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8月第8期（总第37期）

2026年8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 8 月第 8 期（总第 37 期）

2026 年 8 月 12 日

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：7 月，平台经济治理、网络暴力治理、互联网信息服务监管以及数据资源开发利用成为中央和地方政策制度建设的重要着力点。相关制度一方面持续压实网络平台主体责任与减轻小型个人信息处理者合规负担并存，体现安全与发展平衡的立法思路，另一方面加快完善数据产权登记、公共数据授权运营和政务数据共享等基础规则，筑牢数据价值释放制度保障。

部委层面，国家互联网信息办公室发布《中华人民共和国反网络暴力法（征求意见稿）》，对网络暴力概念、治理机制、平台责任、政府治理、社会共治和司法保护作出系统规定，要求网络服务提供者加强网络暴力监测识别、信息溯源和人工智能生成传播风险防控。市场监管总局、商务部发布《电子商务法（修正草案征求意见稿）》，拟建立平台经济工作协调机制，完善新业态电子商务平台经营者义务、域外适用和执法协作制度等。国家互联网信息办公室发布《互联网信息服务管理办法（修订草案征求意见稿）》，增设平台信息服务和智能信息服务专节，强化账号管理、内容治理、网络暴力防范和人工智能服务安全等。国家互联网信息办公室、公安部发布《小型个人信息处理者个人信息保护简化措施规定》，对处理不满 10 万人个人信息的处理者适用简化合规要求，明确个人信息处理规则的简便公开方式，并细化轻微违法、初次违法不予处罚或者可以不予处罚的情形。国家数据局公布《数据产权登记工作指引（试行）》，从登记机构资质、登记程序和审查

责任等方面规范数据产权登记，要求登记机构对数据来源合规性和数据产权明确性进行合理审慎审查。

地方层面，北京印发《北京市公共数据资源授权运营管理办法》，建设统一授权运营管理服务平台，对授权管理、合规审核、运营监管和安全管控实施全流程管理，并明确公共数据纳入授权运营范围的条件。宁夏出台公共数据资源授权运营实施方案，试行整体授权模式，对数据开发利用实行“一场景、一申请”，优先推动民生、产业和战略价值较高的公共数据资源开发利用。四川印发政务数据共享实施细则，建立统一目录和在线供需对接机制，明确共享申请、审核、答复和使用流程，并将数据分类分级、保密风险评估和个人信息保护影响评估纳入目录管理等。

关键词：平台经济；网络暴力治理；互联网信息服务；小型个人信息处理者；数据产权

（一）部委层面动向

1. 市场监管总局、商务部发布《电子商务法（修正草案征求意见稿）》

7月4日，市场监管总局、商务部发布《电子商务法（修正草案征求意见稿）》，提出二十条修改意见，包括新增构建监管合力工作机制、新业态电子商务平台经营者相应义务、域外适用等条款。

修正草案征求意见稿提出，将现《电子商务法》第六条作出修改，建立监管合力工作机制，规定国家有关部门按照线下线上业务归口管理一致原则，依据部门职责分工负责电子商务发展促进、监督管理等工作。国务院建立平台经济工作协调机制，明确综合监管牵头部门。

修正草案征求意见稿提出增加比例罚，在现《电子商务法》第八十五条之后增加一条，规定电子商务平台经营者违反本法第二十七条、第二十九条、第三十五条、第三十八条等规定，情节特别严重、影响特别恶劣、造成特别严重后果的，由国务院市场监督管理等部门依职责责令停止违法行为，没收违法所得，处以相关经营者上一年度营业额百分之五以下的罚款。

修正草案征求意见稿提出增加梯次监管工具，在现《电子商务法》第八十五条之后增加一条，规定电子商务平台经营者未依法履行法定责任和义务，扰乱或者可能扰乱网络市场秩序的，有关主管部门可以采取约谈整改、专项调查、出具警示函等措施。有关主管部门调查涉嫌违反本法行为，电子商务经营者等主体应当配合。（来源：国家市场监督管理总局）

2. 国家互联网信息办公室发布《中华人民共和国反网络暴力法（征求意见稿）》

7月29日，国家互联网信息办公室发布《中华人民共和国反网络暴力法（征求意见稿）》，共七章六十条。

征求意见稿拟规定以下七方面内容：（1）明确网络暴力概念定义和治理原则。对网络暴力内涵外延进行界定，拟规定网络暴力是指通过网络对个人、组织集中或者持续实施的侵害名誉权、荣誉权、隐私权、肖像权、个人信息等合法权益的活动；（2）规定网络暴力治理体制机制；（3）压实网络暴力治理平台责任。要求网络服务提供者建立健全网络暴力监测识别机制和防护功能，发现存在利用人工智能技术制作、复制、发布、传播网络暴力信息或者实施其他网络暴力活动风险的，应当采取相应措施、开展信息溯源，并向有关部门报告。明确大型网络平台的网络暴力治理特殊义务；（4）优化网络暴力政府治理。规定国家网信部门会同国务院公安、教育、电信、民政、文化和旅游、卫生健康、广播电视等有关部门建立网络暴力治理机制，对网络暴力进行分类治理；（5）深化网络暴力社会共治；（6）加强网络暴力司法保护；（7）明确法律责任。（来源：中央网信办）

3. 国家文物局发布《国有文物资源数据管理办法》

6月9日，国家文物局发布《国有文物资源数据管理办法》，自2026年11月1日起施行。《办法》共九章三十三条，包括数据采集、数据加工、数据存储等内容。

《办法》规定，国有文物管理机构应通过自主采集或委托采集的方式进行数据采集。数据采集应符合文物数字化采集技术标准，由具备专业技术能力、文物安全知识的人员执行，并签署数据保密承诺书。所采集原始数据应及时校验和移交，受委托机构、工作人员个人不得擅自留存和使用。可移动文物应在国有文物管理机构内采集。已采集的原始数据能够满足数据使用要求的，不得重复采集。

《办法》提出，数据加工应符合文物数据加工技术标准，明确加工场所，部署完善的物理安全防护设施，采取访问控制、操作审计等管控措施。所加工数据应及时移交，受委托机构、工作人员个人不得擅自留存和使用，加工过程中所产生的临时、缓存数据及文件等应及时删除。（来源：国家文物局）

4. 国家数据局综合司公布《数据产权登记工作指引（试行）》

7 月 1 日，国家数据局综合司公布《数据产权登记工作指引（试行）》，共六章四十二条，包括登记机构、登记程序、登记类型以及法律责任。

《指引》提出，登记机构应当具备以下基本条件：（1）在境内依法成立、运营状况良好的企事业单位法人，其中企业法人的实缴注册资本不得低于一亿元，事业单位法人应当具备与其开展登记业务相适应的经费保障；（2）有固定办公场所及满足业务需求的基础设施；（3）有二年以上数据登记或数据流通相关服务经验；（4）有完善的治理结构、登记业务管理制度、登记审查人员管理制度、数据安全管理制度、数据安全风险处置预案和服务退出保障预案；（5）配备专职审查团队，专职审查团队成员应当具备数据、法律等相关领域的专业能力和三年以上工作经验；（6）建成支撑数据产权

登记业务的信息系统，完成信息系统网络安全等级保护三级或以上备案，具备与国家数据产权登记服务系统对接的基础条件；（7）近三年内无不正当竞争、经营异常等行为，且无重大违法违规记录。

《指引》规定，登记机构受理数据产权登记申请后，应当对数据描述的准确性、数据来源的合规性、数据产权的明确性等进行合理审慎的审查。登记机构可以要求登记申请人补充佐证材料，必要时可以向利害关系人或其他有关主体核实。登记申请人无法补充佐证材料且登记机构无法通过合法渠道核实的，可终止登记。（来源：国家数据局）

5. 国家互联网信息办公室发布《互联网信息服务管理办法（修订草案征求意见稿）》

7 月 3 日，国家互联网信息办公室发布《互联网信息服务管理办法（修订草案征求意见稿）》，共六章九十四条，拟对《办法》作全面修改完善。

修订草案征求意见稿主要修订内容如下：（1）明确原则要求和管理机制；（2）完善互联网信息服务提供者管理要求。进一步完善准入条件、规范网络资源使用、强化从业人员管理等；（3）强化互联网信息服务活动管理规定。进一步加强用户账号管理、完善网络信息内容规范等，并针对特定情形新增制度要求；（4）压实网络平台主体责任。增设“平台信息服务”专节，要求具有较大影响力的互联网用户公众账号生产运营者不得制作、复制、发布、传播含有法律、行政法规禁止内容的信息和不良信息，规定加强网络暴力识别监测，发现存在网络暴力风险等情况应当及时采取相关措施，并为用户提供快捷取证等功能。规范对互联网信息内容多渠道分发机构签

约账号及其发布信息的管理等；（5）促进智能信息服务安全和发展。增设“智能信息服务”专节，对应用人工智能技术提供互联网信息服务的情形进行专门规范；（6）健全法律责任制度和监管措施“工具箱”。结合互联网治理实践，建立互联网领域严重失信主体名单管理制度，增设完善限制账号功能、禁止注册新用户账号等管理措施。（来源：网信中国）

6. 国家金融监督管理总局发布《银行业保险业网络安全管理办法（征求意见稿）》

7 月 10 日，国家金融监督管理总局发布《银行业保险业网络安全管理办法（征求意见稿）》，共八章七十二条，包括网络安全治理、网络安全建设和运行管理、网络安全风险监测等内容。

征求意见稿规定，金融机构审计部门负责网络安全审计，制定网络安全审计计划，开展网络安全审计工作，提出整改意见，并推动整改落实。必要情况下，可委托第三方机构对网络安全进行审计和评价，并向金融监管总局或者其派出机构报送外部审计报告。

征求意见稿提出，金融机构应制定符合业务和科技发展需要的网络安全建设规划，网络关键节点、重要电力及通信线路、重要设备设施应当采取冗余备份措施，网络带宽和设备性能应当能够满足业务高峰期需求，应当确保网络安全保护措施与信息化建设“同步规划、同步建设、同步使用”。（来源：国家金融监督管理总局）

7. 《国家网络身份认证公共服务管理办法》实施一周年，已提供网络身份认证 2.8 亿次

7 月 15 日，公安部等六部门联合发布的《国家网络身份认证公共服务管理办法》正式施行满一周年。一年来，国家网络身份认证公共服务以自愿、免费为原则，积极服务相关行业领域发展，在便民利企、保护公民个人信息方面取得显著成效。

在服务覆盖方面，截至目前，已免费为 400 余家行业主管部门、地方政府部门、企事业单位以及大型互联网平台提供身份认证服务，接入各类 App、小程序、网站 530 余个。国家网络身份认证 App 下载量达 9000 万次，4000 万人申领数字身份，提供网络身份认证 2.8 亿次，解答社会各界咨询 360 万条。制度保障体系同步完善，一年来已有 8 部法律法规、部门规章或规范性文件明确提及或鼓励优先使用该项服务，累计 25 个相关法律法规、部门规章或政策文件将国家网络身份认证公共服务写入具体条款。此外，1 项国家标准、6 项行业标准相继发布，规范了应用单位对接公共服务的要求、流程和技术接口。国家网络身份认证 App 和系统平台累计发布 19 个版本更新，推出轻量化小程序端降低使用门槛，完善个人信息授权使用保护机制。

在应用领域拓展方面，互联网领域，微信、QQ、微博、淘宝、京东、拼多多、百度、快手、美团、滴滴、小红书、抖音等主流互联网平台均已实现网络身份认证一键登录；微信、闲鱼、优酷、腾讯视频、腾讯新闻等已在账号安全等身份认证场景应用，平台不再获取网民真实身份信息，实现了“实名不显名”。政务服务领域，国家政务服务平台以及北京、山东等 17

个省市级政务服务应用，国家税务总局、国家市场监管总局、住房和城乡建设部等部委相关政务系统陆续接入。金融服务领域，工、农、中、建、交、邮储六大国有银行及中国人寿、人保集团等头部保险机构已接入服务。医疗健康领域，北京协和医院 App 已对接服务，新疆医保平台也已上线应用。中国联通、中国移动手机营业厅及部分线下营业厅、邮政寄递实名认证、网上国网等场景均可使用。（来源：公安部网安局）

8. 国家互联网信息办公室、公安部发布《小型个人信息处理者个人信息保护简化措施规定》

7 月 22 日，国家互联网信息办公室、公安部发布《小型个人信息处理者个人信息保护简化措施规定》，共二十二条，自 2026 年 9 月 1 日起施行。

《规定》明确，所称小型个人信息处理者，是指处理不满 10 万人个人信息的个人信息处理者。《规定》提出，小型个人信息处理者个人信息处理规则至少应当包括下列内容：（1）小型个人信息处理者名称或者姓名；（2）个人行使权利的受理部门或者人员及联系方式；（3）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限等。小型个人信息处理者线下收集个人信息的，可以通过在经营场所醒目位置张贴公告等简便方式公开个人信息处理规则；线上收集个人信息的，可以通过服务协议、产品服务客户端弹窗和网站公告等方式公开个人信息处理规则。

《规定》强调，小型个人信息处理者开展个人信息处理活动有下列情形之一的，应当不予处罚：（1）违法行为轻微并及时改正，没有造成危害后果的；（2）有证据足以证明没有主观过错的，法律、行政法规另有规定的，

从其规定；（3）其他依法不予处罚的情形。小型个人信息处理者开展个人信息处理活动，初次违法且危害后果轻微并及时改正的，可以不予处罚。依法不予处罚的，履行个人信息保护职责的部门应当视情采取约谈、发送提示函等监管措施。（来源：网信中国）

（二）地方层面动向

1. 宁夏回族自治区人民政府办公厅印发《宁夏回族自治区公共数据资源授权运营实施方案》

6 月 25 日，宁夏回族自治区人民政府办公厅印发《宁夏回族自治区公共数据资源授权运营实施方案》，包括授权运营模式、运营机构的选择、授权运营公共数据资源范围及目录等。

《方案》提出，全区公共数据资源授权运营工作在试行期间采取整体授权模式，数据开发商开发利用公共数据采取“一场景、一申请”方式进行。《方案》强调，自治区公共数据资源授权运营优先开展与民生紧密相关、行业增值潜力明显、产业战略意义重大的数据资源。第一批拟授权运营的公共数据资源主要为发展改革、工业和信息化、公安、卫生健康、教育等行业公共数据。数据资源目录实施动态更新机制，在授权运营过程中，如现有数据资源无法满足应用需求，运营机构可向实施机构提出补充完善数据资源的申请。申请中应明确所需数据的业务场景、预期用途、数据字段、更新频率等具体内容，实施机构会同数源单位评估后，报管理机构审核。审核通过后，实施机构组织落实数据资源的补充和更新。（来源：宁夏回族自治区人民政府）

2. 广东省政务服务和数据管理局等 11 部门印发《广东省推进城市全域数字化转型 建设智慧城市行动方案》

6 月 30 日，广东省政务服务和数据管理局、中共广东省委社会工作部、中共广东省委政法委员会等 11 部门印发《广东省推进城市全域数字化转型建设智慧城市行动方案》，围绕打造城市全域数字化转型重点场景、筑牢城市全域数字化转型坚实底座、激活城市全域数字化转型内生动力三个方面，提出 21 项措施。

筑牢城市全域数字化转型坚实底座方面，《方案》提出健全安全保障体系：一是提升网络安全防护能力。鼓励构建统一安全运营服务模式，集约化管理城市网络安全。完善云网边端纵深防御体系建设，建立边界网络访问控制与态势感知机制，强化应用安全性评估与定期安全检查；二是强化数据安全防护能力。加强城市数据基础设施安全保障，实现可信接入、安全互联、跨域管控、全栈防护。构建端到端数据信任闭环与全流程监管体系，健全数据分类分级管理、大模型应用安全管理、安全风险评估及应急处置等机制。

激活城市全域数字化转型内生动力方面，《方案》提出探索体制机制创新。鼓励有条件的地市构建场景导向、数据驱动的城市综合治理体制，创新跨部门数据合作机制。深化网格化管理，完善矛盾隐患排查预防机制。探索建立场景创新孵化机制，强化应用场景培育开放。探索粤港澳大湾区智慧城市群共建机制，推动“百千万工程”数字化应用跨区域协同创新。（来源：广东省政务服务和数据管理局）

3. 北京市政数局印发《北京市公共数据资源授权运营管理办法》

7 月 2 日，北京市政务服务和数据管理局印发《北京市公共数据资源授权运营管理办法》，自印发之日起施行。《办法》共八章三十六条，包括职责分工、授权管理、数据基础设施等内容。

《办法》规定，北京市建设统一的公共数据资源授权运营管理服务平台等共性基础设施，为公共数据资源授权运营管理提供安全可控环境，实现授权管理、合规审核、运营监管和安全管控等全流程管理，确保公共数据资源开发利用过程可管、可控、可追溯。

《办法》提出，北京市数据管理部门指导实施机构编制公共数据资源授权运营目录，对不危害国家安全、公众利益，不侵犯商业秘密和个人隐私、个人信息权益，以及法律法规未禁止共享的公共数据资源，纳入授权运营范围，并通过数据接口、匿名化处理、隐私保护计算等方式向运营机构授权使用。以政务数据共享方式获得的国家部委或其他地区公共数据，用于授权运营的，应征得数据提供单位同意。对不同意纳入授权运营范围的，数据提供部门应说明理由和依据。（来源：北京市政务服务和数据管理局）

4. 四川省政府办公厅印发《四川省政务数据共享实施细则》

7 月 3 日，四川省人民政府办公厅印发《四川省政务数据共享实施细则》，自 2026 年 7 月 15 日起施行。《细则》共七章三十八条，包括管理体制、目录管理、共享使用等规定。

《细则》规定，政务数据实行统一目录管理。省级政务数据共享主管部门按照统一标准规范，组织编制省级政务数据目录。市（州）、县（市、区）

政务数据共享主管部门按照统一标准规范，组织编制本行政区域内政务数据目录。政府部门应当依照本部门职责，按照统一标准规范编制本部门政务数据目录，依法开展保密风险评估、个人信息保护影响评估等，并经部门首席数据官审核同意。政务数据目录应当包括目录名称、数据项、提供单位、数据格式、数据更新频率以及共享属性、共享方式、使用条件、数据分类分级、所在层级等内容。

《细则》提出，政务数据共享主管部门应当建立健全政务数据共享供需对接机制，指导政府部门依托一体化数据平台实现政务数据共享在线供需对接，明确政务数据共享申请、审核、答复、提供等工作流程。政务数据需求部门应当根据履行职责需要，按照统一发布的政务数据目录，经本部门首席数据官确认同意后，依法在线提出真实、合法和必要的政务数据共享申请，并明确使用依据、使用场景、使用范围、共享方式、使用时限等。政务数据提供部门对政务数据需求部门提出的政务数据共享申请进行审核，审核结果经本部门首席数据官或者数据执行官同意后作出答复。（来源：四川省人民政府）

5. 江苏省发布《江苏省未成年人保护条例（修订草案）》

7 月 31 日，江苏省发布《江苏省未成年人保护条例（修订草案）》，共九章八十三条，包括网络保护、政府保护、司法保护等内容。

网络保护方面，修订草案提出，网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当针对不同年龄阶段未成年人使用其服务的特点，按照国家有关规定和标准，设置未成年人模式，完善网络社区规则和用

户公约，引导规范未成年人的网络行为，遏制网络不良信息传播；不得以打赏排名、虚假宣传等方式诱导未成年人盲目追星、盲目消费，不得违反规定向未成年人提供现金充值、在线支付等打赏服务。严禁未成年人参与网络低俗表演、网络不良社交等活动。网络游戏服务提供者应当利用电子身份认证等技术，识别参与网络游戏的未成年人身份，不得以任何形式向未实名注册和登录的未成年人提供网络游戏服务。

政府保护方面，修订草案提出，网信、教育、公安等部门应当加强对未成年人的个人信息保护，指导、监督个人信息处理者规范未成年人个人信息的收集、存储、使用、加工、传输、提供、公开、删除等，防止未成年人的个人信息泄露。（来源：江苏省人大）

境内前沿观察二：治理实践

导读：7 月，公安机关、网信部门、通信管理部门等围绕个人信息保护、网络犯罪打击、网络内容生态治理和网络数据安全持续推进专项治理，治理重点进一步向恶意程序攻击、网络舆情敲诈、短视频虚假摆拍、未成年人网络保护以及人工智能生成不良内容等突出问题延伸。

公安机关方面，围绕网络黑客犯罪、网络谣言、网络暴力、侵犯个人信息和网络水军等违法犯罪活动持续加大打击力度。公安部公布 2026 年上半年网络空间治理成果，全国公安机关累计侦办网络黑客犯罪案件 1900 余起、网络谣言案件 8000 余起、网络暴力案件 2000 余起，清理违法有害信息 50 万余条等。浙江杭州、上海浦东、湖南蒸湘等地公安机关分别查处“银狐”木马攻击、利用黑客技术批量爬取企业数据和 DDoS 攻击案件；广东河源公安机关打掉利用人工智能体操控网络账号、制造负面舆情并实施敲诈的犯罪团伙，反映出公安机关对恶意程序产业链、企业数据窃取和人工智能技术辅助网络犯罪等新型风险持续保持严打态势。

网信部门方面，围绕短视频内容标注、未成年人网络保护、网络娱乐团播等问题持续开展专项整治。中央网信办部署“清朗·网络娱乐团播乱象整治”专项行动，重点治理违规 PK 刺激打赏、低俗团播内容、侵害未成年人权益及 MCN 机构管理失范等问题。中央网信办同时启动未成年人网络保护专项行动，集中整治利用 AI 技术恶搞动画形象、批量制作猎奇审丑 AI 短剧、AI 软件输出低俗内容以及教授未成年人利用 AI 换脸破解人脸识别等问题，并推动平台规范算法推荐和未成年人模式建设。围绕汛

期灾害和国内外时事信息，网信部门进一步强化信息来源标注和谣言治理，集中处置未标注、错标漏标及拼凑剪辑、夸大歪曲事件的信息内容，体现出网络内容治理正由事后删除处置向信息标注、来源溯源和平台推荐机制规范延伸。

通信管理部门方面，上海、浙江通信管理局分别部署电信和互联网行业网络和数据安全检查，将关键信息基础设施、云平台、工业互联网、车联网、数据服务平台和移动应用等纳入检查范围，重点检查网络和数据安全保障体系、重要数据目录管理、风险评估、对外共享、威胁监测和事件应急处置等情况，推动行业治理由单一 App 合规检查向网络、系统、平台和数据全链条安全监管拓展。

其他部门和司法实践方面，最高人民检察院公布 2026 年上半年检察工作情况，全国检察机关起诉利用网络实施的犯罪 7.7 万人，其中起诉电信网络诈骗犯罪 3.2 万人、侵犯公民个人信息犯罪 2641 人等。

关键词：网络内容治理；网络犯罪；未成年人网络保护；网络和数据安全

（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通报 72 款违法违规收集使用个人信息的移动应用

7 月 9 日消息，经国家计算机病毒应急处理中心检测，2026 年 5 月 20 日至 2026 年 6 月 22 日期间，72 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。

1. 24 款移动应用在 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。

2. 37 款移动应用隐私政策未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等。

3. 14 款移动应用个人信息处理者向其他个人信息处理者提供其处理的个人信息的，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；App 客户端向第三方提供个人信息，未经用户同意，未做匿名化处理。

4. 2 款移动应用未在征得用户同意后才开始收集个人信息或打开可收集个人信息的权限。

5.5款移动应用未提供有效的更正、删除个人信息及注销用户账号功能；为更正、删除个人信息或注销用户账号设置不必要或不合理条件；虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内完成核查和处理。

6.3款移动应用投诉、举报未在承诺时限内受理并处理；个人信息处理者未建立便捷的个人行使权利的申请受理和处理机制。

7.13款移动应用未向用户提供撤回同意收集个人信息的途径、方式；个人信息处理者未提供便捷的撤回同意的方式。

8.1款移动应用未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

9.3款移动应用个人信息处理者处理不满十四周岁未成年人个人信息的，未制定专门的个人信息处理规则；收集未成年人信息未取得监护人单独同意。

10. 1款移动应用个人信息处理者向境外提供个人信息的，未向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

11. 17款移动应用未采取相应的加密、去标识化等安全技术措施。

12. 1款移动应用实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，将人脸识别技术作为唯一验证方式。个

人不同意通过人脸信息进行身份验证的，未提供其他合理、便捷的方式。

13. 4款移动应用无隐私政策。（来源：公安部网安局）

2. 公安部公布2026年上半年网络空间治理成果，清理违法有害信息50万余条

7月11日，公安部发布2026年上半年网络空间治理成果。据统计,2026年以来全国公安机关累计侦办网络黑客犯罪案件1900余起、网络谣言案件8000余起，关停违法违规账号2.3万余个，清理违法有害信息50万余条。

在平台治理方面，针对用户数量庞大的超大型互联网平台，各地公安机关网安部门全面推进“线上巡查、线下核查”工作，2026年以来共办理网络信息安全领域违法行政案件947起，依法约谈企业108家次，出具风险提示函76份。

在个人信息保护方面，公安部会同中央网信办等部门深入推进系列专项行动，2026年以来公开曝光违法违规收集使用个人信息移动App470款，下架整改不到位移动App139款。同时加快国家网络身份认证公共服务在互联网平台和政务、金融、交通、文旅、考试等领域的推广应用，目前已对接应用500余款、提供匿名认证服务1.2亿余次。

信息内容治理方面，聚焦造谣引流、刷量控评、舆情敲诈、有偿删帖等网络水军违法犯罪活动，持续开展严厉打击。北京公安机关打

掉刷单炒信、刷单骗补犯罪团伙 11 个，湖北公安机关打掉有偿刷量控评、刷单炒信犯罪团伙 2 个。依法严打网络暴力，聚焦网上侮辱谩骂、造谣诽谤、侵犯隐私等各类活动，全链条打击网暴发起者、组织者、实施者，2026 年以来累计侦办此类案件 2000 余起，依法查处体育运动员、抗洪救灾村干部被网暴案等多起典型案件，加大震慑力度。

依法严打仿冒网站和软件方面，精准识别仿冒国家部委及各级党政机关网站，全链条查处虚假认证、制售假证、网络诈骗等各类违法犯罪活动，2026 年以来累计侦办相关案件 65 起，封堵关停 105 个仿冒网站。（来源：公安部）

3. 浙江杭州网安破获一起“银狐”木马案，十二家电商企业遭受定向攻击

6 月 29 日，据央视新闻报道，浙江杭州市公安局网安部门近日破获一起专门针对电商企业的“银狐”木马病毒案件，共有 12 家电商企业遭到同一木马程序攻击。

本案中，嫌疑人冒充普通顾客，以线上咨询为名向电商客服发送伪装成商品款式需求等内容的文件包。客服人员一旦点击，木马即植入计算机并获取控制权限。据警方介绍，“银狐”木马是专门针对企事业单位管理、财务等从业人员设计的恶意程序，犯罪分子通过即时通信软件发送钓鱼信息实施“投毒”，进而窃取敏感数据和财产。

该犯罪团伙内部分工明确，技术人员负责制作和更新木马，销售人员通过境外聊天软件寻找下家，老板则负责整体统筹。木马售出后，

团伙通常会提供 7 天至 30 天的后续维护服务，在此期间不断更新以规避杀毒软件检测。木马销售单价约在 1 万至 1.8 万元之间，团伙累计违法所得达 110 余万元。

杭州网安部门近年来持续严厉打击涉“银狐”木马黑灰产犯罪活动，至今已成功打掉 4 个犯罪团伙，抓获犯罪嫌疑人 34 名，查获木马样本 100 余个、源代码文件 3 万余个，涉及全国被侵害电脑设备 3000 余台。（来源：公安部网安局）

4. 广东河源公安打掉一个利用网络舆情实施敲诈的犯罪团伙

7 月 2 日消息，广东省河源市公安局近日成功打掉以李某军为首的利用网络舆情实施敲诈犯罪团伙，抓获犯罪嫌疑人 12 人。

经查，李某军团伙成立 MCN 机构（多频道网络机构），注册公司名称为“某文化传播有限公司”，实控多个微信公众号和微博账号，总粉丝量超千万。该团伙长期雇佣网络写手，搜罗、拼接各类明星八卦，利用某人工智能体控制其持有的多个大 V 账号发帖，在电视剧、综艺播放期间故意制造负面舆论热点。该团伙发帖制造负面舆论后，相关剧组方承受舆论压力，主动联系李某军协商删帖事宜。李某军借此要求电视剧播放平台或明星经纪公司购买其所谓的“护剧”服务，否则拒不删除负面网帖。

该团伙的“护剧”服务一般包括发送剧集正向宣传帖文、删除前期发布的相关明星负面帖文，以及承诺在剧集播出期间不再发布有关

剧集和明星的负面帖文等。该团伙通过操控多个大V账号，制造负面舆论、变相强迫影视方购买“护剧”服务等方式，利用网络舆情实施敲诈。调查发现，李某军团伙的MCN机构实施敲诈的受害方，涉及数名知名演员及多部热播电视剧发行方，前期已被多名艺人、多家经纪公司或影视出版方以名誉侵权为由起诉。李某军团伙严重扰乱影视行业正常宣发秩序，破坏网络舆情生态，侵害出品方（投资方）及艺人方合法权益。

查清全案后，河源市公安局赴8省、2市将该团伙骨干成员12人悉数抓捕归案。经审讯，李某军团伙对违法犯罪事实供认不讳。案件正在进一步侦办中。（来源：公安部网安局）

5. 湖南永州网警查处一起停车管理系统运营企业未履行个人信息保护义务案

7月3日消息，湖南永州冷水滩公安网安部门近日查处一起停车管理系统运营企业未履行个人信息保护义务的违法案件。

2026年6月，冷水滩公安网安部门在辖区内某停车运营管理企业开展网络安全专项检查时，排查发现该公司的停车管理系统存在数据安全风险隐患。经查，该企业在日常运营管理中，未建立个人信息管理制度和操作规范，相关从业人员未定期进行安全教育和培训，对用户数据也未采取相应的安全技术措施，存在数据泄露风险。目前，属地公安机关已依法对该公司不履行个人信息保护义务的行为作出行政处罚。（来源：公安部网安局）

6. 上海浦东警方破获一起非法获取计算机信息系统数据案

7 月 4 日消息，上海浦东警方近日破获一起利用黑客技术非法获取互联网企业数据案。

近日，某电商平台向警方报案称，公司经营系统后台出现大量异常访问，疑似有人利用技术手段批量爬取公司内部数据，相关数据泄露可能引发同行恶意竞争、企业信誉危机及用户隐私风险。根据报案人提供线索，浦东分局网安支队迅速抓获犯罪嫌疑人杨某某、孙某某、李某等 6 人。经查，杨某某为非法牟利，伙同孙某某等人，通过黑客技术绕过平台安全防护机制，劫持平台流量包数据，非法获取商品 ID、未公开的价格、库存规格等信息，并雇佣人员进行培训后大规模爬取平台数据非法出售牟利。

截止案发，杨某某、孙某某、李某等 6 人共出售相关数据百万余条，获利 50 余万元人民币。目前，杨某某、孙某某等 5 人因涉嫌非法获取计算机信息系统数据罪已被移送检察机关审查起诉，李某已被批准逮捕。（来源：上海网警）

7. 湖南蒸湘网安成功破获一起 DDoS 攻击案

7 月 14 日消息，湖南蒸湘网安成功破获一起 DDoS 攻击案。

2026 年 6 月，湖南蒸湘公安分局网络安全保卫大队接到辖区某游戏公司报警称：6 月 17 日，公司的网站及游戏服务器突然遭持续 DDoS 恶意流量攻击，造成系统资源被占满后服务器被迫启动了“黑洞模式”，导致软件无法正常运行致使企业运营受到严重影响。

接警后，该队在局领导部署安排下立即抽调精干力量成立专案组，开展案件侦破工作。期间，办案民警调取大量核心电子证据，经过多日不间断研判，并奔赴外省实施线下落地抓捕，于 7 月 10 日抓获涉案嫌疑人，成功破获了该起破坏计算机信息系统案件。

经审讯，涉案人员交代，其因私人纠纷出资购买攻击流量，对该游戏公司服务器发起 DDoS 攻击，以此达到报复企业的目的。目前，涉案嫌疑人已被采取刑事强制措施，案件还在进一步侦办中。（来源：湖南网警）

8. 中越执法合作取得新战果，一名涉嫌破坏计算机信息系统犯罪嫌疑人被押解回国

7 月 20 日消息，按照公安部统一部署，在我驻越南使馆全力支持以及越南公安部门积极配合下，山东省公安机关近日派出工作组赴越南成功接收某破坏计算机信息系统案首犯潘某君并将其押解回国。

2025 年 7 月，山东淄博公安机关在工作中发现，本地网民杨某搭建、维护多个钓鱼网站，诱导用户下载捆绑“银狐”木马病毒的软件安装包，非法控制受害人电脑，窃取用户信息，牟取非法利益。2025 年 7 月至 2026 年 5 月，公安机关深入侦查并开展多轮次集中收网，相继打掉多个涉案犯罪团伙。2025 年 8 月，案件主要犯罪嫌疑人潘某君潜逃至境外，自此销声匿迹。

2026 年 6 月 4 日，在我公安机关不懈努力下，在我驻越南使馆大力支持下，越南警方成功将潘某君抓获。与此同时，公安机关在广

东、广西等地同步开展集中收网行动，将该案其余 11 名犯罪嫌疑人一举抓获。6 月 6 日下午，潘某君被押解回国。（来源：公安部网安局）

9. 重庆公安机关 2026 年上半年打掉境内外电诈团伙 198 个

7 月 24 日，重庆市政府新闻办举行 2026 年全市反诈工作新闻发布会。据介绍，2026 年以来，重庆市电诈警情数、立案数、损失数同比分别下降 38%、36.4%、43%，破案数、涉案人员打击处理数同比分别上升 124.2%、43.9%，累计为群众守住超 8 亿元潜在被骗资金。

2026 年以来，重庆警方成功打掉境内外电诈犯罪团伙 198 个，彻底摧毁长期盘踞缅甸北部、严重危害我国公民生命财产安全的“徐老发”特大武装电诈犯罪集团；先后从柬埔寨、老挝押解 1800 余名涉诈人员回渝，其中 97.7%被依法逮捕。同时，重庆在全国率先实现涉诈资金返还全流程网办，平均返还周期从以前的 66 天缩短至现在的 31 天。群众只需要登录“渝快办”APP 就可以在线提交返还申请、查询办理进度，实现涉诈资金返还“零跑腿”。重庆市 2026 年已向受害群众返还被骗资金 1.97 亿元。（来源：公安部网安局）

（二）网信部门治理实践

1. 两部门部署开展网络平台涉志愿服务违规信息专项整治

6 月 19 日，中央网信办秘书局、中央社会工作部办公厅印发《关于开展网络平台涉志愿服务违规信息专项整治的通知》，决定自 2026

年6月下旬至8月下旬，集中开展为期2个月的网络平台涉志愿服务违规信息专项整治。

专项整治期间，重点清理处置七类涉志愿服务违规信息及相关网络账号：一是以各种形式售卖志愿服务时长、志愿服务证书；二是违背志愿精神的相关宣传内容。包括但不限于如何快速获得志愿服务时长；以参观研学、在线答题、捐书捐物、购买助农产品等非志愿服务活动或以截图发朋友圈、AI生成图片、拍照打卡等未实际开展志愿服务的行为，宣传可以获得志愿服务时长、志愿服务证书的信息、短视频等；三是容易误导学生和家长的相关宣传内容。包括但不限于入团、入党对志愿服务时长数量有硬性要求的虚假宣传，鼓吹志愿服务时长与各类评先评优、升学入职挂钩的不良宣传等；四是为各类商事活动招募志愿者，或有偿招募安保员、后勤人员等所谓的“志愿者”。将营利性活动包装成志愿服务活动招募志愿者；五是假冒、仿冒“地域+志愿”、“行业+志愿”等官方账号误导社会公众；六是商标、商业广告以及其他营利性活动中使用志愿服务标识；七是其他以“志愿者”、“志愿服务”、“志愿服务组织”等名义，在网上开展的违背社会公德、损害社会公共利益或他人合法权益，危害国家安全的活动或发表的不当言论等。（来源：网信中国）

2. 中央网信办部署开展“清朗·网络娱乐团播乱象整治”专项行动

7 月 1 日，中央网信办印发《关于开展“清朗·网络娱乐团播乱象整治”专项行动的通知》，在全国范围内开展为期 2 个月的“清朗·网络娱乐团播乱象整治”专项行动。

专项行动重点围绕娱乐团播整治以下 6 类问题：（1）团播账号注册使用违规；（2）团播之间或团播成员间违规 PK 刺激打赏；（3）运用不当团播玩法诱导打赏；（4）团播场景内容低俗不良；（5）团播侵害未成年人权益；（6）团播 MCN 机构管理失范。（来源：网信中国）

3. 中央网信办发布一批短视频内容标注不规范的账号和平台

7 月 10 日，中央网信办发布一批短视频内容标注不规范的账号和平台。据统计，2026 年 5 月部署推进短视频内容标注工作以来，各重点网站平台已累计清理违反标注规定的短视频 24.1 万余条，处置账号 2.1 万余个，对错标漏标的短视频进行纠正或补标 127.5 万余次。此次发布的典型行为包括：

一是针对部分账号未进行标注，演绎“残疾妻子再次怀孕”“重病患儿募捐求助”等剧情，利用残障人士形象卖惨，消费公众同情心问题，对“爱 I 满人间”“陪宁宝打怪中”等网络账号予以关闭处置。

二是针对部分账号未进行标注，以外卖员身份持续摆拍“单身父亲带娃送外卖”“带娃送外卖瘫坐路边”等场景，虚构“失散28年的女儿怀孕送外卖”“外卖骑手送餐途中不慎刮蹭百万级豪华汽车”等桥段，渲染悲情误导公众认知问题，对“贵州小洪6868”“洞房名猪”“香港浩南正能量生活记录”“娟子感恩有你”“乐在其中xy”等网络账号予以禁言或关闭处置。

三是针对部分账号未进行标注，演绎婆媳争吵冲突桥段，虚构“相恋五年双方因彩礼僵持不下”“三角恋争夺情人”等情节，刻意放大家庭或情感矛盾，激化社会焦虑问题，对“丁丁婆婆”“如意（婆媳日常）”“惠子不服气”“谷丹晨的日常”“欣欣宝贝”“芊芊（不负众望）”等网络账号予以禁言或关闭处置。

四是针对部分账号未进行标注，虚构“宾利车主高速救助被弃结婚新人”“登山者深山救助流浪女子”等见义勇为事迹，以及演绎伪造“揭秘零差评神店谁敢给差评”等内容，以虚假正能量骗取公众好感和信任问题，对“八宝粥”“桐桐要坚强”“杨丽2328”“一个小八哥”“澜珊倾听|科恩”等网络账号予以禁言或关闭处置。（来源：网信中国）

4. 中央网信办部署开展“清朗·未成年人网络保护”专项行动

7月20日消息，中央网信办近日印发通知，在全国范围内部署启动为期4个月的“清朗·未成年人网络保护”专项行动。

专项行动分两个阶段开展。第一阶段为“清朗·2026 年暑期未成年人网络环境整治”专项行动，抓住暑期关键时间节点，聚焦信息内容生产传播全流程、全链条，集中力量整治网上涉未成年人乱象问题，防范化解各环节潜在风险隐患，为未成年人欢度假期营造健康安全的网络环境。第二阶段为“清朗·整治侵扰未成年人身心健康的网络信息”专项行动，从严从细排查可能影响未成年人身心健康的各类乱象问题和突出风险，压实网站平台主体责任，规范网上信息内容呈现。

第一阶段重点整治三个环节的突出问题：一是发布环节问题。编造毒动画，利用 AI 技术恶搞经典动画形象，刻意放大暴力恐怖元素。发布窒息挑战等鼓动危险行为。包装炒作“神童转世”“早熟小美女”等，打造争议儿童人设。摆拍逃学旷课、厌学躺平等视频内容，宣扬不良价值观。批量炮制猎奇、审丑的 AI 短剧，误导未成年人认知。部分 AI 软件创设不良人设角色，输出暧昧、低俗内容。二是互动环节问题。以“找闺蜜”等为幌子，诱骗未成年人发送私密照片。部分群组以“二次元福利”为噱头，向未成年人定向传播色情漫画等违法内容。在未成年人出镜视频下发布性暗示表情包等黑话烂梗，对未成年人造成侵扰。以“暑期陪玩”等话术，诱骗未成年人进行软色情陪聊。开设“表黑墙”等版块，集纳曝光未成年人隐私信息，提供有偿代骂服务。三是营销环节问题。以招募内衣体验官等形式，诱导未成年人拍摄性感特写照片。部分直播间采取限量发售、绝版溢价等话术，诱导未成年人购买盲盒抽卡。部分商家利用暗语诱导售卖电子烟。部分平台装扮商城等环节提供软色情个性装扮内容。部分商家提供 AI

换脸等技术，教授未成年人破解人脸识别验证。利用“预售享优惠”等话术诱导未成年人转账汇款，实施网络诈骗。

第二阶段着力规范三个方面：一是规范平台推荐行为。按照《可能影响未成年人身心健康的网络信息分类办法》相关要求，持续排查平台推荐不良行为、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问题。指导平台优化算法推荐服务机制，不得设置诱导网络沉迷、过度消费等算法模型，不得利用“附近的人”“可能感兴趣的人”等功能诱导未成年人不良交友。二是规范学习教育版块。督促平台对经典儿童动画等内容采取更严格的审核标准，严处借“启蒙早教”等标签发布不良导向内容的网络账号。合理限制账号发布未成年人出镜内容时长频次，不得以学习分享等为名，要求未成年人频繁出镜、引流牟利，MCN 机构不得利用旗下账号包装炒作网红儿童等。三是规范未成年人模式建设。排查未成年人模式进入、退出核验情况，模式下是否存在诱导打赏、投票打榜等易沉迷功能，模式下是否存在不良导向内容等情况。深入排查应用商店未成年人专区是否存在违规有害、年龄不适等 APP。针对儿童智能手表等专属设备，排查整治互动聊天、输入法等环节存在有害内容，第三方 APP 诱导充值消费、输出违法不良信息等问题。（来源：网信中国）

5. 中央网信办、应急管理部部署开展汛期灾害事故违法不良信息集中清理整治

7 月 23 日消息，中央网信办和应急管理部近日联合印发通知，在全国范围内部署开展汛期灾害事故违法不良信息集中清理整治。《通知》重点整治五类突出问题：一是移花接木与恶意剪辑类问题。二是旧闻翻炒与历史嫁接类问题；三是夸大其词与虚构数据类问题；四是编造险情与冒充权威类问题；五是技术伪造与借机诈骗类问题。（来源：网信中国）

6. 国家互联网信息办公室发布《国家信息化发展报告（2025 年）》

7 月 24 日，国家互联网信息办公室发布《国家信息化发展报告（2025 年）》，系统总结 2025 年各地区各有关部门推进信息化发展成效。

《报告》指出，2025 年是“十四五”收官之年，《“十四五”国家信息化规划》各项目标任务顺利完成，网信科技创新取得新突破，基础支撑能力实现新提升，产业生态建设取得新进展，信息化重点应用取得新成效，法规制度建设迈出新步伐，网络空间合作实现新拓展，实现信息化发展从重点突破到全面赋能的迈进。

《报告》分析了 2025 年国家信息化发展情况网络问卷调查结果。调查显示，受访网民普遍认为，人工智能等网络信息技术更加深入广泛融入日常生活，持续拓宽学习渠道、提升工作效能、改善生活品质，

让人民群众在信息化发展中有更多获得感、幸福感、安全感；受访网信企业表示，积极推进技术创新、人才培育和市场拓展，进一步提升企业产品服务的市场竞争力。

《报告》认为，“十五五”时期是网络强国建设夯实基础、全面发力的关键时期。信息化迈向数字化、网络化、智能化全面跃升的新阶段，数字化转型持续加速，网络化协同深入拓展，智能化升级不断涌现，信息化对经济社会高质量发展的赋能作用、倍增效应更加凸显。要锚定网络强国建设目标，把握好当前和长远、整体和局部、开放和自主、发展和安全的关系，以战略规划为牵引，以科技创新为动力，以产业生态为核心，以基础设施为支撑，以重点应用为关键，以法规标准为保障，健全完善信息化工作体系，体系化深层次推进“十五五”信息化发展，以信息化赋能高质量发展，奋力开创网络强国建设新局面。（来源：中国网信网）

7. 国家网信办发布2026年7月数据出境安全管理政策法规问答

7月24日消息，国家互联网信息办公室对近期收到的咨询问题发布答复，对以下三个问题进行答复：（1）个人信息处理者向境外提供个人信息，应如何有效履行告知同意义务；（2）已通过数据出境安全评估的，申请延长评估结果有效期应当符合哪些条件；（3）人员招聘场景中，如何判断境内求职者简历出境的必要性。

其中，关于个人信息处理者向境外提供个人信息，应如何有效履行告知同意义务的问题。国家网信办指出，个人信息处理者向境外提供个人信息的，应当履行告知、取得个人单独同意等义务。告知内容包括：境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项。同时，根据《个人信息保护法》第三十条规定，如向境外提供的是敏感个人信息，还应当向个人告知出境敏感个人信息的必要性以及对个人权益的影响。个人信息处理者取得个人单独同意个人信息出境，应当具体明确，不得与其他个人信息处理活动捆绑，不得采取“一揽子”授权方式取得同意。取得个人单独同意的方式可参考GB/T 42574-2023《信息安全技术 个人信息处理中告知和同意的实施指南》，采用书面签署、弹窗确认、邮件短信回复等方式开展。个人信息出境活动属于《个人信息保护法》第十三条第一款第二项至第七项规定情形的，不需取得个人同意，但仍应履行个人信息出境告知义务。（来源：网信中国）

8. 中央网信办通报“自媒体”未规范标注信息情况，并发布典型案例

7月27日消息，网信部门近日督导网站平台推进信息来源标注工作，发现一些“自媒体”在发布涉国内外时事相关内容时，未规范标注信息来源，混淆视听，严重误导公众认知。期间，督促网站平台依法依约处置违规账号3704个，纠正错标漏标短视频4.8万余次。

中央网信办同步通报三起典型案例：（1）抖音“致静”、快手“大秦说书”等“自媒体”账号，以直接搬运或简单整合方式，发布国际时事信息，未标注信息来源，网民无法溯源信息原始出处。涉及的账号已被依法依约处置；（2）微博“骑着电驴去荡圩”、快手“路路讲局势”等“自媒体”账号，发布国内外时事时模糊标注信息来源，使用“网传”“网友爆料”“外媒消息”等表述刻意规避审核，网民难以辨别信息真实性。涉及的账号已被依法依约处置；（3）抖音“全球”、哔哩哔哩“军武司令猿”等“自媒体”账号，以“雷霆出击”“又打起来了”等夸张表述作为标题、封面文字，配以国际时事资料画面，或是拼凑剪辑网络图片、视频，片面、歪曲解读相关事件，未标注信息来源，博取网民“眼球”、误导网民认知。涉及的账号已被依法依约处置。（来源：网信中国）

9. 网信、公安等部门联动打击六月网络谣言，重点整治汛情灾害、教育考试及民生政策领域三类乱象

7 月 2 日，中央网信办发布 2026 年 6 月网络谣言治理情况。6 月，网络谣言主要集中在汛期防灾、教育考试、民生政策等领域，呈现出拼接素材、蹭炒热点、虚构事件的特征，误导公众认知、干扰防汛救灾工作、扰乱正常社会秩序。网信、公安等部门快速响应、联动核查，及时发布权威辟谣信息，依法打击、曝光造谣传谣行为，全力护航高考中考平稳有序、为防汛救灾工作顺利推进营造良好舆论氛围。

在协同治理方面，中央网信办举报中心自2026年6月起开设“涉AI应用乱象举报专区”，专项受理公众举报。针对部分涉及地域发展、产业民生的谣言，6月启动的“丝路捉谣记之求真之旅”行动中，一批正能量网络达人化身“辟谣侠”，逐一鉴伪、果断辟谣，生动展现丝路沿线发展新面貌。公安机关依法打击造谣传谣行为，对“2026年高考答案”“孤女模拟考648分遭亲舅舅烧书阻止高考”“湖南救灾村支书佩戴的‘金耳环’有二两重”等造谣传谣相关责任人依法予以行政处罚。（来源：网信中国）

10. 因履行个人信息保护义务不到位，一物业公司被网信部门处罚

7月9日消息，重庆市南川区网信办近日对辖区一物业管理公司履行个人信息保护义务不到位的行为依法作出行政处罚。

经查，该公司运营的停车场扫码缴费系统设置“停车券兑换”诱导性入口，用户点击后提供非必要敏感个人信息，相关协议为默认勾选，未在显著位置告知用户信息收集的目的和范围。该公司将缴费系统委托第三方公司开发运营，内部缺乏个人信息保护管理等相关制度，日常监管缺失，导致曾因非“纯净码”问题被投诉整改后，同类问题再次出现。其行为违反《个人信息保护法》第六条、第十四条、第十七条、第二十一条、第二十七条、第二十八条、第二十九条、第三十条的规定。

南川区网信办依据《个人信息保护法》第六十六条的规定，责令该公司限期整改，并给予警告的行政处罚。同时要求该公司立即删除违规收集的个人信息，将扫码缴费页面整改为“纯净码”模式，取消非必要敏感个人信息的收集，建立完善内部个人信息保护管理制度。（来源：网信重庆）

11. 重庆自贸试验区首个数据出境负面清单使用案例落地

7 月 26 日消息，长安汽车近日通过使用《中国（重庆）自由贸易试验区数据出境管理清单（负面清单）（2025 版）》，成功向国家网信部门申报数据出境安全评估并顺利通过，成为重庆自贸试验区首家享受负面清单政策红利的企业，标志着重庆在探索构建高效便利安全的数据跨境流动机制方面取得实质性突破。（来源：网信重庆）

12. 湖南省网信办发布湖南网信系统 2026 年上半年网络执法案例

7 月 27 日，湖南省网信办发布湖南网信系统 2026 年上半年网络执法案例。据统计，上半年湖南省网信系统共依法约谈警告违法违规网站、账号 345 次，责令违法违规网站、账号改正 2888 次，处置违法违规网站、APP887 次。

案例一：湖南某传媒有限公司运营的某风网未取得互联网新闻信息服务许可，违规开展互联网新闻信息服务活动，被行政处罚后整改不到位。省网信办协调省通信管理部门依法予以关闭网站。

案例二：湖南某科技有限公司网等 26 家网站存在涉黄涉赌违法信息，破坏网络生态，相关网站负责人无法取得有效联系。省网信办协调省通信管理部门依法予以关闭网站。

案例三：湖南 2 个备案大模型 AI 生图内容存在违法违规信息。省网信办及时组织约谈 2 家责任单位，通报问题、明确整改要求，下发责令整改通知书。

案例四：何某纠集龚某某等 8 人在汨罗市公共场所摆拍低俗场景，刻意制造网络话题，破坏公序良俗，造成恶劣社会影响。网信部门联合公安机关依法查处，对策划组织者何某采取刑事拘留措施，对参与摆拍的龚某某等 8 人依法予以行政拘留，对涉事违规账号予以封禁。

案例五：衡阳县视频账号“红梅”在直播间发布低俗谩骂、污言秽语、色情信息等违规行为。衡阳县网信办联合公安机关对陶某予以行政处罚，对相关视频账号予以封禁。

案例六：株洲刘某、张某等 8 人在明知上线利用 APP 进行网络赌博的情况下，仍租借账号直播引流。株洲市网信办联合公安机关查获涉案设备，对涉案的刘某等 8 人依法予以行政拘留，对涉事账号予以封禁。

案例七：邵阳武冈胡某（账号“旭胡氏传承中草药”）通过网络平台夸大中草药疗效，诱骗开展售卖经营，涉嫌非法行医售假药。武冈市网信办联合卫健局依法对其作出罚款 3 万元的行政处罚，并删除虚假信息内容。

案例八：郴州5家自媒体账号为引流以谐音暗语诱导购买烟花、非法转卖烟花爆竹，严重扰乱秩序。郴州市网信办联合公安机关对相关责任人作出行政拘留13日的行政处罚，对相关自媒体账号予以关停或禁言。

案例九：郴州永兴县网民李某某通过AI生成软件生成郴州市中考志愿填报指南等AI图片，编造“2026年永兴一中中考‘指标生’名额减少”等不实信息引发恐慌。永兴县网信办联合公安机关依法对李某某作出罚款的行政处罚。

案例十：怀化溆浦网民舒某利用AI工具生成“湖北部分小作坊生产线使用霉碎米陈米加工黄曲霉超标”谣言视频发布。溆浦县网信办联合公安机关依法作出罚款的行政处罚，责令删除相关视频。

案例十一：湘西龙山3名网民注册购买大量账号，使用AI工具编造“证监会暂缓IPO”虚假政策内容批量传播引发市场恐慌。网信部门联合公安机关依法对主要组织者予以行政拘留，其余2名涉案人员处以行政罚款，对涉事账号予以封禁。

案例十二：永州东安灯某网未取得版权授权，擅自传播售卖影视音像作品。东安市网信办联合公安机关责令该网站关停并注销ICP备案，并对相关责任人依法作出行政警告处罚。

案例十三：集中排查发现湘潭市有50家机关事业单位备案网站存在访问异常情况，湘潭市网信办依法组织约谈未按要求反馈的5家党政机关和事业单位，责令限期整改。目前，涉事问题网站已全部整改到位，其中注销备案33个、恢复正常运行4个、保留使用13个。

案例十四：岳阳楼区某医院微信服务号存在信息泄露漏洞，存在较大网络安全风险。岳阳楼区网信办依法对该医院作出警告、罚款1万元的行政处罚。

案例十五：株洲天元某公司多个互联网平台存在系统漏洞和弱口令，限期内整改不积极。天元区网信办联合公安机关对该公司处以罚款5万元。

案例十六：益阳某中医医院、沅江市某医院信息系统未履行网络安全、数据安全、个人信息保护义务，致敏感数据存在泄露风险。益阳市网信办责令改正，给予警告，并对其中一家医院给予罚款的行政处罚。

案例十七：湖南某酒店管理有限公司未履行个人信息保护义务，其运营微信小程序存在违法违规收集使用个人信息问题。省网信办依法立案调查，责令公司改正，给予公司警告的处罚。

案例十八：长沙市某民营医院在收集使用个人信息时未明示处理目的、方式和范围，未按规定留存网络日志。长沙市网信办依法责令公司改正，给予警告，对违法处理个人信息的应用程序责令终止提供服务。

案例十九：常德某文化传媒有限公司、湖南某文化传媒有限公司未经未成年人的父母或者其他监护人书面同意，组织未成年人参与演出、节目制作。常德市网信办联合文化市场综合行政执法支队依法作出警告、没收违法所得、罚款的行政处罚。

案例二十：怀化中方某停车场管理企业在收集个人信息时未履行告知义务，技术防护薄弱存在泄露风险。中方县网信办联合公安机关责令限期整改，处以警告的行政处罚。（来源：网信湖南）

（三）通信管理部门治理实践

1. 工信部通信管理局以及安徽、浙江等地通信管理部门通报侵害用户权益的 APP（SDK）

（1）工信部

7 月 2 日，工业和信息化部信息通信管理局通报 2026 年第 4 批（总第 57 批）侵害用户权益行为的 APP（SDK）。工业和信息化部近日组织第三方检测机构进行抽查，共发现 32 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，工业和信息化部将依法依规组织开展相关处置工作。

（2）安徽

7 月 14 日，安徽省通信管理局通报 2026 年第 4 批侵害用户权益的 APP。安徽省通信管理局近日对省内 APP 进行拨测检查，检测发现 20 款 APP 存在违法违规收集使用个人信息的问题，2026 年 5 月 28 日对上述违规 APP 企业下达了责令改正通知书，要求限期完成整改工作。截至通报，尚有 10 款 APP 未完成问题整改，相关 APP 企业应在 2026 年 7 月 17 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。

7 月 17 日，安徽省通信管理局通报下架 11 款侵害用户权益 APP。针对 2026 年第 3 批次整改不到位的 APP，安徽省通信管理局已对相关 APP 予以公开通报，并要求限期整改。截至目前，尚有 11 款 APP 逾期未完成整改。经研究，决定对上述 APP 进行下架，相关应用商店应在本通报发出后，立即对涉及的应用软件进行下架处理。

（3）上海

7 月 22 日，上海市通信管理局通报下架 64 款侵害用户权益行为的 APP（SDK）。2026 年 6 月，上海市通信管理局向社会公示了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 64 款 APP（SDK）未按照要求落实整改，现对上述 APP（SDK）采取下架处理。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。

7 月 27 日，上海市通信管理局通报 2026 年第五批侵害用户权益行为 APP（SDK）。上海市通信管理局近日组织第三方检测机构对我市 APP（SDK）进行抽查，共发现 25 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 个工作日内将整改报告报送至邮箱 hlwglc@mailshca.miit.gov.cn，自评估报告通过安全监管平台报送。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。

（4）浙江

7 月 23 日，浙江省通信管理局通报 2026 年第 6 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卫健、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 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 8 月 3 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。

（5）山东

7 月 29 日，山东省通信管理局通报 2026 年第 2 批不合格 APP 整改情况。山东省通信管理局近日对山东省各类 APP 进行合规性检测。截至 7 月 29 日，有 12 款存在问题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。8 月 5 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 7 月 29 日，有 7 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。（来源：工信部、安徽省通信管理局、上海市通信管理局、浙江省通信管理局、山东省通信管理局）

2. 上海市通信管理局部署开展2026年电信和互联网行业网络和数据安全检查

7月7日，上海市通信管理局部署开展2026年电信和互联网行业网络和数据安全检查。

检查对象是提供公共互联网网络信息服务的基础电信企业，增值电信企业、互联网企业（含云平台服务提供商、APP和小程序运营企业、车联网企业、工业互联网平台和标识解析企业等）、域名注册服务机构等。重点检查相关网络运行单位的重要网络单元及承载重要数据的信息系统，包括但不限于关键信息基础设施、通信网络基础设施、公共云服务平台、域名服务系统、工业互联网平台、工业互联网标识解析系统、车联网平台及应用等。

检查内容主要包括以下十项，分别是网络和数据安全保障体系建设落实情况、通信网络安全防护工作落实情况、网络数据安全保护落实情况、车联网网络和数据安全防护情况、工业互联网企业网络安全防护情况、暴露面风险管理情况、网络安全威胁监测情况、网络和数据安全事件应急处置情况、互联网基础资源管理、个人信息和用户权益保护工作情况。（来源：上海通信圈）

3. 浙江省通信管理局部署开展2026年电信和互联网行业网络和数据安全检查

7月15日，浙江省通信管理局通知在2026年7月至11月期间开展2026年电信和互联网行业网络和数据安全检查。

检查对象是相关单位建设运营的网络、系统、平台、应用、业务，重点检查重要网络单元及承载重要数据的信息系统，包括但不限于关键信息基础设施、通信网络基础设施、5G 行业应用、互联网接入服务系统、互联网数据中心、网上营业厅、企业门户网站、网络管理系统、网络交易系统、计费系统、域名系统、电子邮件系统、物联网服务平台、工业互联网平台、工业互联网标识解析系统、车联网平台、数据服务平台、公共服务云平台、移动智能终端及移动应用分发平台、APP 及小程序等。

检查内容主要包括以下六项，分别是网络和数据安全保障体系建设落实情况、通信网络安全防护工作落实情况、数据安全保护落实情况、工业互联网企业网络安全防护情况、车联网安全防护管理情况、个人信息和用户权益保护工作情况。其中，数据安全保护落实情况要求检查相关单位落实“之江数安”工作部署要求情况，包括重要数据识别认定及目录管理、数据安全风险评估、数据对外共享安全管理、数据安全风险监测与预警处置、数据安全事件应急预案制定与应急演练等。（来源：浙江省通信管理局）

（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《关于仿冒教育培训类 APP 的手机木马病毒的预警报告》

7 月 10 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在我

国境内捕获发现针对我国用户的仿冒教育培训类 APP 的安卓平台手机木马病毒。

用户一旦安装运行仿冒 APP，该 APP 会诱导用户授予其后台运行和使用无障碍服务的权限。在获取权限后，恶意程序会在手机系统后台静默运行，手机屏幕页面则显示正常画面。经分析，该恶意 APP 为金融盗窃类手机木马病毒的新变种，具有拦截用户短信、窃取通讯录、窃取手机密码、开启摄像头、录屏、录音等侵犯公民个人信息的恶意功能，并进一步通过短信和社交媒体软件进行传播。

国家计算机病毒应急处理中心建议，一是不要从短信、社交媒体软件、网盘等非官方渠道传播的网络链接或二维码下载 APP 程序，仅通过官方网站或正规手机应用商店下载安装相应 APP 程序；二是保持手机预装的安全保护功能或第三方手机安全软件处于实时开启状态，并保持手机操作系统和安全软件更新到最新版本；三是在手机使用过程中，谨慎处理非用户主动发起的 APP 安装请求，一旦发现 APP 在安装过程中发起对设备管理器、后台运行和使用无障碍功能等权限请求，应一律予以拒绝；四是对已下载的安装包或可疑文件，可访问国家计算机病毒协同分析平台进行上传检测。（来源：国家计算机病毒应急处理中心）

2. 2026 年上半年全国检察工作情况公布，起诉利用网络实施的犯罪 7.7 万人

7 月 16 日，第十六次全国检察工作会议在京召开。据介绍，2026 年 1 月至 6 月，全国检察机关批准逮捕各类犯罪嫌疑人 31.2 万人、提起公诉 60.3 万人，同比分别下降 4.4%、11.5%。

在网络犯罪治理方面，检察机关积极参与“净网 2026”等专项行动，依法惩治网络暴力、网络谣言、网络敲诈、“网络水军”等违法犯罪，上半年起诉利用网络实施的犯罪 7.7 万人。深入推进打击跨境电信网络诈骗专项行动，起诉电信网络诈骗犯罪 3.2 万人。发布公民个人信息保护典型案例，起诉侵犯公民个人信息犯罪 2641 人，办理公益诉讼 2090 件。（来源：最高人民检察院）

3. 国家数据局：全国已建成高质量数据集 12 万个

7 月 18 日消息，根据国家数据局信息，我国已建成高质量数据集 12 万个。截至 2026 年 6 月底，全国已建成科学研究、工业制造、医疗卫生、教育教学等行业领域的高质量数据集总体量超 1565 拍字节（PB），较一季度末增长超 60%，现有体量相当于中国国家图书馆数字资源总量的 547 倍左右。同时，我国数据标注产业加快发展，有效支撑高质量数据集建设。截至 6 月底，四川成都、辽宁沈阳、安徽合肥、湖南长沙、海南海口、河北保定、山西大同七个数据标注先行先试城市标注规模超 119 拍字节（PB），数据标注从业人员达 14 万人。（来源：国家数据局）

境内前沿观察三：人工智能安全专题

导读：7 月，我国推动成立世界人工智能合作组织，并通过世界人工智能大会、APEC 人工智能高级别论坛等多边平台持续凝聚治理共识。人工智能政策推进重点聚焦智能体安全治理、产业应用促进等方面。总体看，相关部署继续沿着促进人工智能创新发展与强化安全治理并重的思路推进。

国际合作层面，人工智能治理国际合作持续深化，重要国际组织成立、多份重量级政策文件相继发布，为全球治理合作注入了新的动力和方向。联合国全球网络安全常设机制首次会议期间，中国代表团提交《中国关于数智时代全球网络治理的立场文件》，提出数字主权重要原则。世界人工智能合作组织成立，29 个国家成为世界人工智能合作组织创始成员国，将重点推动人工智能政策交流、技术合作、人员培训和联合研究等工作。会议方面，2026 世界人工智能大会暨人工智能全球治理高级别会议在上海举办。会议期间，发布主席声明，推出《智能体互信互联互操作全球合作倡议》《国际人工智能伦理治理行动计划》《人工智能合作发展行动计划》一系列成果，标志着人工智能全球治理正从理念探讨迈向务实合作的新阶段。APEC 人工智能高级别论坛在成都举办，通过《关于促进亚太地区人工智能发展的声明》，围绕安全发展和部署、负责任普及应用、创新环境建设以及普惠合作提出多项倡议。

智能体安全治理方面，《智能体应用安全基本要求》强制性国家标准正式立项，拟面向公众服务领域智能体产品和服务，将网络安全、数据安全等治理要求转化为可检测、可执行的技术合规要求。全国网安标委发布《网络安全标准实践指南——智能体部署使用安全指引》，围绕评估、准备、部署、使用和停用五个阶段提出全生命周期安全要求，重点强调最小权限、访问范围限制、日志全量记录、高风险操作二次确认、技能来源审查和敏感信息保护。

监督执法方面，中央网信办公布“清朗·整治 AI 应用乱象”专项行动第一阶段成果，围绕大模型备案、平台审核能力等问题，处置违规网站、应用程序和智能体等 AI 产品 1.4 万余款。公安机关上半年开展人工智能应用服务监督检查 600 余次，依法查处利用 AI 生成网络谣言以及提供违法生成内容服务等行为。

关键词：人工智能全球治理；智能体安全；AI 应用治理

1. 世界人工智能合作组织成立，29 个国家成为创始成员

7 月 16 日，29 个国家在上海签署《关于成立世界人工智能合作组织的协定》，成为世界人工智能合作组织创始成员国。协定包括组织宗旨、基本原则、职能、组织架构、决策程序、成员资格等内容。

据介绍，中方将会同创始成员国推动组织尽早启动运转，未来将重点开展三方面工作：一是把加强人工智能能力建设国际合作作为优先事项，通过政策交流、技术合作、人员培训、联合研究等方式，促进人工智能技术和服务的可及性，确保发展中国家在新一轮智能浪潮中平等受益；二是在开展沟通对话、建立政策共识、分享最佳实践的基础上，切实发挥供需对接平台作用，推动各国优势资源深度融合互补，结合各国国情推进“人工智能+”行动，加强科技和产业合作，鼓励共建开源生态，打造务实合作成果；三是坚定捍卫联合国宪章宗旨和原则，支持更好地发挥联合国作用，落实《全球数字契约》和联合国可持续发展目标，在人工智能领域推动构建公正合理的全球治理体系。（来源：新华网）

2. 2026 世界人工智能大会暨人工智能全球治理高级别会议举行，通过大会主席声明提出十五点共识

7 月 17 日至 20 日，2026 世界人工智能大会暨人工智能全球治理高级别会议在上海举行。大会发布《2026 世界人工智能大会暨人工智

能全球治理高级别会议主席声明》，从人工智能发展、治理、安全、合作等多角度提出十五点意见。

在人工智能发展方面，声明指出，创新是人工智能发展的核心驱动力。倡导培育以企业为主体、以市场为牵引、以应用为导向、以科研为基础、以人才为根本的创新生态。人在人工智能发展中发挥关键作用，要高度重视培养具备数字和人文素养、创新能力和全球视野的人工智能领域人才。

在人工智能安全与治理方面，声明强调要秉持“同球共济”精神，通过人工智能国际协调为全球治理树立新范式。大会认为，应当统筹发展和安全、平衡创新和治理、兼顾本国利益和全球福祉。要始终用人类智慧和国际共识引领人工智能发展，使其真正成为增进全人类福祉、推动人类文明进步的强大正能量。

在国际合作方面，声明呼吁加强人工智能国际合作，讨论和解决智能时代人类共同面对的重大问题、紧迫挑战。把人工智能能力建设国际合作置于人工智能全球治理的突出位置，着力解决资源分布不均、权力分配不公等突出问题，帮助全球南方国家在人工智能发展进程中平等受益。（来源：新华社）

3. 中国发布《中国关于数智时代全球网络治理的立场文件》，强调重视新兴技术对网络和数据安全带来的颠覆性影响

7 月 20 日至 24 日，联合国全球网络安全常设机制首次会议在纽约联合国总部举行。中国代表团向全球机制提交《中国关于数智时代

全球网络治理的立场文件》。继网络主权后，中方此次提出了数字主权的重要原则，是中国落实全球治理倡议和推动构建网络空间命运共同体的最新举措。

文件指出，当前以人工智能等新兴技术为核心的数智革命迅猛发展，网络安全成为事关各国主权、安全、发展利益的重大问题。“网络战”禁忌已被公然打破，人工智能等新兴技术推高网络安全风险，网络攻击和国家间网络冲突门槛降低，关键基础设施网络安全风险突出，全球数智产业链供应链被人为割裂，全球网络治理赤字加剧，数智世界面临分裂失序危险。

文件表示，2026 年是联合国全球网络安全常设机制开局之年。中方遵循构建网络空间命运共同体理念，基于全球发展倡议、全球安全倡议、全球文明倡议和全球人工智能治理倡议四大全球倡议以及《全球数字契约》等国际共识，进一步提出三点主张，分别是遵守国际规则，维护和平稳定；尊重数字主权，共促普惠发展；坚持多边主义，有效应对风险。

其中，文件强调，要重视人工智能、量子技术等新兴技术对网络和数据安全带来的颠覆性影响，与时俱进发展和制定网络空间国际规则。要平衡发展与安全，坚持政府主导、多方参与，推动完善多边、民主、透明的全球网络治理体系。不搞“公司治理”代替“国家治理”，不搞“小圈子治理”代替国际治理，不单方面向他国强加规则。应推动建立全球性的人工智能大模型网络安全风险等级测试评估标准和体系，确保人工智能成为网络安全的新护盾，而不是单方面谋求霸权

的新工具。应推动全球数据跨境流动合作，促进数据跨境流动，推动制定全球数据跨境流动原则和规范，维护各国数据安全。（来源：新华社）

4. APEC 人工智能高级别论坛举行，通过《关于促进亚太地区人工智能发展的声明》

7 月 24 日，APEC 人工智能高级别论坛在四川成都举行，论坛通过《关于促进亚太地区人工智能发展的声明》。各成员经济体重申致力于在人工智能领域深化交流、凝聚共识、加强合作、促进创新，继续实施《2040 年 APEC 布特拉加亚愿景》《APEC 互联网和数字经济路线图》和《APEC 人工智能倡议（2026—2030）》。

声明鼓励各经济体在促进人工智能安全发展和部署，加快人工智能的负责任普及应用，营造有利于人工智能创新的环境，推动广泛参与、普惠共享的 APEC 合作等领域开展合作。具体来说，声明鼓励推动安全优先的人工智能发展，促进旨在应对风险、造福人民的创新。鼓励各成员经济体就促进发展可靠、可及、可扩展、可信、安全且有韧性的人工智能基础设施，以及提升数字基础设施可及性交流最佳实践。声明提出将促进数据跨境流动，这对人工智能发展至关重要，同时增强消费者和企业信任。（来源：中央网信办）

5. 全国网安标委发布《网络安全标准实践指南——智能体部署使用安全指引》

7 月 1 日，全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——智能体部署使用安全指引》，面向人工智能智能体部署使用的安全风险防范，覆盖评估、准备、部署、使用、停用等全生命周期五个阶段，为组织和个人部署使用智能体提供标准化实践指引，也可为选择使用商业智能体服务提供参考。

《指引》明确，智能体（agent）是指具备自主感知、记忆、决策、交互与执行能力的智能系统，特指面向个人助手场景、需要用户授予较高权限、基于大模型的人工智能智能体，一般为软件系统。

在部署阶段，《指引》要求不应使用操作系统管理员权限运行智能体，宜仅授予完成预期任务所必需的最小权限；应限制智能体的可访问目录范围，为智能体建立专用工作目录；应将智能体及其相关服务配置为仅本机可访问，确需通过互联网访问的应配置加密访问并限制来源；应开启日志记录功能，对文件操作、指令执行、网络活动、技能调用等进行全量记录；应提前建立高风险操作清单，对清单内操作实行二次确认或直接阻断，高风险操作包括停止系统服务、终止进程、格式化磁盘、批量删除、权限修改、修改防火墙规则、访问密码管理器等，涉及转账、支付等影响财产安全的操作也应列入清单。

在使用阶段，《指引》要求对安装与配置情况进行复查，确保使用者能有效了解执行状态并进行安全管理；应使用来源可靠的技能并加强安全测试；向智能体提供个人信息时应坚持最小必要原则，涉及

生物特征、家庭隐私等敏感信息的应审慎提供，未获授权不应提供第三方个人信息及敏感数据；应定期检查智能体公网接口必要性和安全性，及时关闭非必要暴露的接口；定期开展容灾备份，手动查看长期记忆文件记录内容并及时处理不宜存储的信息；及时回收敏感权限，清理不再使用的技能与敏感对话记录；持续关注安全公告，出现安全事件时及时采取升级、降级或版本锁定等措施。（来源：全国网安标委）

6. 国家网信办发布《智能体互信互联互操作全球合作倡议》

7 月 17 日，2026 世界人工智能大会暨人工智能全球治理高级别会议主论坛期间，中国国家互联网信息办公室会同有关方面提出《智能体互信互联互操作全球合作倡议》。

《倡议》共十点，分别是（1）强化技术研发，驱动协同创新；（2）促进标准互认，消弭生态壁垒；（3）共建基础设施，保障互联可及；（4）共推应用落地，加速场景示范；（5）共促产业协同，繁荣全球生态；（6）共筑安全底线，恪守伦理准则；（7）促进数据流动，强化普遍保护；（8）加强资源共享，弥合智能鸿沟；（9）营造包容文化，尊重多元治理；（10）提升数字素养，确保人人受益。

其中，共筑安全底线，恪守伦理准则方面，《倡议》呼吁坚持负责任创新的基本立场，建立覆盖智能体全生命周期的安全治理框架，并将安全与伦理考量嵌入技术研发、系统部署与运行维护，重视智能体对网络安全的深刻影响，负责任发布和使用智能体，确保智能体互

信、互联、互操作始终不逾越安全底线与人类尊严红线。（来源：网信中国）

7. 国家发改委会同有关部门发布《人工智能合作发展行动计划》

7 月 17 日，2026 世界人工智能大会暨人工智能全球治理高级别会议期间，国家发展改革委会同有关部门共同发布《人工智能合作发展行动计划》。

《行动计划》共提出八项行动，分别是优质数据供给行动、智能算力普惠行动、开源生态共享行动、人工智能深度赋能行动、数智人才共育行动、规则标准共建行动、安全治理协作行动以及人工智能向善行动。

其中，安全治理协作行动方面，《行动计划》要求共建人工智能安全治理机制，加强网络安全威胁信息共享和应急处置合作，防范人工智能技术误用、滥用。研究提升人工智能可解释性、透明性、安全性，加强人工智能数据治理，为全球人工智能发展营造良好环境。提倡建立开放性平台，共享最佳实践，在全球范围推动人工智能安全治理国际合作。（来源：人民网）

8. 工业和信息化部会同有关方面共同指导发布《国际人工智能伦理治理行动计划》

7 月 17 日，2026 世界人工智能大会暨人工智能全球治理高级别会议期间，工业和信息化部会同有关方面共同指导发布《国际人工智能伦理治理行动计划》。

《行动计划》共提出六项措施，分别是推动各方广泛参与伦理治理、强化人工智能全生命周期伦理治理、深化人工智能伦理风险防控合作、形成敏捷治理的动态伦理治理机制、培育产业链协同的伦理治理生态以及营造伦理治理社会氛围。

《行动计划》提出，在数据采集与算法设计环节，提升数据真实性和准确性，提升人工智能系统的透明性与可解释性。在人工智能系统部署与使用环节，避免技术的误用、滥用与恶用。关注前沿人工智能系统可能引发的重大伦理风险，探索建立面向关键信息基础设施、重要行业和社会公众的分级风险告知机制。共同探索开展伦理风险分级分类定期评估，适时更新伦理风险分级分类参考标准。积极适应人工智能系统快速迭代和智能体自主行动能力增强的趋势，实施敏捷治理。（来源：澎湃新闻）

9. 全球首部智能体安全强制性国家标准正式立项

7 月 28 日消息，国家标准化管理委员会近日正式下达《智能体应用安全基本要求》强制性国家标准计划（计划号：20263116-Q-252）。该标准为全球首部面向智能体安全的强制性国家标准，填补了

公众服务领域智能体安全强制性标准的国际空白，是我国完善人工智能综合治理体系的一项战略性举措。标准由中央网信办归口管理，中国移动通信集团有限公司、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心牵头起草。

该标准聚焦面向公众的智能体产品与服务，紧密围绕防范关键安全风险、守牢安全底线的目标构建安全合规框架，同时注重将宏观安全治理红线转化为可落地、可检测的技术合规要求，为后续行业监管、市场准入和技术测评提供法定底层依据，为技术创新与场景落地预留合理发展空间。

在全球智能体应用与产业战略博弈的关键期，规则话语权已成为核心竞争力之一。该强制性国家标准计划作为国家统筹发展与安全的前瞻性治理抓手，既为防范智能体产业系统性风险、守住网络安全和数据安全底线提供了基准，也为构建安全、可靠、可控的人工智能产业生态奠定了基础。同时，这也是我国深度参与全球人工智能治理、输出中国治理思路、争取智能体领域国际规则话语权的重要实践。（来源：网信浙江）

10. 北京市发展和改革委员会等五部门发布《关于印发北京市加快智能体引领发展若干措施的通知》

7 月 21 日，北京市发展和改革委员会、中共北京市委网络安全和信息化委员会办公室等五部门发布《关于印发北京市加快智能体引

领发展若干措施的通知》，提出持续提升基础模型能力、强化智能体底层共性技术攻关、加速智能体原生应用和标杆场景建设等十项措施。

持续提升基础模型能力方面，《通知》提出，推动代理式人工智能（Agentic AI）技术创新，提升模型在线学习、持续学习和自主进化能力，优化超长程任务、复杂推理与规划等基础算法。支持创新主体开展模型新架构、新训练范式以及原生融合智能体大模型、世界模型、群体智能等技术攻关，突破智能上限。持续提升大模型实际任务完成能力，支持创新主体开展工具调用、长上下文、多智能体协同、记忆等共性技术攻关。

全面提升安全治理能力方面，《通知》提出，探索建立智能体分级分类监管机制，完善与创新发展相适应的科学监管方式。引导行业加强自律自治，开展人工智能和智能体技术恶意滥用常态化整治，防范滥用市场优势地位，促进行业健康有序发展。加快推动人工智能产业立法，营造鼓励创新、规范发展的法治环境。加快智能体安全基础设施建设，支持创新主体建设智能体安全服务平台，搭建靶场环境和可信沙箱，开发安全大模型提升“以模治模”能力，开放智能体漏洞扫描、安全检测、攻防对抗、安全认证等共性服务。（来源：北京市人民政府）

11. 江苏省发布《江苏省人工智能产业发展促进条例（草案）》

7 月 31 日，江苏省发布《江苏省人工智能产业发展促进条例（草案）》，共八章六十三条，包括基础要素、应用赋能、安全治理等内容。

基础要素方面，草案规定，数据主管部门应当会同有关部门建立公共数据资源开发利用责任制，构建支撑人工智能技术研发与应用的公共数据资源体系，动态调整高价值公共数据清单。数据主管部门应当健全公共数据授权运营机制，提高公共数据社会化开发利用水平和数据利用价值。有关部门应当按照规定向数据主管部门归集公共数据，强化数据动态更新和质量管理。

安全治理方面，草案强调，从事人工智能研究、开发、应用的单位和个人，应当履行主体责任，建立健全人工智能相关内容审核、应急处置等安全管理制度，定期开展风险评估，采取有效措施保障人工智能安全。人工智能服务商应当按照国家有关规定履行安全评估和备案手续、对人工智能生成合成内容进行标识。（来源：江苏省人大）

12. 中央网信办发布“清朗·整治 AI 应用乱象”专项行动第一阶段工作成果

7 月 6 日，中央网信办发布“清朗·整治 AI 应用乱象”专项行动第一阶段工作成果。

“清朗·整治 AI 应用乱象”专项行动自 2026 年 4 月启动以来，中央网信办聚焦未按规定履行大模型备案登记义务、AI 平台安全和

审核过滤能力不足、AI 数据投毒、生成合成内容标识落实不到位等 AI 应用乱象，部署各地网信部门深入推进第一阶段重点整治任务，并开设“涉 AI 应用乱象举报专区”，专项受理公众举报。第一阶段累计处置违规网站、应用程序、智能体等 AI 产品 1.4 万余款，清理违法违规信息 600 余万条，处置账号 2.6 万余个，下架违规 AI 商品 1300 余个、违规开源数据集 9 个。

各地网信部门认真履行属地管理责任，结合实际采取有效监督管理措施。如：北京网信办建立“平台自查+常态巡查+技术筛查+线索核查”联动工作机制，及时下架一批违规 AI 应用和运营账号。上海网信办针对平台类型细化工作要求，指导平台升级举报机制、主动发布治理公告。浙江网信办从模型审核能力、训练语料安全、AI 数据投毒等多维度，组织开展优化语义判断能力、高频回归测试等针对性整改。江苏网信办开设 AI 应用乱象专项举报窗口，收集 AI 数据投毒、未落实生成合成内容标识要求等 5 类违法违规情形举报线索，及时核实处置。广东网信办建立属地多部门协调监管机制，综合运用技术巡查、人工复核、现场督导、约谈惩戒方式开展 AI 应用乱象全链条治理等。

重点网站平台积极履行主体管理责任，有针对性地加强管控。如华为在应用商店中增加生成式人工智能服务备案和标识专项审核；阿里巴巴完善数字指纹比对与关键词拦截机制，提升违法违规内容识别精度；智谱构建多模态审核模型，针对多轮对话意图反转等复杂场景开展交叉复核；稀宇及时识别阻断利用 AI 编写病毒、钓鱼软件等恶

意行为；DeepSeek 在数据采集和预处理环节嵌入异常检测算法，防止恶意样本隐蔽操控等。（来源：网信中国）

13. 公安部发布 2026 年上半年打击利用新技术实施违法犯罪活动的打击治理情况，共开展人工智能应用服务监督检查 600 余次

7 月 24 日，国务院新闻办公室举行“开局起步‘十五五’”系列主题新闻发布会，公安部相关负责人介绍针对利用人工智能等新技术实施的违法犯罪活动的打击治理情况。据介绍，公安机关高度重视利用人工智能等新技术实施的违法犯罪，从依法严厉打击，震慑违法犯罪；开展智能预警，提高防范能力；多部门协同共治，加强行业监管；强化建章立制，完善法律体系四方面采取措施打击和整治。

据统计，今年上半年，共侦办利用人工智能工具生成网络谣言案件 170 余起，依法查处 190 余人。公安部联合网信办、工信部、国家广电总局发布《人工智能生成合成内容标识办法》，规范内容标识，向公众提示人工智能合成内容。同时，加强监督检查，针对人工智能大模型可能存在的安全风险开展重点监测，并通报运营主体，及时消除隐患。今年上半年，共开展人工智能应用服务监督检查 600 余次，对相关服务提供者进行警告、责令整改、关停等行政执法 30 余次。此外，积极推进《网络犯罪防治法》等法律法规立法进程，完善人工智能风险治理法律规范体系。研究构建人工智能安全审查制度，防范此类服务被滥用于实施违法犯罪。研究制定人工智能代码生成、深度

合成图像等领域的安全标准，不断推进和完善人工智能的安全标准体系建设。（来源：国务院新闻办公室）

14. 北海市网信部门对“豆灵 AI”平台依法作出处罚

7 月 16 日消息，北海市互联网信息办公室近日在工作中发现，北海三鲜电子商务有限公司运营的“豆灵 AI”微信小程序（备案号桂 ICP 备 2024026178 号-5X，备案服务名称“AI 搜索助手”）可生成违法信息，依法开展立案调查。经查实，北海三鲜电子商务有限公司提供可生成违法信息的生成式人工智能服务，违反了《生成式人工智能服务管理暂行办法》。7 月 9 日，北海市互联网信息办公室依据《生成式人工智能服务管理暂行办法》责令该公司限期改正违法行为，对其处以警告、通报批评的行政处罚。（来源：网信北海）

15. 周某利用 AI 工具编造“高考估分 715 查分 299，女孩称试卷不是自己的”谣言被行政拘留

7 月 19 日消息，一篇题为《高考估分 715 查分 299，女孩称试卷不是自己的》的网文近日在网络平台大范围传播，引发网民热议。经四川绵阳市教育体育局、四川省教育考试院联合全面核查，整篇内容纯属人为编造的谣言。经查，该帖发布人周某为福建厦门籍网民，其借助人工智能工具批量生成虚假网文。目前，周某已被公安机关抓获，绵阳市公安机关依法对其作出行政拘留处罚，并依法办理异地拘留执行手续。（来源：公安部网安局）

境外前沿观察：月度速览十则

导读：7月，境外各国及组织围绕关键基础设施韧性、人工智能安全以及个人信息保护等领域持续推进政策法律安排。

网络安全与关键基础设施韧性方面，美国、澳大利亚、加拿大、英国、新西兰等国家的网络安全中心联合发布《关键基础设施隔离指南——隔离关键系统建议》，提出关键基础设施运营者必须有意识、有序地将关键运营技术系统与所有其他网络断开，并在危机持续期间维持关键服务运行。美国、英国、日本、荷兰等多国网络安全机构联合发布协调漏洞披露指南，推动软件制造商和在线服务提供商建立漏洞报告、风险评估、修复等。

人工智能治理方面，欧盟委员会发布《网络安全与人工智能行动计划》，提出促进先进人工智能安全使用、提升关键行业应对人工智能驱动型网络威胁的能力，并通过模型上市前评估和安全测试平台支持人工智能在网络防御领域部署。欧盟数据保护委员会发布《生成式人工智能背景下网络抓取指南》，要求生成式人工智能训练数据抓取遵守合法性、目的限制、数据最小化和透明度原则。新加坡个人数据保护委员会发布《生成式人工智能中个人数据使用指导性指南》，指出系统部署者无论自行开发系统，还是采购软件即服务、应用程序接口等外部服务，均对所采用的生成式人工智能系统能否符合新加坡《个人数据保护法》要求承担主要责任。

个人信息保护方面，日本通过《个人信息保护法》修正法案，在特定人工智能开发和统计用途下适度放宽公开敏感信息的使用限制，同时设置公开披露和书面协议等配套要求。执法方面，监管重点正进一步延伸至人工智能语音数据、跨平台行为追踪、定向广告画像和关联公司之间的数据跨境流动。韩国个人信息保护委员会因苹果公司违法收集、使用 Siri 语音录音及转录文本，并未充分履行个人信息跨境传输告知义务，对其处以罚款并责令整改；因 TikTok 违法收集第三方网站和应用中的用户行为信息、将同意与服务使用捆绑并违法跨境传输个人信息，对其处以高额罚款。

关键词：网络安全；人工智能；个人数据保护；关键基础设施韧性

1. 欧盟 EDPB 发布《生成式人工智能背景下网络抓取指南》

7 月 7 日，欧盟数据保护委员会发布 1.0 版《生成式人工智能背景下网络抓取指南》。

指南指出，当网络抓取涉及个人数据的提取、清洗、结构化和存储等处理活动时，应当适用 GDPR。参与训练数据集收集和使用的组织应当根据具体处理活动，逐案认定为控制者、共同控制者或处理者。控制者应当遵守合法性、目的限制、透明度、数据最小化和准确性等原则，并在开展抓取前确定合法处理依据。

指南提出，私营实体通常以“合法利益”作为生成式人工智能训练中网络抓取的处理依据，但必须同时满足存在合法利益、处理具有必要性以及数据主体的利益和基本权利不优先于该合法利益等条件。控制者还应当采取技术和组织措施，明确收集标准，排除不必要的数据类别和明确反对抓取的网站，优先考虑使用合成数据，并对个人数据进行过滤、匿名化或者假名化处理。（来源：欧盟 EDPB）

2. 欧盟委员会发布《网络安全与人工智能行动计划》

7 月 7 日，欧盟委员会发布《网络安全与人工智能行动计划》。该计划旨在应对先进人工智能模型带来的网络安全风险，同时充分利用其在网络防御领域的潜力。《行动计划》提出三大战略目标：一是促进先进 AI 的安全与负责任使用，确保其在欧洲网络安全领域的安全部署；二是强化欧盟网络安全与韧性建设，支持关键行业和中小企业应对 AI 驱动的网络威胁；三是提升欧洲将 AI 技术应用于网络安

全领域的能力，发展欧洲生态系统并持续加强前沿 AI 领域的自主能力，减少战略依赖。

为了促进先进人工智能的安全使用，委员会将在模型上市前对其进行评估。此外，委员会还将与欧盟网络安全局合作，制定一项关于安全使用先进人工智能系统的欧洲计划，并建立安全测试平台，帮助能源、交通、医疗、金融和公共行政等关键领域的组织能够安全地测试和部署人工智能解决方案。（来源：欧盟委员会）

3. 日本参议院通过《个人信息保护法》修正法案

7 月 10 日，日本参议院全体会议通过《个人信息保护法》修正法案，旨在放宽人工智能数据使用限制，推动国产人工智能发展。

修正案规定，在 AI 开发或统计等不与个人身份直接挂钩的用途方面，企业可以在未经本人同意的情况下收集社交平台上公开的疾病史、犯罪记录等敏感信息。具体而言，若数据仅用于统计制作（含可归类为统计的 AI 开发），向第三方提供个人数据、获取公开的敏感个人信息，无需本人同意。企业若依据此例外进行数据转移或收集，须在其网站或指定渠道公开披露企业名称、统计分析的详细信息等。对于第三方数据转移，还需在转移方与接收方之间以书面协议明确约定该数据转移系依据本例外进行。（来源：日本参议院）

4. 美英日等多国网络安全机构联合发布指南《建立与安全研究人员合作的协调漏洞披露计划》

7 月 15 日，美国网络安全和基础设施安全局（CISA）、美国国家安全局（NSA）、日本计算机应急响应小组协调中心（JPCERT/CC）、荷兰国家网络安全中心和英国国家网络安全中心联合发布指南《建立与安全研究人员合作的协调漏洞披露计划》。指南面向软件制造商和在线服务提供商，提出设计和实施协调漏洞披露计划的最佳实践，支持供应商与外部安全研究人员合作报告和修复漏洞。

指南建议，供应商应当制定并公开漏洞披露政策，明确安全测试范围、禁止活动、最低报告要求、漏洞报告渠道、善意研究人员的“安全港”保障，以及漏洞修复、信息共享和公开披露的时间安排。指南同时要求建立漏洞报告确认、分诊、风险评估、修复和 CVE 编号分配流程。供应商还应当及时发布完整、准确的 CVE 记录和安全公告，定期评估并更新协调漏洞披露计划；自身能力不足时，可利用 CISA 等第三方协调机构或者国家计算机安全事件响应机构补充或者代为实施相关工作等。（来源：美国 CISA）

5. 欧盟委员会发布《人工智能系统提供者与部署者透明度义务指南》

7 月 20 日，欧盟委员会发布《人工智能系统提供者与部署者透明度义务指南》，协助人工智能系统的提供者与部署者履行《人工智能法》（AI Act）项下的透明度义务。委员会指出，相关义务将自 2026

年 8 月 2 日起适用，有助于公众识别自己何时正在与人工智能交互、或内容何时由人工智能生成或篡改，从而降低受欺骗和操纵的风险。

指南明确了哪些提供者和部署者须遵守交互式人工智能系统的透明度义务，以及人工智能生成内容的标记与标注义务。根据《人工智能法》，提供者须在设计人工智能系统时确保在用户直接与人工智能交互时予以告知，并须添加机器可读的标记，以便对人工智能生成或经篡改的内容加以检测。部署者则须在用户接触深度伪造内容、未经人工审阅或编辑把关的涉公共利益人工智能生成内容，以及情绪识别或生物特征归类系统时，向用户作出告知。

指南对若干概念作出阐释并给出豁免情形与示例，包括何为直接交互式人工智能系统（如聊天机器人）、何为合成内容（含部分或全部由人工智能生成的文本、深度伪造内容、涉公共利益的人工智能生成文本），以及拼写和语法校正等常规编辑等相关例外情形。指南还说明了如何证明符合《人工智能法》的透明度义务，以强化法律确定性并提供简便务实的合规证明途径。《人工智能法》部分规则将自 2026 年 8 月 2 日起适用。委员会正积极推出指南、行为准则以及“人工智能法服务台”（AI Act Service Desk）等一系列工具。此次指南与欧盟委员会于 6 月发布的《人工智能生成内容透明度行为准则》（Code of Practice on Transparency of AI-Generated Content）相互补充，帮助各类机构更好理解其在该法项下的相关义务。（来源：欧盟委员会）

6. 新加坡 PDPC 发布《生成式人工智能中个人数据使用指导性指南》

7 月 20 日，新加坡个人数据保护委员会发布《生成式人工智能中个人数据使用指导性指南》，明确新加坡《个人数据保护法》（PDPA）在生成式人工智能模型和系统开发、部署及使用过程中的适用要求。

在模型开发阶段，组织通过网络抓取收集包含个人数据的数据集时，可以考虑适用“公开可获得信息例外”，但应判断有关数据是否确实向公众普遍开放。对于设置付费墙、注册要求、身份验证、地域或资格限制、反自动抓取工具等数字障碍的数据，组织应结合障碍的目的和实际效果、访问数据所需步骤，以及相关数据能否从其他网络来源不受限制地取得等因素进行评估。对于用户直接提供，或者在使用产品、服务过程中产生的个人数据，组织可以先判断是否适用同意例外或者推定同意；不适用相关依据时，必须取得用户同意，并说明收集、使用或者披露个人数据的目的。

在部署阶段，指南指出，系统部署者无论自行开发系统，还是采购软件即服务、应用程序接口等外部服务，均对所采用的生成式人工智能系统能否符合 PDPA 要求承担主要责任，并应取得有关上游安全措施的充分信息。对于具有智能体功能的生成式人工智能系统，系统部署者应定期审查保护措施是否充分，并在确定智能体应用范围时，审慎考虑隐私保护与系统效用之间的权衡。在部署后阶段，组织原则上应处理个人提出的访问和更正请求；但如果提供访问会造成不合理的负担或费用、与个人利益不成比例，或者组织有合理理由认为不应

作出更正，可以依据 PDPA 规定不予访问或更正。（来源：新加坡个人数据保护委员会）

7. 美澳加等国网络安全机构联合发布指南《关键基础设施隔离指南——隔离关键系统建议》

7 月 28 日，美国网络安全和基础设施安全局（CISA）、联邦调查局（FBI），以及澳大利亚、加拿大、英国、新西兰等国家的网络安全中心联合发布《关键基础设施隔离指南——隔离关键系统建议》。指南提出，关键基础设施运营者必须有意识、有序地将关键运营技术（OT）系统与所有其他网络断开，并在危机持续期间维持关键服务运行。指南提出实现系统隔离的六个关键步骤：一是识别关键系统和网络，确定支持关键服务的最小必需系统集，涵盖 OT 和 IT 资产。二是识别关键客户。明确依赖该基础设施的上下游实体（如军事设施、生命线服务等）。三是确定网络和主机的关键性和信任等级。将 OT 环境中的设备按关键程度和威胁暴露程度划分适当的安全区域。四是绘制与关键系统的连接图并识别潜在隔离点。记录关键网络与所有其他系统之间的互联点。五是构建有效的隔离点。在关键网络与非关键网络之间建立物理分离和隔离控制。六是制定并测试隔离计划。制定可根据威胁环境恶化程度逐步执行的渐进式隔离计划。（来源：美国 CISA）

8. 美国白宫启动“金鹰计划”，建立网络安全漏洞协调机制

7 月 14 日，美国白宫宣布启动“金鹰计划”（GOLD EAGLE）。该计划是一个由开源软件合作伙伴和美国关键基础设施企业共同建设的网络安全漏洞协调中心，旨在协调接收、验证、排序和修复网络安全漏洞。“金鹰计划”依据美国总统特朗普于 6 月 2 日签署的第 14409 号行政命令《促进先进人工智能创新与安全》设立。美国白宫、财政部、国土安全部及其下属网络安全和基础设施安全局、战争部等机构与产业伙伴共同参与实施。该计划将利用前沿人工智能能力，加快漏洞利用活动的发现和响应，减少重复扫描，并向联邦政府和私营部门的防御人员提供经过优先级排序、具有可操作性的威胁及修复信息。（来源：美国白宫）

9. 因违法收集 Siri 语音数据，苹果被韩国 PIPC 罚款 2.52 亿韩元

7 月 23 日，韩国个人信息保护委员会宣布，因苹果公司在缺乏合法处理依据的情况下收集、利用 Siri 用户的语音录音及转录文本，并在个人信息跨境传输过程中未充分履行告知义务，决定对苹果关联公司 Apple Distribution International Limited（ADI）处以 2.52 亿韩元罚款，同时对另一关联公司 Apple Services Pte. Ltd.（ASPL）作出整改命令。

调查显示，截至 2019 年 8 月，用户使用 Siri 时，苹果会收集相关语音录音及其转录文本，并将其用于改善语音识别功能和搜索结果，

但未就上述处理活动另行取得用户同意。自 2019 年 10 月起，苹果开始就利用语音录音改进服务征得用户同意，但仍在没有另行取得同意或者具备其他合法依据的情况下，将转录文本用于服务改进。所谓转录文本，是指将收集到的语音录音转换为文字后形成的数据。PIPC 还发现，苹果在将用户个人信息传输至美国 Apple Inc.等关联公司时，未在隐私政策中充分说明跨境传输的个人信息种类、接收方的使用目的以及保存和使用期限等法定事项。（来源：韩国个人信息保护委员会）

10. 因违法收集利用第三方行为信息，TikTok 被韩国 PIPC 罚款 103.06 亿韩元

7 月 23 日消息，韩国个人信息保护委员会近日调查核实 TikTok 违反个人信息保护法，存在违法收集、利用第三方行为信息以及违法跨境传输个人信息等行为，决定对 TikTok 处以 103.06 亿韩元罚款，同时作出整改命令和公示命令。

经调查，TikTok 在未经合法授权的情况下，通过其向其他网站和应用分发的行为信息收集工具（如 TikTok Pixel、Events SDK、Events API 等），收集了用户在第三方网站和应用上的活动记录（如点击、购买、加入购物车、咨询、下载、搜索、内容浏览等），即“第三方行为信息”。截至 2025 年 12 月，韩国约有 7.1 万家企业使用 TikTok 的行为信息收集工具，TikTok 据此从 945 万名国内活跃用户处收集了第三方行为信息。

TikTok 将收集到的用户第三方行为信息与移动设备广告标识符（Android 为 GAID，iOS 为 IDFA）及浏览器标识符（Cookie：ttp）等结合，与 TikTok 会员账户关联，通过分析推断用户特征和兴趣偏好，并将其用于定向广告。然而，TikTok 在用户注册时未以明确可见的方式进行告知，而是将相关同意与其他必要个人信息捆绑为强制性同意选项，实质上迫使希望使用 TikTok 服务的用户必须接受为定向广告目的收集第三方行为信息，使得用户无法有效行使自主同意权。此外，TikTok Lite 在提供积分现金提现服务过程中，向关联公司转移用户个人信息时，未公开或告知转移的个人信息项目、接收方的使用目的及保存使用期限等法定事项。委员会认定 TikTok 无法律依据收集使用第三方行为信息及向境外转移个人信息，分别违反了《个人信息保护法》第 15 条第 1 款（个人信息的收集使用）及第 28 条之 8 第 1 款（个人信息的境外转移）。（来源：韩国个人信息保护委员会）

行业前沿观察：各地协会动态

各单位步履不停，党建联建、技能培训、技术研讨、竞赛比武、标准发布、人才对接、科普宣传等多条战线同步推进，从机关到企业，从高校到社区，一条覆盖多场景、多层级、多领域的行业行动线正在展开。广西网络安全协会联合多支部赴龙州开展主题党日活动；茂名市计算机信息网络安全协会成功承办电白区网络和数据安全专题培训活动；市公安局网安支队六大队与武汉市网络安全协会联合开展“迎七一·强党性·保安全”主题党日活动；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；宁波市计算机信息网络安全协会医疗行业数据安全技术研讨会圆满举行；“数智赋能 网联同行”联学联建活动领导嘉宾一行到访广东省网络空间安全协会参观指导；肇庆市信息协会 2026 年肇庆市 CIO 沙龙——卓豪线下研讨会圆满成功；中关村可信计算产业联盟国内首个面向信息系统的可信纵深防御参考架构团体标准发布；海南省网络安全和信息化协会举办“AI+网安”技术交流沙龙；广州网络空间安全协会“密码安全点对点 商密科普零距离”专项系列科普活动开展说明会顺利举行；北京网络空间安全协会入藏国家版本馆--网民网络安全感满意度调查报告捐赠仪式在京举行，2026 年调查活动拉开帷幕搭校企桥梁，筑网安人才生态丨首场人才对接交流会圆满举办，第二期活动筹备中；金华市网商协会金华开发区跨境电商模式报关培训会成功举办；安徽省网络安全协会安徽省等保测评工作规范专题培训会顺利举办；惠州市计算机信息网络安全协会走进中国

移动惠州分公司开展网络与数据安全培训；肇庆市计算机学会获评第十届“创客广东”肇庆市大赛优秀组织奖;珠海市网络空间安全协会数据跨境流动政策与人工智能产业发展推介会成功举办；深圳市网络与信息安全行业协会 2026 年盐田区“网络安全进基层”系列活动成功举办；上海市信息安全行业协会 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圆满落幕；南昌市网络信息安全协会 2026 年南昌市“洪工杯”网络安全行业职工职业技能竞赛线下决赛圆满落幕；上海市信息网络安全管理协会 2026 第五届上海网络安全博览会将于 9 月在沪隆重召开，诚邀参展参会。

关键词：党建联建、行业培训、技术研讨、警协交流、标准发布、科普宣传、技能竞赛、人才对接、展览展会、版本馆入藏、荣誉表彰

1. 广西网络安全协会联合多支部赴龙州开展主题党日活动

为深入贯彻习近平新时代中国特色社会主义思想，庆祝中国共产党成立105周年，广西网络安全协会联合自治区公安厅网安总队第二党支部，组织网络安全企业党支部党员代表于2026年6月25日至26日到崇左市龙州县下冻镇下冻村联合开展“支部共建凝聚合力 警企村同心护安全”主题党日活动，区公安厅网安总队党委委员、副总队长陈而廉参加此次活动。

2. 茂名市计算机信息网络安全协会成功承办电白区网络和数据安全专题培训活动

为深入贯彻落实《中华人民共和国网络安全法》《信息安全技术网络安全等级保护基本要求》等法律法规，全面提升电白区网络和数据安全保障能力，扎实做好广东省第十七届运动会网络安全保障工作，6月25日，由茂名市电白区政务服务和数据管理局主办，茂名市计算机信息网络安全协会承办，中国联合网络通信有限公司茂名市分公司、广东比特豹科技有限公司、北京时代新威信息技术有限公司、广东深界科技有限公司协办的“筑牢数字政府防线护航电白高质量发展”网络和数据安全专题培训活动成功举办。来自全区各街道（镇）、区直有关单位的网络安全管理员及技术骨干参加培训。

3. 武汉市公安局网安支队六大队与市网络安全协会联合开展“迎七一·强党性·保安全”主题党日活动

2026 年 6 月 30 日下午，在中国共产党成立 105 周年即将到来之际，武汉市公安局网络安全保卫支队六大队党支部与武汉市网络安全协会党支部在武汉警察博物馆联合开展“迎七一·强党性·保安全”主题党日活动。双方党员通过共学党史、共研安全、共谋发展，深化了警会协同共识，凝聚了守护网络空间的强大合力。

4. 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。

5. 宁波市计算机信息网络安全协会医疗行业数据安全技术研讨会圆满举行

7 月 2 日，医疗行业数据安全技术研讨会圆满举行。本次研讨会由第一医院人工智能与信息化部部长吴斌主持，市公安局、市卫健委、安全协会、全市多家医院代表及行业技术专家齐聚一堂，围绕医疗数据合规管理与技术防护体系建设展开深入研讨，旨在为医疗行业数据全生命周期管理提供可行路径。

6. “数智赋能 网联同行”联学联建活动领导嘉宾一行到访广东省网络空间安全协会参观指导

7 月 7 日，由中国网络社会组织联合会主办、广东省互联网业联合会承办“数智赋能 网联同行”联学联建活动期间，中网联有关部门负责人及会员单位代表到访广东省网络空间安全协会参观指导。

7. 肇庆市信息协会 2026 年肇庆市 CIO 沙龙——卓豪线下研讨会圆满成功

7 月 7 日，由肇庆市计算机学会、肇庆市信息协会携手卓豪（ManageEngine）举办的肇庆市 CIO 沙龙——卓豪线下研讨会在肇庆品臻酒店成功举行。来自风华高科、星湖科技、宏华科技、永达辉集团、高峰机械、广东邦科、风华新能源、四会互感器、金龙宝电子、恒港电力、绿宝石电子、三浦科技、新明珠集团、广东邦健、广东鸿劲、金叶集团、博士芯电子、苏泰精密、欧陆新材料、肇水集团、铝遊家科技、中科威科、和佳电子、大润发等优秀企业的负责人、CIO 及技术专家受邀齐聚一堂，共探数字化运维新趋势，共话数智未来！

8. 中关村可信计算产业联盟国内首个面向信息系统的可信纵深防御参考架构团体标准发布

2026 年 7 月 9 日，中关村可信计算产业联盟正式发布《面向信息系统的可信纵深防御参考架构》团体标准，并将于 2026 年 10 月 9 日正式实施。该标准由网商银行牵头联合 10 余家行业龙头、科

研院所与安全机构共同编制，为未来企业信息安全防护体系的演进方向提供了一个可行指引，有助于解决企业数字化、智能化发展过程中的安全挑战。

9. 海南省网络安全和信息化协会举办“AI+网安”技术交流沙龙

2026 年 7 月 10 日，海南省网络安全和信息化协会在海口龙华数字经济产业园举办“AI+网安”技术交流沙龙。来自省内网络安全、信息化领域的专家学者、企业代表齐聚一堂，围绕人工智能与网络安全融合发展这一前沿话题展开深入研讨。

10. 广州网络空间安全协会“密码安全点对点 商密科普零距离”专项系列科普活动开展说明会顺利举行

2026 年 7 月 17 日上午，“密码安全点对点 商密科普零距离”专项系列科普 活动开展说明会以线上形式顺利举行。本次会议在广州市密码管理局指导下，由广州网络空间安全协会、广州市商用密码产业联盟联合主办，广东省网络空间安全协会支持举办。首批承办单位代表线上参会。

11. 北京网络空间安全协会入藏国家版本馆--网民网络安全感满意度调查报告捐赠仪式在京举行，2026 年调查活动拉开帷幕搭校企桥梁，筑网安人才生态丨首场人才对接交流会圆满举办，第二期活动筹备中

2026 年 7 月 20 日下午，由中国国家版本馆、网民网络安全感满意度调查活动组委会、北京网络空间安全协会联合主办的“网民网络安全感满意度调查报告捐赠仪式暨 2026 网民网络安全感满意度调查活动启动”在中国国家版本馆文华堂举行。来自全国各地的调查活动发起单位代表、高校代表和志愿服务团队代表参加本次活动。

12. 金华市网商协会金华开发区跨境电商模式报关培训会成功举办

为帮助跨境电商企业涉税申报合规，近日，由金华市网商协会协办的金华开发区跨境电商模式报关培训会在菁英产业园成功举办，开发区 100 余名跨境电商企业代表到场参训。

13. 安徽省网络安全协会安徽省等保测评工作规范专题培训会顺利举办

为深入落实《网络安全法》《网络安全等级保护条例》工作要求，统一全省等保测评项目实施流程与报告编制标准，全面提升测评机构从业人员专业能力与合规执业水平，有效防范测评全流程安全风险，7 月 22 日，由安徽省网络安全协会等保专委会主办的安徽省网络安全等级保护测评工作规范专题培训会在合肥蜀山区工投高新智谷 B5 栋成功召开。本次培训采用线下主会场+腾讯会议线上同步直播模式，全省在皖开展等保测评业务的机构负责人、项目负责人、测评师、渗透测试工程师、报告编制骨干等业务人员参与培训。

14. 惠州市计算机信息网络安全协会走进中国移动惠州分公司开展网络与数据安全培训

7 月 27 日，惠州市计算机信息网络安全协会赴中国移动惠州分公司开展网络与数据安全专题培训，培训对象为公司派驻各业主单位的实施人员。培训着力提升一线实施人员服务业主单位的网络安全专业能力，推动网络安全防护要求融入项目实施全过程，同时同步开展安全专业证书申报及考证相关工作，助力从业人员完善资质配置。

15. 肇庆市计算机学会获评第十届“创客广东”肇庆市大赛优秀组织奖

2026 年 7 月 28 日，第十届“创客广东“肇庆市中小企业创新创业大赛决赛暨颁奖仪式”顺利举办。肇庆市计算机学会积极动员组织会员企业参赛，扎实开展赛事宣讲、项目组织与对接服务，获评大赛优秀组织奖；多家会员企业参赛项目凭借技术优势与产业化潜力斩获重要奖项。

16. 珠海市网络空间安全协会数据跨境流动政策与人工智能产业发展推介会成功举办

7 月 28 日下午，由粤港澳大湾区生成式人工智能安全发展联合实验室珠西中心指导，珠海市网络空间安全协会（以下简称“协会”）主办，中电南方软件园、珠海海岸数智科技有限公司、中山大学软件工程学院承办的“数据跨境流动政策与人工智能产业发展推介会”在

中电南方软件园隆重举行。会上，“人工智能安全和数据跨境流动工作服务站”正式揭牌成立，标志着我市在构建数据合规与 AI 安全产业服务体系上迈出了关键一步。

17. 深圳市网络与信息安全行业协会 2026 年盐田区“网络安全进基层”系列活动成功举办

为切实提高市民网络安全防范技能，增强全社会网络安全意识，在中共深圳市委网络安全和信息化委员会办公室的指导下，深圳市网络与信息安全行业协会（下称“协会”）正在全市各区党政机关、企事业单位、居民社区、工业园区等基层单位深入开展“网络安全进基层”系列教育活动。

18. 上海市信息安全行业协会 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圆满落幕

7 月 30 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闭幕式在浦东软件园三林园顺利举办，历经两个多月的赛事圆满收官。市职工技术协会、浦东新区总工会、浦东新区网信办、三林镇总工会、市信安行业协会、浦东软件园三林园等相关单位的领导，参赛选手、参赛单位代表、嘉宾、专家学者及媒体记者等 80 余人出席了闭幕式活动。

本次大赛紧扣数字中国战略部署，深度融入上海城市数字化发展

布局，以“匠心铸盾，数智护航”为主题，聚焦人工智能时代数据安全治理与软件供应链安全防护等重点领域，通过技能竞技、攻防实战博弈等形式，提升从业人员专业技能，挖掘优质数字安全人才，为上海筑牢数字安全屏障、赋能数字经济高质量发展夯实人才与技术根基。

19. 南昌市网络信息安全协会2026年南昌市“洪工杯”网络安全行业职工职业技能竞赛线下决赛圆满落幕

2026年7月31日，由中共南昌市委网信办、南昌市总工会联合主办，南昌市网络信息安全协会协办的2026年南昌市“洪工杯”网络安全行业职工职业技能竞赛线下决赛圆满落幕。市委宣传部分管日常工作的副部长、市委网信办主任熊中高出席启动仪式并致辞。

20. 上海市信息网络安全管理协会2026第五届上海网络安全博览会将于9月在沪隆重召开，诚邀参展参会

本届展会将全面覆盖网络安全全产业链技术、产品与解决方案，精准锚定2026年数字安全发展核心趋势与关键防护需求，聚焦前沿技术创新、核心安全能力建设与行业场景化落地。展会汇聚国内外顶尖网络安全企业、科研机构及专业力量，全方位展示新一代网络安全技术成果与实战化防护方案，为政企单位、关键信息基础设施运营者及各行业用户搭建技术交流、商贸对接、采购选型、生态合作的一站式专业平台，助力筑牢数字安全屏障，推动网络安全产业高质量发展。

诚邀全球网络安全企业、科研机构及生态伙伴共赴盛会，携手共创数字安全新未来！