要求 Anthropic 暂停“任何外国公民”对两款模型的访问。此后，Anthropic 与美国政府开展协商谈判并改进安全分类器等安全措施。6 月 26 日，美国商务部长致函 Anthropic，认定已具备“适当的保障措施”，允许其向选定的一组美国组织恢复 Mythos 5 访问。6 月 30 日，商务部正式解除对两款模型的出口管制。

Anthropic 表示，此次事件表明业界需要一套评估人工智能“越狱”（即通过漏洞绕过安全保护限制）严重程度的一致标准，其正与亚马逊、微软、谷歌等合作伙伴共同起草一套包括“能力提升幅度”、

“能力提升广度”、“武器化难易度”和“可发现性”四项标准的越狱评分行业框架，并邀请其他厂商共同参与起草。同时，Anthropic还表示将深化与美国政府在“发布前的政府访问与评估”“安全防护措施信息共享”“联合研究资源投入”“行业基准设计”等领域加强合作。（来源：Anthropic 官网）

行业前沿观察：各地协会动态

各地协会立足本职服务大局，紧扣国家战略需求，在人工智能创新应用、网络安全人才培养、行业标准建设、数字素养提升、产业协同交流及社会服务等领域广泛发力，各展所长、协同联动，同频共振助力数字中国建设，为经济社会高质量发展注入行业动能。肇庆市信息协会全程指导的肇庆市首届“榕智杯”大学生网络安全知识大赛决赛圆满落幕；海南省计算机学会共同承办的2026科创咖啡时间“人形机器人与具身智能技术研讨会”成功举办；北京网络空间安全协会网络安全专业人才职称体系建设与人才吸引策略主题沙龙圆满落幕；安徽省网络安全协会指导的2026绿盟科技徽安峰会圆满落幕；惠州市计算机信息网络安全协会“蒲公英文明种子计划”六一专场活动圆满举办；甘肃省商用密码行业协会主办的“2026年密码法治陇原行”活动在陇南市成功举办；西藏自治区互联网协会联合主办的“笃行AI 见实见效”2026深信服城市峰会拉萨站成功举办；海南省网络安全和信息化协会联合主办的“2026年海南省大学生网络安全能力提升培训班”在海南大学网络空间安全学院正式开班；北京网络行业协会新媒体治理与合规专委会召开首次行业闭门研讨会 新当选的主任田维主持并发布合规指引；湖南省网络空间安全协会走访华为技术有限公司；上海市信息安全行业协会“匠心铸盾，数智护航”——链盾软件供应链攻防博弈竞赛（团队赛）决赛顺利完赛；澳门国际科技产业发展协会成功举办「AI赋能澳门商户与个人创作者实战营」；苏州市互联网协会参加2026年度

全省互联网行业赋能行动；苏州市新媒体联合会联合协办的第二届苏州物业企业发展交流大会圆满举办；广东省网络空间安全协会顺利召开2026年广东省网络空间安全标准化技术委员会工作会议；肇庆市计算机学会成功组织协办“数智赋能·安全同行”人工智能主题宣传活动；深圳市网络与信息安全行业协会联合承办深圳市2026年数字体验展暨鸿蒙生态体验活动；金华市网商协会联合协办的创业政策及企业合规专场活动成功举办；陕西省互联网协会受邀出席陕西太乙数字艺术研究院成立大会并深度参与研讨；陕西省信息网络安全协会赴省公安厅网安总队开展交流学习活动。

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. 肇庆市信息协会全程指导的肇庆市首届“榕智杯”大学生网络安全知识大赛决赛圆满落幕

2026 年 5 月 10 日，由肇庆市计算机学会、肇庆市信息协会全程指导，广东榕智环球科技有限公司、深信服科技股份有限公司联合主办，广州应用科技学院协办的肇庆市首届"榕智杯"大学生网络安全知识大赛决赛，在广州应用科技学院顺利落下帷幕。来自肇庆多所高校的网安学子同台竞技，一场兼具专业性与观赏性的网络安全盛会，就此圆满收官。

2. 海南省计算机学会共同承办的 2026 科创咖啡时间“人形机器人与具身智能技术研讨会”成功举办

5 月 21 日下午，由海南省科学技术协会主办，海南省计算机学会、海南医科大学智能医学与技术学院（大数据研究中心）、海南大学计算机科学与技术学院、乐聚智能（深圳）股份有限公司、海南恒洛智港科技有限公司、海南省网络安全和信息化协会以及海南医科大学大学生活动中心共同承办的“2026 科创咖啡时间——人形机器人与具身智能技术研讨会”在海南医科大学大学生活动中心一楼演播大厅成功举办。

3. 北京网络空间安全协会网络安全专业人才职称体系建设与人才吸引策略主题沙龙圆满落幕

2026 年 6 月 2 日，为深耕会员服务、精准对接企业职称筹备刚需，由北京网络空间安全协会组织的网络安全专业人才职称体系建设与人才吸引策略主题沙龙在绿地中心中国锦圆满落幕。

首都经济贸易大学、北京北信源软件股份有限公司、国富瑞数据系统有限公司、永信至诚科技集团股份有限公司、北京威努特技术有限公司、北京北科控股有限公司、长安通信科技有限责任公司、北京国瑞数智技术有限公司、北京国舜科技股份有限公司、北京建恒信安科技有限公司、北京格尔国信科技有限公司、中国节能环保集团有限公司、北京长亭科技有限公司、北京知其安科技有限公司等多家高校及网络安全领域企事业单位的人事负责人与技术专家齐聚现场，围绕北京市网安职称评审落地细则、企业内部职称体系搭建、人才长效激励方案展开深度研讨。

4. 安徽省网络安全协会指导的 2026 绿盟科技徽安峰会圆满落幕

近日，由安徽省网络安全协会指导、绿盟科技集团主办的 2026 绿盟科技徽安峰会在安徽巢湖圆满落幕。本届峰会以“安全内生筑基·数智赋能焕新——智构未来安全体系”为主题，已是连续成功举办六年的行业盛会。峰会汇聚政府主管部门、通信运营商、金融、能源、交通、科教及各大企事业单位的行业同仁与网络安全专家，聚焦数智

化转型安全核心议题，共探 AI 与网络安全深度融合新路径，为安徽区域网络安全产业协同发展、千行百业数智化安全建设凝聚合力、赋能赋能。

5. 惠州市计算机信息网络安全协会“蒲公英文明种子计划”六一专场活动圆满举办

为进一步筑牢未成年人网络安全防护屏障，近日，由惠州市捡跑协会主办，惠州市网安协会、惠州学院红帽先锋网安协会等协办的新时代文明实践“蒲公英文明种子计划”捡跑下社区+N 拓展项目六一儿童节专场活动圆满落幕。本次活动将信息网络安全宣传、垃圾分类宣传、环保宣传及防溺水宣传与文艺展演深度融合，吸引众多亲子家庭参与，为社区群众呈现了一场兼具知识性与趣味性的文明盛宴。

6. 甘肃省商用密码行业协会主办的“2026 年密码法治陇原行”活动在陇南市成功举办

2026 年 6 月 4 日，由省国家密码管理局指导、省商用密码行业协会主办、 陇南市国家密码管理局承办的“2026 年密码法治陇原行”陇南站活动成功举办。省、市国家密码管理局相关同志、陇南市重要网络与信息系统运营者单位负责人、省商用密码行业协会专家及会员单位代表等共 50 余人参加。省国家密码管理局相关领导出席活动并致辞。

7. 西藏自治区互联网协会联合主办的“笃行 AI 见实见效”2026 深信服城市峰会拉萨站成功举办

当前，人工智能技术正加速从概念落地至产业全场景，成为驱动数字经济高质量发展的核心引擎，为搭建行业交流平台，汇聚前沿实践经验，推动 AI 技术在全区各行业的落地应用。

2026 年 6 月 5 日，由西藏自治区互联网协会联合深信服科技股份有限公司、西藏自治区信息协会、西藏自治区网络与数据安全协会、西藏自治区网络空间与数据安全协会主办的“笃行 AI 见实见效”2026 深信服城市峰会拉萨站在拉萨圣地天堂洲际大饭店圆满举行。来自政府机构、行业协会、区内外企业等 200 余位代表参会。西藏自治区党委网信办副主任吴坚出席并致辞。

8. 海南省网络安全和信息化协会联合主办的“2026 年海南省大学生网络安全能力提升培训班”在海南大学网络空间安全学院正式开班

椰风送爽，盛夏燃情。2026 年 6 月 6 日上午，由海南省网络安全和信息化协会、新华三集团、海南大学联合主办的“2026 年海南省大学生网络安全能力提升培训班”在海南大学网络空间安全学院正式开班。来自海南大学、海南师范大学、海南软件职业技术学院等省内高校的约 30 名网络安全专业学子齐聚一堂，开启为期三天的实战化集训，为即将到来的全省网络安全大赛蓄力备战。

9. 北京网络行业协会新媒体治理与合规专委会召开首次行业闭门研讨会，新当选的主任田维主持并发布合规指引

为落实中央及北京市关于加强网络内容治理、规范新媒体传播秩序的工作要求，北京网络行业协会-新媒体治理与合规专业委员会（以下简称“专委会”）于近日在北京召开成立后首次行业闭门研讨会。专委会主任田维主持会议并发布《2026 新媒体内容合规与版权保护指引（试行）》，来自头部平台、MCN 机构、版权服务机构及法律专家代表共 30 余人参会。

10. 湖南省网络空间安全协会走访华为技术有限公司

2026 年 6 月 12 日，湖南省网络空间安全协会理事长苏金树教授带队前往华为技术有限公司开展走访交流活动，多家会员单位代表一同参与，华为湖南政企解决方案部部长罗立强及技术团队热情接待。

11. 上海市信息安全行业协会“匠心铸盾，数智护航”——链盾软件供应链攻防博弈竞赛（团队赛）决赛顺利完赛

6 月 13 日，“2026 年上海职工职业技能系列竞赛--数据安全管理员技能大赛暨第四届浦东新区数智未来守护者大赛”——“链盾”软件供应链攻防博弈竞赛（团队赛）决赛，在上海浦东软件园三林园圆满落幕。

12. 澳门国际科技产业发展协会主办的「AI 赋能澳门商户与个人创作者实战营」成功举办

由澳门国际科技产业发展协会主办、工商业发展基金资助、粤澳国际产业融合青创发展基地及博维智慧科技有限公司支持的“AI 赋能澳门商户与个人创作者实战营”于 6 月 13 日至 14 日在澳创家共享空间成功举办。活动旨在聚焦澳门本地商户与个人创作者在数字化转型及内容传播方面的实操需求。

13. 苏州市互联网协会参加 2026 年度全省互联网行业赋能行动

6 月 16 日至 17 日，2026 年度“苏网领航 发展同行”全省互联网行业赋能行动在苏州举行，省市网信办相关工作负责同志和网络社会组织代表参加活动。

本次活动过程中，江苏省委网信办原二级巡视员、省互联网行业联合会常务副会长杜家雷分别在同程网络科技股份有限公司和苏州大禹数字文化科技集团有限公司，看望慰问了企业新就业群体代表，与大家亲切交流，详细了解工作生活情况，对大家立足岗位、服务社会作出的积极贡献表示充分肯定，并勉励大家坚定信心、立足本职，不断提升专业技能和服务水平，在推动互联网行业高质量发展中展现新作为。

14. 苏州市新媒体联合会联合协办的第二届苏州物业企业发展交流大会圆满举办

6 月 16 日，由苏州市新媒体联合会理事单位苏房物研（物研智库）主办的 2026 第二届苏州物业企业发展交流大会在苏州狮山国际会议中心圆满举办。苏州市新媒体联合会作为本次大会的联合协办单位之一，积极参与并支持了活动的组织与传播工作。

本次大会以“品质立身·数智赋能”为核心主题，汇聚政府主管部门代表、物业企业高管、行业专家、科技服务商、法律服务机构及主流媒体等近 200 位嘉宾，大家齐聚一堂，共谋行业前行之路。

15. 广东省网络空间安全协会顺利召开 2026 年广东省网络空间安全标准化技术委员会工作会议

2026 年 6 月 24 日下午，2026 年广东省网络空间安全标准化技术委员会工作会议在广州顺利召开，会议聚焦标准政策环境研判、组织结构优化、重点标准方向等核心议题深入研讨。广东省网络空间安全协会黄丽玲会长、成珍苑副会长、蔡舒婷执行秘书长，省网安标委委员、工作组成员等代表出席会议。会议由协会党支部专职副书记黄汝锡主持。

16. 肇庆市计算机学会成功组织协办“数智赋能·安全同行”人工智能主题宣传活动

2026 年 6 月 24 日，由省委网信办，市委网信办联合主办，南方

新闻网、市工业贸易学校、中国电信肇庆分公司联合承办；肇庆市委社会工作部、肇庆市融媒体中心、肇庆市发展和改革局、肇庆市教育局、肇庆市科技局、肇庆市工业和信息化局、肇庆市司法局、肇庆市科协、肇庆市计算机学会、肇庆市信息协会各个组织协办的数智赋能·安全同行”人工智能主题宣传活动在肇庆市工业贸易学校举行，紧扣国家《2026 年提升全民数字素养与技能工作要点》及全省全民数字素养与技能提升月统一安排，聚焦人工智能科普宣传，提升群众 AI 应用与安全防护意识，弥合数字鸿沟，让智能化更好服务生产生活。

17. 深圳市网络与信息安全行业协会联合承办深圳市 2026 年数字体验展暨鸿蒙生态体验活动

6 月 25 日—26 日，由深圳市委网信办主办的 2026 年深圳市全民数字素养与技能提升月主题活动——数字体验展暨鸿蒙生态体验系列活动在深圳湾科技生态园鸿蒙生态创新中心体验馆举办。活动围绕“数智赋能 全民共享”主题，立足深圳数字经济产业优势，通过沉浸式展览、实景场景体验、技术成果展示等多元形式，全方位展示深圳在数字经济发展、国产化智能生态构建、智慧场景落地应用等方面的丰硕成果，立体化呈现数智技术赋能城市发展、产业升级、民生提质的全新图景。

18. 金华市网商协会联合协办的创业政策及企业合规专场活动成功举办

6 月 25 日下午，由金华开发区组织人社部、浙江菁英电子商务产业园主办，金华市网商协会、金华市网络界人士联谊会等单位协办的菁英荟·创业沙龙——创业政策及企业合规专场活动，在浙江菁英电子商务产业园二楼会议室顺利开展。本次沙龙聚焦人社创业扶持、金税四期财税管理、企业法务风控三大企业经营核心刚需，旨在切实解决我市创业企业政策申领难、财税不合规、法律风险突出等经营痛点，助力广大网商企业吃透扶持政策、筑牢合规经营防线

19. 陕西省互联网协会受邀出席陕西太乙数字艺术研究院成立大会并深度参与研讨

近日，陕西太乙数字艺术研究院成立揭牌仪式暨 AI 数字艺术人才培养专题研讨会顺利举办。陕西省互联网协会受邀参会，与省民政厅、省社科联、文化科技企业、高校艺术院所代表齐聚现场，全程参与揭牌、行业研讨等系列环节，围绕数字技术与文化艺术融合、AI 数字人才培育、数字文创产业协同发展开展深度交流，为我省文化强省、数字经济协同发展建言献策。

活动现场，省民政厅社管局、省社科联社会组织管理部相关负责人发表致辞。当前数字文创技术迭代加速，传统艺术、影视设计行业迎来全面技术重构，数字艺术复合型人才缺口持续扩大。研究院计划打造五大核心平台，覆盖数字艺术产业智库、作品数智转化、专业人

才培养、非遗海外数字传播、文化数智场景创新，构建从理论研发、内容创作、版权保护到市场运营、国际传播的完整产业闭环，秉持规范化、市场化、国际化发展理念，联动行业专家、高校、头部文化科技企业协同运营。

20. 陕西省信息网络安全协会赴省公安厅网安总队开展交流学习活动

2026 年 7 月 1 日，协会组织班子成员赴省公安厅网安总队开展交流学习。网安总队唐洁支队长、张轩大队长、叶宗祥党建指导员等人出席座谈，协会淡战平会长、张成秘书长等一行参会，围绕政策文件学习、党建工作、协会业务发展三项内容深入研讨。

本次汇报学习，既是一次政策理论充电、党建思想淬炼，更是一次全面对标监管要求、校准工作方向的业务对接。下一步，协会将系统梳理本次座谈交流内容，不折不扣落实四份文件相关工作部署，建立与省公安厅网安总队常态化沟通汇报机制，始终坚持党建引领业务发展，严格按照行业主管部门工作部署优化各项行业服务，切实履行行业自律职责，携手守护全省信息网络安全稳定。