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9月第9期（总第38期）

2026年9月15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 9 月第 9 期（总第 38 期）

2026 年 9 月 15 日

主办单位：公安部第三研究所网络安全法律研究中心
联合主办：北京网络空间安全协会
牵头组织：网安联秘书处
协办单位：网安联认证中心
技术支持：北京关键信息基础设施安全保护中心

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：8 月，公安部、国家互联网信息办公室围绕网络空间安全监督检查、个人信息保护发布相关制度文件，进一步厘清数据安全风险评估相关要求；地方层面，浙江、上海、海南、河北、山西、江西、山东围绕地方数据资源保护和利用、行政处罚裁量基准、网络安全等发布相关规范性文件。

部委层面，公安部发布《公安机关网络空间安全监督检查办法》，修订 2018 年《公安机关互联网安全监督检查规定》，对监督检查对象、内容等予以完善，以适应新形势下公安机关维护网络空间安全需要。国家互联网信息办公室发布《大型个人信息处理者个人信息保护规定（征求意见稿）》，明确大型个人信息处理者的认定标准，落实《个人信息保护法》关于处理大量个人信息的个人信息处理者的特殊要求。中央网络安全和信息化委员会印发《促进网信企业高质量发展行动计划（2026—2030 年）》，提出企业培育服务行动、安全有序发展行动等 7 项行动 21 条举措。

地方层面，河北、山西发布本省数据条例征求意见稿，江西发布《江西省公共数据资源授权运营价格管理办法（试行）》，明确相关主体对数据的持有权、使用权、经营权等权益，推动地方数据授权运营工作。浙江省印发《关于促进直播经济规范健康发展的意见》，要求加强直播行业综合治理，推动行业健康发展。海南省互联网信息办公室发布《海南自由贸易港网络安全条例（征求意见稿）》，提出海南自由贸易港领域内网络安全管理要求。上海市经济和信息化委员会印发《上海市经济和信息化领域行政处罚裁量

权基准适用规定》，吸收《行政处罚法》的相关规定，提出经济和信息化领域行政处罚裁量基准。

关键词：监督检查；大型个人信息处理者；数据授权运营

（一）部委层面动向

1. 公安部发布《公安机关网络空间安全监督检查办法》

8 月 6 日，公安部发布《公安机关网络空间安全监督检查办法》，自 2026 年 10 月 1 日起施行。

当前，网络空间安全形势严峻复杂，公安机关坚持履行法定职责，进一步规范和加强对网络空间安全的监督检查。近年来，国家出台了《数据安全法》《个人信息保护法》等法律法规，需要对 2018 年《公安机关互联网安全监督检查规定》进行修订，对监督检查的对象、内容等予以完善，以适应新形势下公安机关维护网络空间安全的需要。

《办法》共 23 条，主要规定六方面内容：一是明确监督检查对象，包括网络运营者、数据处理者、个人信息处理者等；二是明确监督检查方式，包括线上巡查、线下核查，日常检查、专项检查等；三是明确监督检查内容，包括被检查对象是否履行法定的网络空间安全义务，以及重大活动安保期间的重点检查内容等；四是明确监督检查机制，要求在国家网络安全、数据安全等机制统筹协调下，加强部门协调、联合检查，减少企业负担；五是明确检查结果运用，公安机关按检查情况采取督促整改、发送公安提示函以及处罚等措施；六是明确相关法律责任，明确了公安机关及工作人员玩忽职守、滥用职权、泄露国家秘密等法律责任。

《办法》对健全联合检查机制、减少企业负担作出规定。公安机关应当建立健全与有关部门的监督检查协作配合机制，加强跨部门协

同配合、信息沟通，合理确定现场检查的频次、范围、方式，避免重复检查、交叉检查。公安机关对相关行业开展现场检查的，应当事先告知网信部门、行业主管部门，尽量联合开展检查，减少企业负担。同时，鼓励采用线上巡查等方式开展检查，最大程度降低对企业经营的影响。

《办法》对公安机关执法规范化建设提出进一步要求，明确公安机关开展监督检查的人员、文书等具体要求，以及委托技术支持机构协助开展检查的安全管理要求。对采取漏洞探测、渗透性测试等方式开展远程检测的，要求由地市级以上公安机关组织实施。同时，规定了公安机关及其工作人员对工作中知悉的国家秘密、工作秘密、商业秘密、个人隐私、个人信息等的保密责任。通过进一步规范监督检查的程序，着力提升公安机关执法规范化水平。（来源：公安部）

2. 国家网信办发布《大型个人信息处理者个人信息保护规定（征求意见稿）》

8 月 7 日，国家互联网信息办公室发布《大型个人信息处理者个人信息保护规定（征求意见稿）》，共六章五十条，包括个人信息处理规则、大型个人信息处理者义务、个人信息保护监督委员会等内容。

征求意见稿明确，对大型个人信息处理者的认定，应当综合考虑下列条件：（一）处理 1000 万人以上自然人个人信息；（二）提供涉及个人信息处理的重要网络服务，或者经营范围涵盖多种业务且涉

及个人信息处理；（三）个人信息处理活动对国家安全、经济运行、社会稳定、公共健康和安全等具有重要影响。

征求意见稿要求，大型个人信息处理者应当选择符合下列条件的数据中心，存储在中华人民共和国境内运营中收集和产生的个人信息：（一）设立在中华人民共和国境内；（二）数据中心管理机构的法定代表人或者实际控制人具有中华人民共和国国籍；（三）符合国家有关政策标准要求。

征求意见稿规定，大型个人信息处理者应当围绕个人信息处理活动、个人行使权利响应、安全义务履行等环节，建立健全内部管理制度和操作规程，加强个人信息安全监测预警，及时发现处置个人信息安全问题和事件，防范安全风险。（来源：网信中国）

3. 公安部、国家网信办发布《网络数据安全风险评估办法》实施有关事项答记者问

8 月 20 日，公安部、国家互联网信息办公室有关负责人就《网络数据安全风险评估办法》实施有关事项发布答记者问。

关于如何申请网络数据安全风险评估服务认证方面，公安部有关负责人答复，《办法》第八条规定：“鼓励相关评估机构通过认证。评估机构的认证按照《中华人民共和国认证认可条例》的有关规定执行”。国家网信办数据与技术保障中心、公安部第三研究所、泰尔认证中心有限公司等认证机构已向国家认证认可监督管理委员会备案

《数据安全风险评估服务认证规则》，相关认证机构将依据认证规则和有关标准规范实施认证。评估机构可向上述认证机构申请服务认证。

关于公安机关在网络数据安全风险评估工作中承担哪些法定职责，以及具体有哪些落实举措方面，公安部有关负责人答复，依照有关法律法规规定，在国家数据安全工作协调机制指导下，公安部将会同中央网信办、工业和信息化部等有关部门，建立网络数据安全风险评估专项工作机制，指导、监督网络数据安全风险评估工作。

为确保《办法》落地见效，公安机关将立足法定职责，建立全流程监管机制。依托网络安全等级保护备案等基础工作，掌握辖区内网络数据处理者相关情况，建立并完善动态监管台账。对重要数据处理者的风险评估报告真实性、准确性进行检查核验。对发现存在较大安全风险、发生数据安全事件等情形的，依法督促网络数据处理者委托通过认证的第三方评估机构开展风险评估。发现重要数据处理者的重要数据处理活动可能危害国家安全、公共利益的，依法责令整改；对拒不整改或未达到整改要求的，依法采取责令其停止处理重要数据等措施。对未按规定开展风险评估的网络数据处理者，将依据《数据安全法》《网络数据安全管理条例》等有关法律、行政法规予以处理；第三方评估机构违反《办法》开展风险评估的，公安机关将依法予以处理。

关于重要数据处理者如何报送网络数据安全风险评估报告方面，国家互联网信息办公室有关负责人答复，《办法》第十六条规定：“重要数据处理者应当在年度风险评估完成后的20个工作日内按照有关

主管部门要求向其报送风险评估报告。主管部门不明确的，向省级网信部门或者国家网信部门报送。”主管部门不明确的重要数据处理者可联系咨询各地网信部门报送风险评估报告事宜。（来源：公安部）

4. 中央网信委印发《促进网信企业高质量发展行动计划（2026—2030 年）》

8 月 21 日消息，中央网络安全和信息化委员会近日印发《促进网信企业高质量发展行动计划（2026—2030 年）》，提出企业培育服务行动、安全有序发展行动、发展要素保障行动等 7 项行动 21 条举措。

安全有序发展行动方面，《行动计划》提出，加强网络法治建设。加快推进人工智能、反网络暴力、数字经济、网络平台、区块链等新兴领域立法。推进修订《互联网信息服务管理办法》，完善互联网信息服务管理、“自媒体”管理、算法治理等法律制度。推进制定电信法、网络犯罪防治法、网络安全等级保护条例，完善《未成年人网络保护条例》《网络数据安全管理条例》配套规定。规范涉网信企业行政检查，最大限度减少对网信企业正常生产经营活动的干扰。健全适应互联网发展治理新特点的监督管理执法措施，严厉打击网络违法违规行为。

发展要素保障行动方面，《行动计划》提出，强化数据保障。鼓励引导网信企业建立健全数据安全合规体系，指导帮助企业高效合规开展数据处理活动。高效实施数据出境安全评估、个人信息出境标准

合同、个人信息出境认证等制度。支持自由贸易试验区等在国家数据分类分级保护制度框架下，制定发布数据出境负面清单，建立符合“东数西算”工程布局和有关政策要求的云计算基础设施，面向外资企业、中小企业等提供数据处理服务。组织重点行业领域制定网络数据跨境流动合规指引，鼓励有条件的地区设立数据跨境服务中心，开展数据跨境咨询服务。鼓励生态主导型、产业引领型企业面向中小企业提供普惠性数据产品和技术工具。依法严厉打击涉数据违法犯罪活动。（来源：网信中国）

（二）地方层面动向

1. 浙江省两部门印发《关于促进直播经济规范健康发展的意见》

6 月 10 日，中共浙江省委办公厅、浙江省人民政府办公厅印发《关于促进直播经济规范健康发展的意见》，围绕激发主体活力、拓展发展空间、完善治理体系等四个方面，提出二十项措施。

完善治理体系方面，《意见》提出，推进穿透式监管。迭代升级直播电商智慧监测平台，提升直播电商人防物防技防能力。制定重点直播间账号管理清单，落实关联网络账号绑定管理，推广国家网络身份认证公共服务。探索建立直播经济领域监管研判机制，对新业态发展中出现的技术、市场、安全、法律等方面问题进行场景化、差异化监管评估。

优化发展生态方面，《意见》提出，构建协同共治机制。在直播平台、重点直播服务机构中强化党的组织覆盖和工作覆盖。加强部门协作，坚持线下线上一体化监管，强化信息互通、会商研判、系统共建。引导行业自律，加强社会监督，探索建立公众和第三方专业机构共同参与的监督机制。（来源：浙江省政府）

2. 上海市人民政府办公厅印发《上海市“数字上海”建设“十五五”规划》

7 月 28 日，上海市人民政府办公厅印发《上海市“数字上海”建设“十五五”规划》，围绕强化场景引领、聚力开放协同、深化数实融合等五个方面，提出二十条措施。

聚力开放协同方面，《规划》提出，建强国际数据服务设施。放大数据领域国际合作上海综合试点牵引带动作用。提升国际网络设施服务能级，推进互联网国际出口带宽扩容，完善国际专线、跨境组网和网络加速等服务体系。打造“出海一张网”，推动算力网、链路网、数据网协同建设。深化跨境存算设施部署，在临港、虹桥、东方枢纽等地加快建设国际数据中心，支持境外数据中心和云服务节点在上海布局。推进跨境跨链网关基础设施布局。

深化数实融合方面，《规划》提出，激活数据要素应用新价值。健全以《上海市数据条例》为基础的“1+X”地方立法体系，用好浦东新区法规立法授权，探索出台一批数据领域地方性法规。强化数据要素全生命周期管理，理顺数据要素市场化配置机制。推动高质量数

据集赋能关键领域、重点产业发展，搭建面向人工智能的高质量数据集社区。积极引导经营主体参与数据要素市场化配置。深化数据产品知识产权登记试点。推进数据产权登记及应用。推动多元主体联合，加快建设重点行业可信数据流通基础设施。（来源：上海市政府）

3. 上海市经济和信息化委员会印发《上海市经济和信息化领域行政处罚裁量权基准适用规定》

7 月 29 日，上海市经济和信息化委员会印发《上海市经济和信息化领域行政处罚裁量权基准适用规定》，共十三条，自 2026 年 9 月 1 日起施行，有效期至 2031 年 8 月 31 日。

文件提出，裁量因素是指判断当事人具体违法行为在同种类违法行为中情节轻重的因素，主要包括以下内容：（1）违法行为持续时间；（2）违法行为发生次数；（3）当事人主观过错程度；（4）违法行为危害对象；（5）违法行为手段、方式、规模；（6）违法行为危害后果；（7）当事人改正情况；（8）当事人配合检查、调查情况。其中，违法行为发生次数是指自本次违法行为发生之日（含本日）起向前追溯两年内，当事人因相同违法行为被处理的次数总和，包括行政处罚、认定违法行为成立的不予行政处罚、责令改正。

文件强调，当事人有下列情形之一的，从重行政处罚：（1）违法情节恶劣，造成严重危害后果的；（2）经责令改正后，继续实施违法行为的（罚则对拒不改正情形已作出处罚规定的除外）；（3）伪造、隐匿、毁灭违法行为证据的；（4）阻碍执法人员依法查处违法行为

的；（5）多次实施违法行为的；（6）共同违法行为中起主要作用，或者教唆、胁迫、诱骗他人实施违法行为的；（7）对举报人、证人或者执法人员打击报复的；（8）发生重大传染病疫情等突发事件，违反突发事件应对措施的。上述情形已作为行政处罚裁量因素的，不再重复作为从重行政处罚的考量情节。从重行政处罚的，应当在裁量权基准明确的拟罚款金额的基础上增加一定罚款金额，一般不超过法定罚款幅度的30%，且增加后的最终罚款金额不高于法定最高罚款金额。（来源：上海市经济和信息化委员会）

4. 海南省互联网信息办公室发布《海南自由贸易港网络安全条例（征求意见稿）》

8月3日，海南省互联网信息办公室发布《海南自由贸易港网络安全条例（征求意见稿）》，共七章三十五条，包括网络运行安全、网络信息安全、数据跨境流动的安全保障等内容。

网络运行安全方面，征求意见稿提出，在海南自由贸易港范围内从事网络运营、数据处理、提供网络产品与服务的单位，应当明确网络安全管理负责人。网络安全管理负责人应当组织落实网络安全管理制度和应急预案；组织开展网络安全风险排查、宣传教育和必要的应急演练；配合监管部门开展网络安全检查、事件处置与投诉处理。网络安全管理负责人应当熟悉网络安全法律法规，具备网络安全专业知识和相关管理工作经历，由单位主要负责人或其授权的高级管理人员担任。

网络信息安全方面，征求意见稿提出，海南省网信部门会同有关部门探索制定海南自由贸易港国际互联网信息内容负面清单，并依托该清单建立网络安全风险监测预警、研判及处置机制。对于国际互联网平台上中华人民共和国法律、行政法规禁止发布或者传播的信息传播至海南自由贸易港内网络平台的，海南省网信部门依法实施监督检查和电子数据取证；对监测发现或经举报核实的违法信息，依据危害程度和影响范围实行分级分类处置，依法通知相关运营者采取包括但不限于警示、停止传输、限制功能、阻断访问在内的技术措施。（来源：海南省互联网信息办公室）

5. 河北省数据和政务服务局发布《河北省数据条例》征求意见稿

8 月 12 日，河北省数据和政务服务局发布《河北省数据条例》征求意见稿，共八章五十一条，包括数据资源、数据权益、数据产业等内容。

征求意见稿强调，自然人、法人和非法人组织对其依法获取的或者合法收集的数据，按照法律、行政法规规定享有持有权、使用权、经营权等权益。公共管理和服务机构在履行公共管理和服务职责过程中生成、收集和处理的各类数据，依法享有管理、使用等权限；企业在生产经营活动中合法生成、收集和获取的数据，自然人对其在个人生活、非职务行为中合法生成和收集的数据，依法享有相应权益；法律另有规定的，从其规定。

征求意见稿提出，自然人、法人和非法人组织可以依照法律规定或者合同约定，委托他人处理数据，受托人对委托处理的原始数据、过程数据、结果数据不享有持有权、使用权、经营权；法律另有规定的，从其规定。数据处理者对其合法持有的数据以及通过加工、分析等形成的数据产品和服务，依照法律规定或者合同约定享有数据使用、经营等权益。（来源：河北省数据和政务服务局）

6. 山西省司法厅发布《山西省数据条例（草案）》征求意见稿

8 月 14 日，山西省司法厅发布《山西省数据条例（草案）》征求意见稿，共十章六十五条，包括数据权益、数据资源、数据流通等内容。

征求意见稿提出，自然人、法人和非法人组织对使用自动化工具收集的公开数据，依法享有数据持有权和使用权；在不实质性替代数据被收集方的数据产品和服务的前提下，可以对外提供数据产品和服务。自然人、法人和非法人组织使用自动化工具收集数据，不得有非法侵入他人网络、干扰他人网络服务正常运行、破坏有效技术措施以及其他损害他人合法权益的行为。

征求意见稿指出，县级以上人民政府应当建立数据安全工作协调机制，落实网络安全等级保护制度、数据分类分级保护制度和数据安全风险评估等要求，将安全贯穿数据收集、开发、流通、使用等全过

程，构建政府、企业、社会多方协同的数据安全治理体系。（来源：山西省司法厅）

7. 江西省发展改革委、江西省数据局印发《江西省公共数据资源授权运营价格管理办法（试行）》

8 月 20 日，江西省发展和改革委员会、江西省数据局印发《江西省公共数据资源授权运营价格管理办法（试行）》，自 2026 年 10 月 1 日起施行，试行期 2 年。《办法》共七章二十一条，包括定价范围与权限、定价程序与规则、最高准许收入核定等内容。

《办法》提出，公共数据资源授权运营主体或授权主体指定的机构应当指导运营机构建立数据产品和服务项目清单。对用于公共治理、公益事业的，免费提供；对用于产业发展、行业发展的，可收取公共数据运营服务费。

《办法》规定，制定或调整公共数据运营服务费标准，按照以下程序进行：一是核定最高准许收入。由有定价权限的发展改革部门会同数据主管部门，按照“补偿成本、合理盈利”的原则，核定运营机构的最高准许收入；二是制定上限收费标准。授权主体在核定的最高准许收入范围内，统筹考虑应用场景、数据资源投入、人力资源投入及销售规模等因素，制定各类数据产品和服务的上限收费标准，并书面报告同级发展改革部门、数据主管部门；三是确定具体收费标准。运营机构在不高于上限收费标准的范围内，根据市场供需情况自主确

定具体收费标准。具体可按产品数量、服务次数、服务时间、数据调用量等形式收费。（来源：江西省发改委）

8. 山东省工业和信息化厅发布《山东省新一代信息技术产业高质量发展行动计划（2026—2030 年）（征求意见稿）》

8 月 25 日，山东省工业和信息化厅发布《山东省新一代信息技术产业高质量发展行动计划（2026—2030 年）（征求意见稿）》，提出十项重点领域行动，围绕强化自主创新、培强优质主体、促进区域协同等六个方面提出十八项实施措施。

重点领域行动方面，征求意见稿提出，实施人工智能融通赋智行动。提升人工智能产业供给能力，加快优化“智算设备—智算网络—云边协同”算力产业布局，持续做强数据采集、数据语料、数据治理等关键环节，实施大模型产业“双百工程”，培育一批智能手机、智能家居、智能穿戴等新一代智能终端。以“人工智能+”行动为引领，深化人工智能技术在工业、农业、服务业的融合赋能，拓展更多应用场景，加快形成从智能算力、数据语料、算法模型到智能应用的全链条、全栈式人工智能产业链。（来源：山东省工业和信息化厅）

境内前沿观察二：治理实践

导读：8 月，公安机关、网信部门、通信管理部门等围绕个人信息保护、人工智能技术滥用治理、信息内容生态治理等领域持续推进治理实践。

公安机关方面，公安部发布多起涉侵犯公民个人信息、涉影视行业网络舆情、涉吉隆泥石流网络谣言典型案件。上海、新疆、北京等地公安机关打击网络黑灰产取得显著成效，针对游戏外挂、抢票软件等开展执法工作。

网信部门方面，国家网信办启动对美国派拓公司网络安全审查。中央网信办、工业和信息化部、公安部会同相关部门联合开展的 2026 年个人信息保护系列专项行动取得阶段性成效，已开展教育、交通、卫生健康、金融等领域个人信息风险排查，累计摸排 9 万余家企业和机构，发现并督促整改各类隐患问题 1.2 万余个。中央网信办开展的“清朗·网络娱乐团播乱象整治”专项行动、“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动取得阶段性成果。上海市网信办集中约谈平台履行未成年人网络保护要求，并开展涉汽车行业网络传播治理、网络娱乐团播乱象集中治理两项专项行动。

此外，最高人民检察院发布一起利用抓包软件篡改退款数据案，主犯蔡某因利用系统漏洞，通过他人订单非法退款，被判诈骗罪。

关键词：个人信息保护、网络谣言治理、网络安全审查

（一）公安机关治理实践

1. 公安部网安局公布打击侵犯公民个人信息犯罪 10 起典型案例

8 月 11 日，公安部网安局发布打击侵犯公民个人信息犯罪 10 起典型案例。

案例一：杨某国等人侵犯公民个人信息、买卖国家公文证件案。近日，辽宁沈阳公安网安部门成功侦破一起侵犯公民个人信息案，打掉一个以“高薪兼职注册营业执照”为名实施身份盗用的犯罪团伙。经查，杨某国（男，25 岁）伙同谢某才（男，29 岁）成立“**网络”工作室，组织多名公司人员与中介人员对接，通过“执照充场”等名义，以首次注册营业执照给予 200 元、后续完成手续再结 200-300 元为诱饵，招募不明真相人员携带身份证原件来到现场，进行手持身份证拍摄，非法注册电商账号及工商营业执照。杨某国等人以每条 100-300 元不等的价格，将这些账号出售给下游买家，最终流入涉赌、涉电诈犯罪团伙之手，用于非法支付结算或洗钱。查明，杨某国等人非法获取公民个人信息 3000 余条，涉案金额 20 余万元。目前，该案 27 名犯罪嫌疑人已被依法采取刑事强制措施。

案例二：崔某伟、马某洒等人侵犯公民个人信息案。近日，甘肃临夏公安网安部门从一起电信网络诈骗案件入手，成功扩线侦破一起侵犯公民个人信息案。经查，以崔某伟（男，38 岁）为首的犯罪团伙利用社交软件、短视频平台发布兼职广告，以“闲置账号高价变现”

的名义，大量收购微信、QQ、抖音等各类实名网络账号，并吸引群众提供本人及身边亲友的手机号等信息，注册各类网络账号，层层转卖至境外诈骗团伙，用于实施电信网络诈骗等违法犯罪活动，致使出售网络账号的“号主”成为犯罪分子“帮凶”，严重危害公民个人信息安全及财产安全。查明，崔某伟等人非法获取公民个人信息2万余条，涉案金额130余万元。目前，该案6名犯罪嫌疑人已被依法移送起诉。

案例三：刘某沅等人侵犯公民个人信息案。安徽宣城公安网安部门侦破一起利用黑客技术挖掘系统漏洞、搭建数据查询接口、非法贩卖公民个人信息案。经查，刘某沅（男，20岁）伙同韦某影（男，18岁）、林某（男，18岁）在互联网上搭建社工库，通过收费查档方式，为下游律师、私家侦探、信息中介等群体非法提供公民个人信息查询服务，严重危害公民个人信息安全。查明，刘某沅等人非法获取公民个人信息一批，涉案金额30余万元。目前，该案9名犯罪嫌疑人已被依法移送起诉。

案例四：李某等人侵犯公民个人信息案。近日，四川内江公安网安部门侦破一起侵犯公民个人信息案。经查，李某（男，31岁）伙同李某（女，31岁）在抖音等平台发布“订单解密”广告，向抖音商家推销订单解密业务，同时，指使陈某威（男，28岁）、周某宇（男，30岁）向快手、小红书等平台电商直播间商家推销订单解密业务。上述4人批量获取电商平台订单数据后，由徐某峰（男，38岁）提供技术支持，对订单进行解密，非法获取订单手机号码、收件地址等个人

信息，出售给下游黑灰产团伙，严重危害公民个人信息安全及财产安全。查明，李某等人非法获取公民个人信息200余万条，涉案金额800余万元。目前，上述5名犯罪嫌疑人已被依法移送起诉。

案例五：吴某通等人侵犯公民个人信息案。近日，广东佛山公安网安部门侦破一起侵犯公民个人信息案。佛山公安网安部门接报案，称某房产中介公司经纪人数据遭批量泄露，被用于装修业务精准营销。经查，吴某通（男，36岁）伙同罗某德（男，21岁）等人以广东某科技有限公司为掩护，指使陈某杰入职某房产中介公司，以获取该房产中介公司内部系统权限，并雇佣邓某某等人，利用技术手段绕过该房产中介公司内部系统安全机制，批量爬取经纪人个人信息后进行倒卖，供装修公司推销装修使用，并按成单金额的2%抽成，牟取非法利益，严重危害公民个人信息安全。查明，吴某通等人非法获取公民个人信息1.3万余条。目前，该案4名犯罪嫌疑人已被依法采取刑事强制措施。

案例六：王某杰等人侵犯公民个人信息案。近日，山西太原公安网安部门从频繁出现的教培“精准推销”电话入手，成功破获一起涉及学校、教培机构、眼科医院等多行业工作人员侵犯公民个人信息案。经查，王某杰（男，34岁）在教培机构任职期间，为完成招生指标，与韩某（男，52岁）、班某（男，32岁）、马某（男，33岁）、张某（男，34岁）、王某（男，36岁）、张某雯（男，33岁）、崔某（男，36岁）等多个教培机构工作人员非法交换和出售学生数据，王某杰为进一步获取学生信息，又向康某（男，39岁）、苏某全（男，

53 岁）、李某新（男，44 岁）、侯某飞（男，37 岁）等多家眼科医院和学校的工作人员购买大量学生信息，形成了一条“内鬼窃取、行业倒卖、精准推销”的犯罪产业链，严重危害公民个人信息安全。查明，王某杰等人非法获取公民个人信息 50 余万条，涉案金额 30 余万元。目前，该案 12 名犯罪嫌疑人已被依法提起公诉。

案例七：石某、黄某威等人侵犯公民个人信息案。近日，陕西咸阳公安网安部门从频繁出现的装修骚扰电话入手，成功打掉一个隐藏在装修行业，非法获取、买卖公民个人信息的黑产链条。经查，以石某愿（女，33 岁）、黄某威（男，29 岁）为首的犯罪团伙，从装修公司收集个人信息，同时从为政府单位提供数据维护的信息公司、为政府提供拆迁项目的服务公司、小区物业、售楼部、村委会等行业工作人员处，非法购买个人信息，出售给装修公司、家居经营、房产中介等相关行业工作人员，相关行业工作人员获取信息后，又不断对信息层层买卖、交换、牟利，形成了一条涉及行业众多、利益关联庞杂、隐蔽性强的公民个人信息买卖黑灰产业链，严重危害公民个人信息安全。查明，石某、黄某等人非法获取公民个人信息 600 万余条，涉案金额 50 万余元。目前，该案 11 名犯罪嫌疑人已被依法提起公诉。

案例八：董某等人侵犯公民个人信息案。近日，上海公安网安部门侦破一起侵犯公民个人信息案。经查，以董某（男，36 岁）为首的犯罪团伙，成立“某玺”共享充电设备公司，免费向低价旅馆投放共享充电宝，并约定按照使用收益进行分成，吸引大量低价旅馆合作。合作中，该团伙以提供“刷好评、删差评”等网络评价操控服务为条

件，要求宾旅馆非法提供住客姓名、入住时间等公民个人信息，并通过电话回访、使用非法插件等方式，在多个互联网平台实施网络评价操控，提升合作商家网络评分、降低负面评价，以牟取非法利益。该团伙呈公司化运营，下设销售部、技术部、好评部、差评部、售后部等部门，已形成“设备推广获取资源、非法收集个人信息、数据分析筛选、操控网络评价”的完整犯罪链条。查明，董某等人非法获取公民个人信息100余万条,操控网络平台评价10万余条,涉案金额1100余万元。目前，该案33名犯罪嫌疑人已被依法提起公诉。

案例九：夏某强等人侵犯公民个人信息案。近日，江苏宿迁公安网安部门侦破一起侵犯公民个人信息案。查明，夏某强（男，38岁）伙同姜某帅（男，35岁）等人成立“法律咨询”工作室，通过境外社交平台非法获取公民个人的开房记录、车辆档案、出行轨迹等高敏感隐私信息，再打着“法律辅助”“调查支持”的幌子，在“无讼”APP、淘宝、闲鱼、QQ群等网络平台进行推广引流，高价出售给律师、私家侦探、信息中介等特殊群体，用于在办理离婚、讨债、商业竞争等案件中获取不正当优势，严重危害公民个人信息安全，对司法公正和社会秩序造成恶劣影响。查明，夏某强等人非法获取公民个人信息10万余条，涉案金额100余万元。目前，该案10名犯罪嫌疑人已被依法采取刑事强制措施。

案例十：吴某等人侵犯公民个人信息案。近日，浙江舟山公安网安部门成功侦破一起“私家侦探”侵犯公民个人信息案，打掉一个以“私家侦探”“婚姻调查”“寻亲找人”为名义，实施非法调查业务

的犯罪团伙。经查，以吴某（男，34 岁）为首的犯罪团伙在上海成立“上海**探真咨询有限公司”，在微信视频号、抖音等平台发布“私家侦探”类视频进行引流，声称可提供各类“私人调查”服务，在获取客户需求后，通过勾结多行业“内鬼”非法获取受害者行踪轨迹、开房记录等，同时雇佣专人充当“马仔”，实施 GPS 定位、贴身跟踪、偷拍窃录等非法活动，形成了一条分工明确、手段隐蔽的“线上查档+线下跟踪”黑色产业链，严重危害公民个人信息安全。查明，吴刚等人采取线下跟踪和线上查档的方式为 12 人提供非法获取公民个人信息服务，涉案金额 100 余万元。目前，该案 6 名犯罪嫌疑人已被依法移送起诉。（来源：公安部网安局）

2. 国家计算机病毒应急处理中心检测发现 75 款违法违规收集使用个人信息的移动应用

8 月 14 日，国家网络与信息安全信息通报中心发布消息称，2026 年 6 月 23 日至 2026 年 7 月 28 日期间，国家计算机病毒应急处理中心检测发现 75 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）26 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；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）39 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）8 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）4 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）4 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）1 款移动应用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）5 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 款移动应用通过自动化决策方式向个人进行信息推送、商业营销，未同时提供不针对其个人特征的选项，或者未向个人提供便捷的拒绝方式。

（9）5 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中华人民共和国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）22 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）8 款移动应用无隐私政策。（来源：国家计算机病毒应急处理中心）

3. 公安机关破获 3 起针对影视行业的网络舆情敲诈案

8 月 17 日消息，公安机关网安部门近日破获 3 起针对影视行业的网络舆情敲诈案件，累计抓获犯罪嫌疑人 24 名。

案例一：浙江杭州破获针对文娱领域利用舆论实施敲诈案。经查，以李某、廖某为首的犯罪团伙，通过注册成立文化传媒公司，有组织、有预谋、流程化操控网络舆论。该团伙利用实控的多个百万级粉丝量

自媒体账号，长期针对当下热门影视剧、热播综艺和流量明星，拼凑、捏造并发布大量负面信息，形成舆论压力，倒逼受害方主动联系并购买所谓的“护剧”服务，以此非法牟利。该团伙相关犯罪行为严重扰乱文娱产业的健康生态。查清全案后，杭州市公安局开展集中收网行动，抓获犯罪嫌疑人 10 名。经审讯，以李某、廖某为首的团伙对违法犯罪事实供认不讳，案件正在进一步侦办中。

案例二：福建福州破获捏造新剧和明星的“负面信息”实施敲诈案。经查，郑某、黄某二人长期收集新剧和明星的“负面信息”，操控多个网络热门平台账号，炮制、捏造不实内容。每逢热门电视剧播出、艺人公开活动节点，二人便通过其掌控的账号发布负面内容，人为抬高帖文热度，故意制造负面舆论热点。相关影视剧组、艺人经纪团队因担忧负面舆情影响作品口碑、艺人名誉及商业收益，主动联系二人处置负面信息，二人收取费用后即删除相关负面帖文。该行为严重扰乱影视行业正常宣发秩序，破坏网络舆情生态，侵害影视出品方及艺人的合法权益。目前，2 名犯罪嫌疑人已被公安机关依法采取刑事强制措施，案件正在进一步侦办中。

案例三：广东河源破获以“护剧”为名实施敲诈案。经查，李某军团伙成立 MCN 机构，注册某文化传播有限公司，实际控制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 AI（人工智能）工具操控其持有的多个大 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。待相关剧组承受舆论压力、主动联系协商删帖事宜时，李某军便借机

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”服务一般包括发布剧集正向宣传帖文、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，本质是通过操控账号制造负面舆论、变相强迫交易的方式实施敲诈。该案受害方涉及数名知名演员及多部热播电视剧发行方，前期已有多名艺人、多家经纪公司或影视出品方以名誉侵权为由对该团伙提起诉讼。查清全案后，河源市公安局开展集中收网行动，抓获犯罪嫌疑人 12 名。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）

4. 公安部网安局公布 10 起涉吉隆泥石流网络谣言典型案例

8 月 31 日，公安部网安局公布 10 起涉吉隆泥石流网络谣言典型案例。

案例一：西藏昌都公安网安部门查明，网民邱某在某网络平台主观臆断、编造发布“新闻说 1400 人遇难，实际之前有 3000 人失联了”的谣言信息。目前，属地公安机关已依法对该邱处以行政处罚。

案例二：西藏拉萨公安网安部门查明，网民刘某在某网络平台发布“中国这边已经死亡 3000 多人”的谣言信息。目前，属地公安机关已依法对该刘处以行政处罚。

案例三：西藏拉萨公安网安部门查明，网民谭某在某网络平台发布“日喀则吉隆口岸几千人瞬间没命了”的谣言信息。目前，属地公安机关已依法对该谭处以行政处罚。

案例四：西藏拉萨公安网安部门查明，网民张某在某网络平台发布“明明上千人冲走了，官方居然报道3人死亡，265人失踪”“工作人员近200人，建筑工人在500—600人，还有旅游人员与过关人员，至少突破一千人了”的谣言信息。目前，属地公安机关已依法对该张处以行政处罚。

案例五：西藏拉萨公安网安部门查明，网民潘某在某网络平台发布“今天，泥石流淹没了1000多人”的谣言信息。目前，属地公安机关已依法对该潘处以行政处罚。

案例六：西藏拉萨公安网安部门查明，网民易某在某网络平台发布“不算严重，可能死500个人左右、失踪人口可能全部都死了”的谣言信息。目前，属地公安机关已依法对该易处以行政处罚。

案例七：湖南湘西公安网安部门查明，网民周某在某短视频平台发布“广西没完，西藏又来泥石流，听说有上万人死亡，不知道真假，官方还没通告”“去年这里就泥石流死了2—30个”“几千有，这一波泥石流一个寨子就没有了，不止一千”等谣言信息。目前，属地公安机关已依法对该周处以行政处罚。

案例八：内蒙古呼伦贝尔公安网安部门查明，网民国某在某视频评论区发布“起码得有上千人”的谣言信息。目前，属地公安机关已依法对该国处以行政处罚。

案例九：江西南昌公安网安部门查明，网民杨某在某短视频平台发布“失联人数已上升至826人，令人无比痛心！”的谣言信息。目前，属地公安机关已依法对该杨处以行政处罚。

案例十：重庆公安网安部门查明，网民杨某在某短视频评论区发布吉隆口岸泥石流不实死亡人数的谣言信息。目前，属地公安机关已依法对该杨处以行政处罚。（来源：公安部网安局）

5. 新疆博州、昌吉两地公安机关破获房产领域侵犯公民个人信息案

8月，新疆博州、昌吉两地公安机关针对群众反映强烈的房产领域信息泄露问题，接连破获侵犯公民个人信息案件。涉案人员分别通过偷拍物业业主信息台账、非法购买交易数据等方式获取大量业主个人信息，用于电话推销拓展业务，严重侵害公民个人信息安全。

昌吉市公安机关连续接到群众举报，反映当地某房产中介人员在电话推销中精确掌握购房信息，怀疑个人信息遭泄露。经查，昌吉市某房产中介公司工作人员薛某掌握大量业主信息，涵盖多个小区，涉及姓名、住址、楼栋单元、联系电话、房屋面积等具体信息万余条。进一步调查查明，薛某掌握的业主信息均来自原房产公司工作人员母某。母某利用职务之便收集历年交易房屋业主信息，私自留存后出售牟利；薛某为提升业绩从母某处购买大量小区业主信息，随后分发给业务员拨打电话开展精准推销。薛某、母某对其侵犯公民个人信息的

犯罪事实供认不讳。目前，昌吉市公安机关已对薛某、母某采取刑事强制措施，案件正在进一步侦办中。

博乐市公安局接到群众举报，称刚购置新房即接到当地某装修公司工作人员的推销电话，怀疑个人信息遭泄露。经查，该装修公司工作人员李某持有大量业主信息，包含姓名、住址、楼栋单元、联系电话、房屋面积等。李某在物业公司办理业务时，趁物业工作人员离开办公室，偷拍小区业主信息台账并私自留存。目前，博乐市公安局已依法对李某作出行政处罚。（来源：新疆公安网安部门）

6. 河南鹤壁公安网安部门紧急阻断一起境外钓鱼攻击

8 月 4 日消息，河南鹤壁公安网安部门近日成功阻击了一次境外黑客网络攻击，帮助企业及时消除网络安全隐患，有效保护数据安全。

河南鹤壁公安网安部门在日常工作中发现，属地某 IP 地址持续遭受境外网络攻击，网络设备存在被远程控制、数据存在泄露的风险。网警随即开展分析研判，经多方核查后迅速锁定受害企业。河南鹤壁公安网安部门第一时间赶赴相关企业开展现场处置。经询问，企业负责人回忆，近期曾收到一封陌生邮件。邮件以洽谈业务合作为由，附带一份名为“合作合同”的文件，但下载后无法正常打开。这一异常情况立即引起民警警觉。经技术提取和分析，确认该邮件附件并非普通合同文件，而是经过伪装的远控木马下载器。用户点击附件后，恶意程序会在计算机后台自动下载安装远控木马，整个过程隐蔽难察。攻击者一旦取得控制权限，即可远程操作计算机，窃取账号口令、个

人信息、商业资料等敏感数据，甚至将受控设备作为攻击其他系统的“跳板”。属地网警立即组织开展网络安全“体检”，指导企业完善网络安全防护措施，并修复系统漏洞。

目前，鹤壁公安网安部门正在对该案中制作、传播远控木马的相关违法行为开展进一步侦查。（来源：公安部网安局）

7. 河南商丘公安网安部门查处一起未依法履行网络安全保护义务案

8 月 5 日消息，河南商丘网警近日在日常工作中发现，辖区内某学校的网络服务器开放高危端口，疑似持续遭受网络攻击，存在严重的数据泄露风险。

经查，该校在校园网络安全管理中存在多项突出问题：一是防护措施缺失。校园网络未采取必要的安全防护措施，不具备有效的攻击发现、阻断和处置能力；二是网络日志缺位。未按规定监测、记录网络运行状态及网络安全事件，未依法留存相关网络日志；三是高危服务暴露。存储人脸信息及进出轨迹数据的服务器开放高危端口，并开启 Telnet 服务，直接暴露在互联网中，处于高风险状态。相关数据一旦泄露或者被非法利用，不仅会侵害个人信息权益，还可能引发身份冒用、精准诈骗等次生风险。

该校未采取必要的网络安全技术防护措施，未按规定留存网络日志，对存储敏感个人信息的服务器失察失管，未依法履行网络安全保护义务。属地公安机关依据《网络安全法》相关规定，依法对该校作

出行政处罚，并责令其限期改正。校方负责人表示，将深刻汲取教训，积极开展安全整改，严格落实网络和数据安全主体责任。（来源：公安部网安局）

8. 上海公安网安部门打掉一利用外挂软件抢票的犯罪团伙

8 月 6 日消息，上海公安网安部门近日打掉一利用非法外挂软件进行抢票并加价倒卖，牟取非法利益的犯罪团伙，抓获犯罪嫌疑人 4 名。

2026 年 7 月，上海市公安局徐汇分局网安部门工作中发现，某社交平台上有人频繁发布代拍热门演唱会门票的广告帖，引发大量网民关注和讨论。经查，洪某租用办公场地，以“工作室”模式运营，并雇佣陈某、庄某一同从事网络引流、客户对接和线上抢票；朱某单独经营，并与洪某长期保持业务合作。7 月 25 日，警方抓获洪某、朱某等 4 名犯罪嫌疑人，当场查获作案手机 30 余部、电脑 5 台。审讯中，4 名犯罪嫌疑人对使用外挂程序破坏票务系统正常秩序、非法牟利的行为供认不讳。目前，上述 4 名犯罪嫌疑人已被属地警方依法刑事拘留。（来源：公安部网安局）

9. 新疆巴州公安网安部门成功打掉一个网络黑灰产团伙

8 月 7 日消息，新疆巴州公安网安部门近日成功打掉一个操控实名账户跑分洗钱的网络黑灰产团伙。

经查，该团伙以日结150元至180元为诱饵，在劳务市场招聘零散务工人员，指使受聘人员实名注册淘宝、闲鱼、小红书等社交号并提供个人银行卡信息，并对未实名的支付宝账号完成现场刷脸认证。该团伙操控实名注册的网络平台账号和个人银行账户为电信网络诈骗、网络赌博等各类违法犯罪提供转移涉案赃款等“洗白”服务。公安机关现场查获作案手机500余部、营业执照30余张、银行卡20余张、支付账号280余个。目前，团伙17名犯罪嫌疑人（组织者6名）因涉嫌构成帮助信息网络犯罪活动罪被采取刑事强制措施。（来源：公安部网安局）

10. 北京公安部门打掉一个使用抢票软件非法侵入预约平台实施抢票的犯罪团伙

8月13日消息，北京警方近日破获一起非法抢票案，10名犯罪嫌疑人被依法刑拘。

在“净网—2026”专项行动中，北京警方发现一条利用软件非法抢占热门景点景区门票和预约名额的线索。经查，该犯罪团伙成员分散于多省市，组织严密、分工明确，形成完整违法犯罪链条。其中，杨某某、张某瞄准热门景点景区预约需求，针对多个官方预约系统编写非法抢票软件并对外兜售；张某某购得软件后搭建线下运营团队，在互联网招揽客源，使用软件批量抢占门票和预约名额并加价出售，从中非法牟利。2026年7月30日，多地警方密切配合，在五省市同步开展抓捕行动，一举抓获杨某某、张某等10名犯

罪嫌疑人，现场起获电脑、手机等涉案物品。目前，杨某某、张某等 10 名犯罪嫌疑人已被属地警方依法刑事拘留。（来源：公安部网安局）

11. 湖南岳塘公安部门成功打掉一利用游戏外挂非法牟利团伙

8 月 13 日，湖南岳塘公安接报警称，辖区某“工作室”在网络游戏《三角洲行动》中借“陪玩”名义接单牟利。办案民警立即侦查，迅速掌握嫌疑人犯罪事实和行踪。

8 月 14 日，宝塔派出所、书院路派出所民警联合开展抓捕行动，现场查获该“游戏工作室”内运行外挂的电脑 9 台，控制“工作室”成员 10 余人。经查，以嫌疑人蒋某为首的犯罪团伙为牟取非法利益，于 2026 年年初成立“游戏工作室”。嫌疑人通过某二手交易平台引流接单并雇佣多名人员使用外挂软件非法获取《三角洲行动》游戏数据，实现“透视”“自瞄”“物资雷达”等作弊功能逃避系统安全检测，严重侵害游戏的公平性，破坏网络环境的公平健康。目前，蒋某等 7 人因涉嫌非法获取计算机信息系统数据罪已被公安机关依法采取刑事强制措施。案件正在进一步深挖侦办。（来源：公安部网安局）

12. 重庆公安网安部门开展停车移动应用网络和数据安全问题整治行动

8 月 19 日消息，重庆市公安机关网安部门近日开展停车移动应用专项整治行动。行动中，共梳理全市停车场（库）3000 余个，摸排掌握运营主体单位 400 余家，纳管停车场（库）App 和小程序 34 个，运用技术检测和现场检查相结合的方式，对停车场（库）App 和小程序开展全量监督检查，发现并督导整改网络和数据安全漏洞隐患 67 处。

整治期间，渝中、九龙坡、南岸、北碚等地网安部门针对工作发现的“套路扫码”，超范围、违规收集公民个人信息，未落实分级分类数据保护措施等违法行为，对 6 家停车管理系统运营单位依法给予行政处罚。（来源：重庆网警）

13. 陕西西安公安部门破获一起利用“GOIP”设备实施诈骗案件

8 月 25 日消息，陕西西安公安浐灞分局近日发现辛家庙派出所辖区有人涉嫌利用“GOIP”设备为电信网络诈骗犯罪提供“引流”帮助。辛家庙派出所便衣中队民辅警迅速出击，成功抓获犯罪嫌疑人马某某，现场查获 GOIP 设备 3 套。

GOIP 设备是一种虚拟拨号装置，诈骗分子可通过远程操控，将境外网络信号转换为本地号码拨打电话、发送短信，极大增强诈骗手段的隐蔽性和迷惑性。经查，犯罪嫌疑人马某某 8 月在社交网络平台

上收到网友消息称“可以带他兼职赚钱”，随后该网友为其寄来 3 套 GOIP 设备。在明知违法的情况下，马某某按照对方的指引，潜入辛家庙地区，伪装成电工，将 GOIP 设备藏匿布设在公共通讯设施内，为电信网络诈骗提供通讯中转、引流支持，并从中非法获利 830 元。

目前，马某某被处以行政拘留 13 日，并处罚金 1000 元的行政处罚。公安机关对其违法所得予以追缴。（来源：公安部网安局）

14. 山东烟台公安网安部门打掉一个为“求职类诈骗”引流的犯罪窝点

8 月 29 日消息，山东烟台公安网安部门近日侦破一个涉嫌非法利用信息网络发布虚假招聘信息，为“求职类诈骗”引流的犯罪窝点，依法刑事拘留 10 人。

经查，犯罪嫌疑人李某飞、吴某利用其为某人力资源中介公司负责人职务便利，指使员工通过智联招聘、BOSS 直聘、抖音、58 同城、小红书等互联网平台发布虚假岗位招聘信息，谎称可在国家电网、部队文职、三甲医院等单位安排工作，骗取社会经验较少、求职意愿强烈的应届高校毕业生信任，将受骗人员引至线下，交由诈骗团伙与其签订所谓的“就业合同”，分批次收取高额就业介绍费用进行诈骗。目前，已发现有 106 人被骗，涉案金额达一千余万元。涉案人李某飞、吴某等 10 人已被依法采取刑事强制措施。（来源：公安部网安局）

15. 上海闵行公安网安部门侦破一起非法提供侵入计算机信息系统程序案

8 月 30 日消息，上海闵行网警近日在工作中发现，有人以无人机维修调试等服务为幌子，提供无人机代破解服务。警方循线抓获犯罪嫌疑人薛某，查获用于作案的多台电脑、手机等设备，查明其以 500 元至 1500 元不等的价格提供有偿“代破解”服务，非法获利 2 万余元。目前，薛某因提供侵入计算机信息系统程序罪被闵行区人民法院判处有期徒刑 6 个月，缓刑 1 年，处罚金 2000 元，追缴违法所得。（来源：公安部网安局）

16. 陕西西安公安网安部门通报 5 起打击整治网络暴力典型案例

8 月 31 日，陕西西安公安网安部门通报 5 起打击整治网络暴力典型案例。

案例一：微信群内辱骂他人并泄露个人照片。近日，灞桥公安分局接群众报警，称其在微信群内遭人辱骂且个人照片被泄露。经查，违法行为人王某某因经济纠纷，在成员 400 余人的微信群中发布侮辱性言论，恶意诅咒当事人及其家人，并发布当事人照片，实施网络暴力，严重干扰当事人正常生活，造成不良社会影响。目前，灞桥公安分局已依法对王某某作出行政处罚。

案例二：“网络开盒”泄露他人住址信息。近日，违法行为人魏某某仅凭主观猜测，认定某网络商铺售卖伤害动物类药品，在未核实

事实的情况下，通过某短视频平台发布帖文，以“网络开盒”方式泄露商铺从业人员住址信息，实施网络暴力。该行为侵犯公民个人隐私，造成不良社会影响，扰乱网络公共秩序。目前，莲湖公安分局已依法对魏某某作出行政处罚。

案例三：多平台发布他人肖像配侮辱性言论。近日，灞桥公安分局接群众报警，称其个人肖像及相关信息被人发布至网络平台，并附带侮辱性言论。经查，违法行为人赵某某因经济纠纷心生不满，在微信朋友圈、某短视频平台发布当事人照片，配发侮辱性文字实施网络暴力，严重干扰当事人正常生活，扰乱网络空间秩序，造成不良社会影响。目前，灞桥公安分局已依法对赵某某作出行政处罚。

案例四：微信群内公开发布辱骂言论。近日，长安公安分局接群众报警，称其在微信群内遭人辱骂。经查，违法行为人赵某某因日常琐事心生不满，在微信群中公开发布辱骂性言论，实施网络暴力，严重干扰当事人正常生活，扰乱网络空间秩序。目前，长安公安分局已依法对赵某某作出行政处罚。

案例五：业主群内发布辱骂性言论。近日，灞桥公安分局接群众报警，称其在微信业主群内遭人辱骂。经查，违法行为人牛某某因楼上住户夜间噪音影响休息心生不满，在微信业主群中公开发布辱骂当事人的言论，实施网络暴力，干扰当事人正常生活，扰乱社区网络交流秩序。目前，灞桥公安分局已依法对牛某某作出行政处罚。（来源：陕西网警）

17. 湖南常德公安网安部门侦破一起破坏计算机信息系统案

8 月 31 日消息，湖南省常德市公安局武陵分局近日成功破获一起破坏计算机信息系统案，抓获犯罪嫌疑人朱某某。

2026 年 8 月，武陵分局网安大队接到线索，武陵区某电竞馆遭受 DDoS 攻击致网络瘫痪，严重影响正常经营。大队民警迅速赶赴现场，询问网吧负责人相关情况，走访排查周边网吧异常情况，并向电信运营商调取相关证据。结合网络侦查、大数据侦查，初步锁定嫌疑人朱某某。目前，犯罪嫌疑人朱某某已被公安机关依法予以刑事拘留，案件正在进一步侦办中。（来源：湖南网警）

（二）网信部门治理实践

1. 中央网信办发布“清朗·网络娱乐团播乱象整治”专项行动典型案例

8 月 3 日，中央网信办发布“清朗·网络娱乐团播乱象整治”专项行动情况。专项行动开展以来，中央网信办针对团播违规 PK 刺激打赏、不当玩法诱导打赏、场景内容低俗不良、侵害未成年人权益等问题，指导督促网站平台加强团播内容管理，依法依约处置违规网络团播账号 1840 余个。同期发布四起典型案例。

案例一：团播账号“神威空间”“红黄绿的绿”“洲羽”“Ct-摘星楼”“Lz-天上人间 001”“金麦姐妹花（招人）”“GJ-江诗月”等，团播成员穿着暴露，频繁展示抖胸、挺胯等带有性暗示的动作，

演绎低俗内容，或刻意采用昏暗灯光，通过朦胧光影烘托暧昧、软色情氛围，已予以禁言或限期封禁直播权限处置。

案例二：团播账号“生活磨平了蛋的妙脆角”存在未成年人参与团播问题，已予以关闭账号处置，其所在 MCN 机构由平台予以清退处置。团播账号“泽宇”“渝禧 200”等，通过模仿未成年人语气、穿校服直播等方式诱导打赏，已予以限期封禁直播权限处置。

案例三：团播账号“Dorx-0230”“VG 舞-08”“请叫我杨粒航 TEL”等，使用“解锁福利”等暗语，以口播话术刺激用户转账送礼，或引导粉丝开展线下接触等方式诱导打赏，已予以禁言或永久封禁直播权限处置。

案例四：团播账号“ZL-元气少女”“草莓甜心 101”“BRI 火墨”“RED-9”“沐阳”“贝拉 Lala”等，在 PK 过程中操控团播成员开展低俗恶俗、带有人身侮辱性质的惩罚，或密集进行“帮我组一组”“就差最后一点”等喊话，进行无实质内容 PK 诱导打赏，已予以限期封禁直播权限或限流处置。

24 日，中央网信办再次发布专项行动工作成果。针对娱乐团播场景内容低俗不良、规则设计刺激打赏、侵害未成年人权益等突出问题，中央网信办持续加大违法违规娱乐团播打击力度，累计处置团播违规直播间 7200 余个，严惩违规账号 2200 余个，指导网站平台清退处置一批问题严重的团播 MCN 机构，发布治理公告 17 期。

专项行动期间，中央网信办坚持整治与规范并重，着力细化完善团播审核机制，优化榜单排名和功能玩法，强化团播账号和团播机构

管理，指导督促网站平台积极履行主体责任，有针对性地加强娱乐团播规范管理。抖音推进团播账号主页 MCN 机构信息外显工作，组织开展团播机构培训，从源头规范娱乐团播行为。快手细化团播审核标准，加强技术能力建设，提升对团播低俗玩法和不良互动的识别准确率。微信视频号上线疑似未成年人团播身份核验功能，有效防范未成年人以隐蔽形式出镜参与团播。哔哩哔哩优化调整团播功能玩法，下线倍数积分、梯度加成、“冲榜”等刺激打赏的玩法机制。小红书采取限流等处置措施，严管密集喊话、无实质内容 PK 等团播不当行为。（来源：网信中国）

2. 国家网信办发布“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动典型案例

8 月 4 日，国家网信办发布“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动典型案例。

案例一：“电车小飞”等账号发布虚假信息，恶意抹黑诋毁企业。微博账号“电车小飞”、抖音账号“电车小飞”、小红书账号“玩转电车”，蓄意发布误导性信息，抹黑某汽车企业商品声誉和商业信誉，并借机营销引流牟利。涉及账号已被依法依约关闭。

案例二：“职场五斗米”等账号炒作涉企负面信息，干扰企业正常生产经营。微信公众账号“职场五斗米”、微博账号“股市财报风云”，长期在企业上市融资、财务报表公布等重要时间节点，歪曲解

读企业经营策略，渲染炒作企业营收情况，恶意唱衰企业发展前景。涉及账号已被依法依约关闭。

案例三：“G2观”系列账号发布虚假信息，牟取非法利益。账号“G2观”在今日头条、网易、微信等多个网站平台通过矩阵翻炒企业旧闻旧事，恶意攻击企业高管，账号运营主体以删帖、消除影响为名，向企业索要财物、寻求商务合作。涉及账号已被依法依约关闭。

案例四：“凡信优选”等账号开展虚假测评，诋毁企业产品质量。快手账号“凡信优选”“邻里好物仓”、抖音账号“家电大兵”、哔哩哔哩账号“才神道”、小红书账号“18923t大米姐”，发布虚假不实网络测评信息，贬损企业产品质量和商品声誉，误导消费者认知。涉及账号已被依法依约采取处置措施。（来源：网信中国）

3. 国家网信办启动对派拓公司在华销售产品网络安全审查

8月6日，网络安全审查办公室发布公告，为保障关键信息基础设施安全稳定运行，防范网络安全风险隐患，维护国家安全，依据《国家安全法》《网络安全法》，按照《网络安全审查办法》，对派拓公司（Palo Alto Networks）在华销售的产品实施网络安全审查。（来源：网信中国）

4. 国家网信办发布2026年8月个人信息保护政策法规问答

8月12日，国家互联网信息办公室发布2026年8月个人信息保护政策法规问答，共包括两个问题，分别是处理已公开的个人信息有哪些要求、导致个人信息泄露的常见原因有哪些。

关于处理已公开的个人信息有哪些要求，国家互联网信息办公室表示，《个人信息保护合规审计管理办法》附件《个人信息保护合规审计指引》第十二条对违法违规处理已公开个人信息情形作了细化：（一）向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；（二）利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；（三）处理个人明确拒绝处理的已公开个人信息；（四）对个人权益有重大影响，未取得个人同意；（五）收集、留存或处理已公开个人信息的规模、时间或使用目的超出合理范围。

关于导致个人信息泄露的常见原因有哪些，国家互联网信息办公室表示，一是个人信息明文存储和传输，未采取适当的加密、去标识化等安全技术措施；二是存储个人信息的信息系统、数据库等未采取有效安全措施，如使用弱口令、无登录验证措施；三是可通过互联网访问的数据接口未采取有效的身份验证措施；四是互联网网站页面上包含网站关联的信息系统、数据库的登录账号与口令等。（来源：网信中国）

5. 2026 年个人信息保护系列专项行动取得阶段性成效

8 月 19 日消息，中央网信办、工业和信息化部、公安部近日会同相关部门，开展的 2026 年个人信息保护系列专项行动取得阶段性成效。一是累计对 2 万余款 App、SDK 个人信息收集使用情况开展核查检测，督促 4000 余款完成合规整改，公开通报 1100 余款存在违法违规问题的 App、SDK，对 400 余款采取下架等处置处罚措施；二是针对个人信息处理规则未明确收集个人信息用于广告、用户画像，未提供个性化广告关闭选项等问题，对 1000 余家企业和机构的相关产品开展核查检测并督促整改；三是开展教育、交通、卫生健康、金融等领域个人信息风险排查，累计摸排 9 万余家企业和机构，发现并督促整改各类隐患问题 1.2 万余个；四是加大个人信息违法犯罪打击力度，加强线索监测发现，严打涉信息泄露、信息倒卖等违法犯罪行为，严惩行业“内鬼”。

下一步，中央网信办、工业和信息化部、公安部将深入推进个人信息保护系列专项行动，加强典型违法违规问题治理，加快推进国家网络身份认证公共服务推广应用，深化个人信息保护宣传教育，不断夯实个人信息保护工作基础，有效维护公民合法权益。（来源：网信中国）

6. 上海市网信办集中约谈重点平台，要求切实履行未成年人网络保护责任

8 月 13 日消息，上海市网信办近日推进“清朗守护·为你而来”2026 年未成年人网络环境整治专项行动，组织对属地网络音视频、网络文学、网络游戏、网络社交、电商以及 AI 平台等一批重点平台开展巡查抽检，依法集中约谈问题较为突出的 6 家平台。上海市网信办依据《可能影响未成年人身心健康的网络信息分类办法》，巡查发现三类突出问题：

一是平台显著位置推送低俗内容。属地一音视频平台首页推荐环节出现大量低俗擦边直播间、视频内容，在午夜时间问题尤其严重；一网络文学平台在“书架”版块推荐玄幻修仙类低俗小说，严重影响未成年人正确认知。

二是平台重要环节呈现违法和不良内容。属地一音视频平台算法机制存在漏洞，用户搜索健身常用词汇或普通菜名时，搜索结果呈现低俗擦边内容；两家网络游戏社区审核不严格，用户使用“丧文化”或过激言论作为昵称，传播漠视生命、自我贬损，以及“读书无用论”“唯分数论”等错误观念。

三是平台未成年人模式落实不到位。属地一电商平台未成年人模式下搜索“成人”等关键词，关联词条呈现软色情内容；一 AI 平台未采取有效措施识别未成年人用户身份，输出不当交友内容，满足通宵聊天、无底线聊天需求。（来源：上海市网信办）

7. 上海市网信办开展涉汽车行业网上信息传播秩序问题专项整治

8 月 11 日消息，上海市网信办近日开展涉汽车行业网上信息传播秩序问题专项整治。专项行动开展以来，上海市网信办聚焦网络谣言、违规网络测评、标题党等扰乱汽车市场秩序的虚假和误导性宣传，指导属地重点平台，健全审核发布规则，及时阻断违规内容传播扩散，并对持续违规账号实施阶梯式处置，累计清理违法和不良信息 9.1 万余条，处置违规“自媒体”账号 9000 余个。专项行动发现三类突出问题：

一是“标题党”，夸大标题博取关注，反向营销扰乱秩序。部分账号使用夸张标题，发布标题与内容严重不符的不良信息，恶意唱衰引流，误导社会公众，扰乱公平竞争秩序，违反《网络信息内容生态治理规定》第七条等法律法规。如账号“Shang***”发布《**难怪你卖不好》以贬损企业品牌为噱头博取关注，经核实视频内容实为反向营销行为。此类以“唱衰”之名行“引流”之实的做法，不仅误导消费者对企业品牌的客观认知，更以“黑红也是红”的畸形流量逻辑扰乱公平竞争秩序。账号“说车****”发布多个视频，标题配以“某某车大崩盘”“某某车跌爆炸”等消极表述“吸睛”，渲染市场焦虑情绪，表面“唱衰”实为“带货”，极易误导消费者对市场真实情况的判断，干扰正常价格信息传播秩序。平台已对相关内容作删除处理，市网信办依法约谈账号运营者，并督促整改。

二是“涉企谣言”，AI 伪造抹黑企业，歪曲政策引流变现。部分账号编造、传播虚假信息扰乱经济秩序和社会秩序，造谣引流、歪曲事实，违反《网络安全法》第十三条，《网络信息内容生态治理规定》第六条，《互联网用户公众账号信息服务管理规定》第十八条等法律法规。如账号“轻客***”发布视频称某品牌车辆存在“自燃”问题，通过 AI 伪造车辆现场自燃图片，恶意编造虚假信息，误导社会公众，严重损害企业声誉。经公安部门核查，该账号运营者刘某因虚构事实扰乱公共秩序，已对其依法予以行政处罚。账号“阿振****”等歪曲解读营销政策，编造涉汽车企业置换补贴、金融贷款等不实信息，集中发布抹黑产品性能的同质化内容，以唱衰贬损性信息博取流量，引流推介汽车周边商品。平台已对相关内容作删除处理，对相关账号依法依约予以禁言处置。

三是“违规网络测评”，无资质乱测评，变相拉踩贬损竞品。部分账号开展网络测评活动未坚持客观公正、全面准确原则，未委托有资质机构按标准测试，干扰企业生产经营秩序，违反《网络信息内容生态治理规定》第六条，违反《网络测评活动规范》第二条、第三条、第四条、第六条。如账号“刘浪**”在不具备网络测评活动相关资质的情况下，转发涉及某品牌电池及闪充技术测试的内容。未经核验的测试数据经传播后极易对公众形成误导，干扰消费者对产品性能的正确判断，扰乱了公平竞争的市场秩序。账号“懂车***”发布《全段位夯拉榜》，在多款竞品车型间进行主观优劣排序，缺乏客观实测数据支撑，通过分级定档方式刻意贬低竞品、抬高特定车型，误导消费者

购车决策，平台已对相关内容作删除处理，对相关账号依法依约予以禁言处置。（来源：上海市网信办）

8. 河北省网信办通报 7 月份“清朗·燕赵净网”网络生态治理专项行动成果

8 月 11 日，河北省网信办通报 7 月份“清朗·燕赵净网”网络生态治理专项行动成果。2026 年 7 月，河北省网信系统查处违法违规网站 146 家，查处违规互联网用户账号 50 个，处置各类违法和不良信息 41593 条。

经核查，对未依法履行网络安全保护义务，导致数据被窃取的某网络科技有限公司，依法予以警告，并处罚款 1 万元；对网站存在游戏赌博有害信息的某科技有限公司，依法予以警告；对发布非法移动应用程序下载链接的网站“IT 笔记”，依法予以关闭；对存在色情低俗内容的“寻梦漂流瓶”APP，依法约谈责任主体并责令整改；对发布虚假谣言信息，造成不良影响的“大鱼”“执笔落红尘”等账号，依法责令整改；将“咋你了”等账号涉及的违法线索移送公安机关核查处置。（来源：河北省网信办）

9. 上海市委网信办开展网络娱乐团播乱象治理工作，清退、警告违规 MCN 机构 79 家

8 月 24 日消息，上海市委网信办近日指导属地重点平台加强网络娱乐团播领域治理工作，通过“梳理管理清单—制定合规制度—公

示公约公告”等举措，压实相关 MCN 机构管理责任，规范团播账号运营。专项行动开展以来，已采取关停、限时封禁等方式处置违规直播间 1452 个、违规团播账号 410 个，清退、警告违规 MCN 机构 79 家。

属地网络社交、音视频等重点平台围绕娱乐团播账号注册、规则设计、场景设置、成员行为规范、未成年人网络保护、MCN 机构运营等问题，深入开展综合治理。小红书提高团播审核标准和管理尺度，健全团播账号分级管理体系，对违规团播账号及相关主播采取联动信用降级，严厉打击各类不当团播玩法规则。哔哩哔哩加强团播合规治理，持续向 MCN 机构开展专项治理宣导，对团播直播内容、PK 玩法、互动行为等重点场景实施常态化抽检，不断提升治理成效。同时，网站平台制定团播合规管理制度，发布专项治理公告，引导用户开展才艺展示类优质团播内容，共筑清朗直播生态。（来源：上海市网信办）

10. 广东网信部门公开通报“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动典型案例

8 月 27 日消息，广东网信部门公开通报“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动典型案例。

案例一：“**见闻”等账号对企业进行“舆情敲诈”。“**见闻”“**俱乐部”“**印记”等账号发布涉企负面信息，以删帖、消除影响为名向企业索要高额费用，要挟企业与其进行“商业合作”，遭到

企业拒绝后持续发布企业负面信息。相关平台已依法依约对上述账号采取关闭处置措施，违法犯罪线索已移交公安机关处理。

案例二：“俞**”等账号造谣诽谤企业家。“俞**”“**287”“网友**”等账号为博眼球，采用“标题党”“震惊体”等方式发布大量不实信息，编造企业家“被抓了”“要进去了”等谣言，侵犯其合法权益。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。

案例三：“**商业”等账号唱衰企业发展前景。“**商业”“**顺利”“**会诊”等账号长期集纳炒作涉企负面信息，发布“破产”“裁员”等虚假不实内容，干扰企业正常生产经营秩序。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。

案例四：“**信息”等账号歪曲解读涉企公开信息。“**信息”“**局”“**会”等账号打着“行业动态研究”等幌子，长期歪曲解读财务报表、企业年报等涉企公开信息，散布不实信息误导舆论。相关平台已依法依约对上述账号采取禁言等处置措施。

案例五：“**论道”等账号泛化炒作企业产品质量。“**论道”“**盟”等账号为博眼球、吸流量，频繁蹭炒热点事件，以“标题党”“小作文”等形式诋毁企业产品质量，误导公众认知，煽动消费群体对立。相关平台已依法依约对上述账号采取禁言等处置措施。

案例六：“**酒”等账号滥用AI技术抹黑企业形象。“**酒”“**派”“*苍蝇*门”等账号利用AI工具批量生成含有某企业名称、商标等元素的图片，以明显侮辱性词汇对企业标识进行涂抹恶搞，侵

犯企业合法权益。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。

案例七：“**门”等账号炒作企业不实信息。“**门”“**杂谈”“**记”等账号频繁翻炒企业旧闻旧事，借热点事件关联炒作企业经营问题，发布大量同质化涉企不实信息，并借机引流谋利。相关平台已依法依约对上述账号采取禁言等处置措施。

案例八：“**会员”等账号散布误导性涉企信息。“**会员”“**豪宅”“**说”等账号为博取流量，以“亲身记录”“代体验”等为噱头，持续散布误导性信息，侵害企业商业信誉，煽动网民抵制企业。相关平台已依法依约对上述账号采取禁言等处置措施。

案例九：“**汽车”等账号抹黑诋毁企业品牌。“**汽车”“**赛车”“**说车”等账号在企业新品发布等重要时间节点，通过滥用谐音字造梗、贴负面标签等方式，歪曲解读产品名称、外观，捏造产品抄袭等谣言。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：广东省网信办）

11. 广东省网信办通报第三批属地 App 个人信息收集使用问题

8 月 7 日消息，广东省互联网信息办公室近日对属地 App（含小程序）进行检测，发现 20 款 App（含小程序）存在收集使用个人信息问题。

例如药康夫处方平台 APP 存在三项问题：一是在登录页面时，未勾选隐私政策即可收集手机验证码；二是 App 首次运行未经用户阅读同意隐私政策，收集 OAID、AAID 和 VAID 信息；三是在收集用户身份证号个人敏感信息时，未同步告知用户其目的。

兔灵医药小程序存在两项问题：一是首次进入小程序时，未提示用户阅读并同意隐私政策，且小程序收集手机号信息未提供隐私政策文本、未明示收集用户手机号信息的目的、方式、范围；二是未向用户提供撤回同意收集个人信息的途径、方式。（来源：广东省网信办）

12. 因违反《个人信息保护法》，重庆九龙坡网信办依法对属地一企业作出行政处罚

8 月 10 日消息，重庆九龙坡区网信办近日在监督检查中发现，辖区某科技公司运营的 APP 存在“以用户不同意处理其个人信息为由，拒绝提供相关产品或者服务”等违法行为，侵害用户合法权益。九龙坡区网信办依据《个人信息保护法》相关规定，依法对该企业作出责令改正、给予警告的行政处罚，并要求企业完善个人信息保护合规机制，加强员工互联网法律法规学习，强化技术防护措施，及时排查消除风险隐患，切实履行网络平台主体责任。（来源：重庆市网信办）

13. 因不履行个人信息保护义务，湖南省网信办对某酒店管理有限公司作出行政处罚

8 月 25 日消息，湖南省互联网信息办公室近日依法查明，某酒店管理有限公司微信小程序存在未经用户同意收集使用个人信息、超出必要范围处理个人信息、未公布投诉举报方式等违法行为，会员姓名、手机号码等个人信息在传输、存储过程中未采取加密、去标识化等安全技术措施，未按法律规定留存相关网络日志，相关管理制度不健全。湖南省互联网信息办公室依据《个人信息保护法》对该公司作出警告的行政处罚。（来源：湖南省网信办）

14. 安徽省网信办通报网络生态乱象治理典型案例

8 月 6 日，安徽省互联网信息办公室通报 100 起网络生态乱象治理典型案例，涉及发布涉恶意挑动负面情绪类有害信息共 9 例、发布恶意炒作涉企类有害信息共 11 例、发布涉 AI 应用乱象类有害信息共 16 例、发布涉教育领域类有害信息共 13 例、发布涉公共安全领域类有害信息共 20 例、发布涉法涉诉类有害信息共 14 例、发布涉演绎低俗软色情类有害信息共 12 例、假冒仿冒官方网站账号发布有害信息共 5 例。

截至 2026 年 7 月底，安徽省依法注销或关闭违法违规网站 131 家，约谈网站平台及账号责任人 101 人次，处置违法违规账号 334 个，受理处置公众举报投诉 10449 件。（来源：安徽省网信办）

（三）通信管理部门治理实践

1. 工信部通信管理局以及多地通信管理部门发布侵害用户权益 APP（SDK）名单

（1）工信部

8 月 25 日，工业和信息化部信息通信管理局通报 2026 年第 5 批（总第 58 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 26 款 APP 及 SDK 存在侵害用户权益行为。上述 APP 及 SDK 应当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。（来源：工信部通信管理局）

（2）北京市

8 月 4 日，北京市通信管理局通报 2026 年第八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 4 款移动互联网应用程序未整改或整改不到位。

此外，6 月 30 日，北京市通信管理局曾通报北京市部分存在侵害用户权益行为的移动互联网应用程序并要求整改。截至通报，仍有 5 款移动互联网应用程序未整改或整改不到位，予以全网下架处置。（来源：北京市通信管理局）

（3）江苏省

8 月 5 日，江苏省通信管理局通报 2026 年第 5 批侵害用户权益行为的 APP。江苏省通信管理局组织对省内医疗健康等类型的 APP、小程序进行检测，并通报相关单位限期整改。截至通报，尚有 3 款 APP 未完成整改。相关单位于 8 月 14 日前完成整改并反馈，整改落实不到位的，江苏省通信管理局将依法依规组织对主办者开展相关处置工作。

8 月 28 日，江苏省通信管理局通报 2026 年第 6 批侵害用户权益行为的 APP。江苏省通信管理局组织对省内实用工具等类型的 APP 进行检测，并通报相关单位限期整改。截至通报，尚有 6 款 APP 未完成整改。相关单位于 9 月 11 日前完成整改并反馈，整改落实不到位的，江苏省通信管理局将依法依规组织对主办者开展相关处置工作。（来源：江苏省通信管理局）

（4）上海市

8 月 20 日，上海市通信管理局通报下架 9 款侵害用户权益行为的 APP（SDK）。2026 年 7 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 9 款 APP（SDK）未按照要求落实整改，上海市通信管理局对上述 APP（SDK）采取下架处理，并对上述 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。

8 月 26 日，上海市通信管理局通报 2026 年第六批侵害用户权益行为的 APP（SDK）。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，发现 16 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：上海市通信管理局）

（5）安徽省

8 月 11 日，安徽省通信管理局通报 2026 年第 5 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 21 款 APP 存在违法违规收集使用个人信息问题，2026 年 6 月 23 日对上述违规 APP 开发者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 6 款 APP 未完成问题整改，相关 APP 开发者应在 2026 年 8 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。（来源：安徽省通信管理局）

（6）浙江省

8 月 27 日，浙江省通信管理局通报 2026 年第 7 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相关领域 APP、小程序进行抽查，书面要求违规 APP、小程序开发运营主体限期整改。经核查复检，尚有 15 款 APP、小程序未按要求完成整改。相关运营主体于 9 月 7 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处置工作。

2026 年 7 月，浙江省通信管理局向社会公开通报了第六批存在侵害用户权益行为的 APP（小程序），要求相关运营主体限期整改。经再次核查复检，上述 8 款 APP、小程序已完成通报问题整改。（来源：浙江省通信管理局）

（四）其他部门治理实践

1. 国家数据局发布《中国数据产业发展报告（2026）》

8 月 28 日，国家数据发展研究院在 2026 中国国际大数据产业博览会主论坛上发布《中国数据产业发展报告（2026）》。《报告》显示，2025 年，我国数据产业规模达到 6.78 万亿元，同比增长 15.7%，数据企业数量 48.2 万家。

《报告》展望四个未来发展趋势：一是词元服务将加快发展，进一步催生新的商业模式和产业形态；二是人工智能对数据的需求将持续增长，为数据产业拓展新的发展空间；三是 AI 原生数据技术和产业创新将加速突破，合成数据将成为重要数据来源；四是数据产业规模仍将保持较快增长水平。（来源：国家数据局）

2. 最高人民检察院发布一起利用抓包软件篡改退款数据案，主犯因诈骗罪被判刑

8 月 30 日，最高人民检察院发布一起利用抓包软件篡改退款数据案。本案中，2026 年 7 月，贵州省贵阳市观山湖区检察院提起公诉

的蔡某涉嫌诈骗罪一案宣判，主犯蔡某因犯诈骗罪被判处有期徒刑三年，缓刑四年，并处罚金 2 万元。

本案被害企业某茶叶管理公司开发运营一款为商户和消费者提供网络交易服务的 App。消费者购物前在 App 内充值，充值金额直达第三方资金监管平台。消费者确认收货后，系统自动将费用转入平台商户账户，平台按售卖金额比例收取服务费。2025 年 9 月，该公司客服接到消费者咨询电话，称其订单状态显示为退款但本人并未申请。技术人员核查发现，该订单用户编码与退款单用户编码不符，经进一步排查确认方某、蔡某、詹某三人存在异常退款行为。数据显示，2025 年 9 月共 127 单订单的用户编码被篡改，退款账户被篡改为上述三人银行账户，其中蔡某退款 19.9 万余元并提现 16.7 万余元，方某、詹某分别退款 5 万元和 2 万余元，资金尚未提现。公司当日冻结三人账户余额，次日向公安机关报警。

经查，蔡某此前发现部分购物 App 存在技术漏洞，意图借此牟利。2025 年 9 月，蔡某下载该茶叶管理公司 App 并进行漏洞测试：下单购买茶叶后申请退款，在退款过程中使用抓包软件拦截向服务器发送的退款请求数据包，篡改其中真实订单 ID 后重新发送虚假数据包至服务器。服务器接收虚假数据包后误认为是合法退款指令，遂执行退款程序，将对应交易款项转入蔡某账户。测试成功后，蔡某将该漏洞告知朋友詹某、方某，约定由蔡某提供技术指导和漏洞信息，詹某、方某负责操作，蔡某从二人收益中收取约半数作为报酬，蔡某自

身操作所得由其自行处置。但漏洞很快被公司发现，蔡某虽成功提现16.7万余元，但尚未从詹某、方某处获益时二人账户已被冻结。

2025年10月公安机关立案侦查，11月将三人抓获归案。鉴于蔡某系犯意发起者，在共同犯罪中起组织、主导作用，认定为主犯，诈骗金额近20万元，数额巨大，检察院以涉嫌诈骗罪对蔡某提起公诉。詹某、方某仅听从蔡某安排，使用其提供的工具和方法实施操作，未参与策划、未掌握核心技术，认定为从犯，涉案资金已被全额冻结且自愿认罪认罚，综合考量犯罪情节、危害后果及悔罪表现，检察院对二人作出不起诉决定。

6月，观山湖区检察院以蔡某涉嫌诈骗罪向法院提起公诉。法院审理期间，蔡某家属再次退赔被害企业损失，企业出具书面谅解书。检察院与蔡某重新签署认罪认罚具结书，建议法院适用缓刑。7月，法院采纳检察机关量刑建议作出上述判决。（来源：最高人民检察院）

境内前沿观察三：人工智能安全专题

导读：8 月，境内人工智能安全治理主要聚焦于两个方面：一是促进人工智能发展，发布相关规划、意见，推动人工智能数据标注、算力建设、模型开发等工作；二是推动人工智能相关治理工作，涉及 AI 应用乱象治理等。

促进人工智能发展方面，重庆市人民政府印发《重庆市“十五五”人工智能发展规划（2026—2030 年）》，提出强化人工智能自主创新能力、夯实人工智能基础底座等措施。上海、山东发布软件和信息服务业发展规划，将推动人工智能发展作为重点措施。四川省五部门印发《四川省推进算力网建设的若干政策措施（试行）》，提出优化全省算力区域布局、建设高能级算力中心等措施。安徽省工业和信息化厅发布《安徽省具身智能产业发展行动方案（2026—2028 年）》，提出构建协同发展格局、提升产业创新能力等十六项任务。江西省等三部门印发《关于加快发展数据标注产业建设高质量数据集的若干措施》，提出强化数据资源供给、强化创新驱动发展等十八项措施。内蒙古自治区等六部门印发《内蒙古自治区促进词元经济高质量发展的若干措施》，提出强化词元供给能力、加强词元科技创新、建设 OPC 生态社区等十八项措施。

人工智能治理方面，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——个人用户使用人工智能服务安全指南》，从安全意识提升、安全使用指引、使用行为准则三个维度为个人用户

使用人工智能服务提供系统性安全指引。北京市审结首例破坏人工智能模型刑事案件，某科技公司算法工程师王某因破坏计算机信息系统罪被判处有期徒刑五年十个月。网信、气象、公安、应急等多部门协同联动，依法打击造谣传谣行为，整治 AI 应用乱象。上海市委网信办部署推进“清朗·整治 AI 应用乱象”专项行动第二阶段工作，聚焦 AI 技术生成“数字泔水”、违规提供 AI 产品服务和应用程序等 7 类突出问题，统筹推进排查清理、合规指导、普法宣传等各项工作。

关键词：具身智能；算力建设；词元经济；AI 治理

1. 全国网安标委秘书处发布《网络安全标准实践指南——个人用户使用人工智能服务安全指南》

8 月 24 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——个人用户使用人工智能服务安全指南》，从安全意识提升、安全使用指引、使用行为准则三个维度为个人用户使用人工智能服务提供系统性安全指引。指南适用于个人用户通过互联网使用人工智能服务，尤其是利用人工智能技术提供预测、建议、决策，或生成文本、图片、音频、视频等内容的服务场景。

在安全意识提升方面，指南提出个人用户需要建立四项安全理念：一是正确认知人工智能能力的局限性，认识到其可能提供错误信息、出现理解偏差或无法完成特定任务；二是理性对待人工智能生成结果，增强对虚假、错误、误导性内容的识别能力，避免盲目接受和信任；三是适度使用人工智能，将其作为辅助真实生活的工具，避免沉迷依赖，正确认知情感服务原理，不宜过度替代现实交往；四是关注安全风险动态，增强对人工智能安全风险及伦理安全影响的认识，审慎提供隐私信息，警惕人工智能服务被恶意利用生成仿冒亲友声音、伪造官方通知等。

在安全使用指引方面，指南提出九条具体措施：一是从正规渠道获取人工智能服务，优先选用最新版本，涉及生成式人工智能服务的应选择已通过备案的大模型，不通过来源不明的中转站或未授权代理使用；二是部署使用智能体时应参照相关实践指南采用适宜的部署方

式和安全措施；三是使用前应查看用户协议和隐私协议，了解服务局限性、个人信息收集使用方式、数据是否用作训练数据以及投诉举报机制，核实是否符合最小化收集原则；四是关注服务申请的访问权限，关闭非必要的麦克风、摄像头、相册等授权；五是妥善保护敏感信息，审慎提供隐私信息或敏感个人信息，防范意外泄露或被窃取；六是审慎对待服务输出结果，必要时通过多个人工智能服务或其他渠道交叉验证，对法律、医疗、就业、教育、理财等领域输出结果仅作参考，涉及财产和人身安全时应通过独立渠道核实；七是关注开发者提供的安全更新和补丁并及时安装；八是个人权益受损时向主管部门或有关机构咨询、求助或举报；九是未成年人和老年人用户的监护人应协助其安全使用人工智能服务。（来源：全国网络安全标准化技术委员会秘书处）

2. 重庆市人民政府印发《重庆市“十五五”人工智能发展规划（2026—2030 年）》

7 月 31 日，重庆市人民政府印发《重庆市“十五五”人工智能发展规划（2026—2030 年）》，围绕强化人工智能自主创新能力、夯实人工智能基础底座、构建人工智能应用场景体系等五个方面，提出二十四项措施。

深化全市域要素市场化配置综合改革方面，《发展规划》提出，深化数据要素市场化配置改革。深化落实数据持有权、使用权、经营权“三权分置”产权制度，全面贯彻落实国家数据产权登记制度，鼓

励权利人开展数据产权登记，将登记凭证作为开展或参与数据要素流通交易、融资担保等活动的可信凭证。规范公共数据资源授权运营，鼓励公共数据与企业数据融合开发利用。健全交易中心产品上架挂牌、交付结算、交易存证等规则体系，推广标准化交易合同，开展数据交易价格监测。健全公共数据资源授权运营价格形成机制，探索公共数据授权运营收益分配机制。

确保人工智能安全可控方面，《发展规划》提出，完善人工智能法治规范体系。加快完善人工智能法律法规配套制度，健全责任认定机制，探索人工智能生成内容的知识产权界定和利益分配机制。健全人工智能智能体、模型标准体系，鼓励企业、科研机构主导或参与制定国际、国家标准，支持企业按照相关标准研发产品服务。研究制定重点领域行业标准、应用规范和安全指南，推动重庆标准成果向行业示范应用转化。强化人工智能伦理审查，建立和完善人工智能科技伦理标准体系。强化用户隐私保护，建立用户信息全生命周期安全保护制度。开展现行法律法规、政策指导、应用规范、伦理准则等实施效果评估，有序推进规则条款的修订和废止。（来源：重庆市政府）

3. 天津市工业和信息化局、市发展改革委、市科技局印发《天津市智能机器人产业创新发展行动方案（2026—2028 年）》

8 月 4 日，天津市工业和信息化局、市发展改革委、市科技局印发《天津市智能机器人产业创新发展行动方案（2026—2028 年）》，

提出核心技术攻关行动、产品谱系培优行动、强企兴链聚群行动等六项行动。

核心技术攻关行动方面，《方案》提出，加强高质量数据集供给。围绕汽车、高端装备、新一代信息技术等领域，布局建设智能机器人数据采集、加工、训练综合体，为企业提供数据采集、标注加工、模型训练、检验验证一站式解决方案。鼓励企业、高校、科研机构及相关领域行业组织，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，扩大高质量数据集供给，形成支撑智能机器人训练的高质量数据集不少于100个，组织开展行业高质量数据集建设场景供需对接。（来源：天津市工业和信息化局）

4. 上海市经济和信息化委员会印发《上海市软件和信息服务业发展“十五五”规划》

8月4日，上海市经济和信息化委员会印发《上海市软件和信息服务业发展“十五五”规划》，围绕发挥人工智能引领作用、布局面向未来的新兴赛道、优化完善产业支撑体系三个方面，提出十八项措施。

发挥人工智能引领作用方面，《规划》提出，加快网络安全产业数智化迭代。加快安全产业智能化升级，推动安全防御、检测、响应、治理全链路与人工智能深度融合，扩大智能化、实战化的网络安全软件、软硬件一体化产品供给，升级常态化安全防控能力。培育模型驱动的安全新业态，构建面向智能场景的攻防能力，适配人工智能新业

务新应用，发展智算云安全、AI 防火墙、安全靶场、智能体身份管理等特色解决方案。壮大安全产业专业化服务，支持第三方机构积极拓展模型安全检测、内容合规评测、AI 安全规划咨询等服务能力，挖掘安全服务增长点，完善配套服务体系。

布局面向未来的新兴赛道方面，《规划》提出，布局原生安全。探索“模型定义安全”新一代技术架构，攻关底层安全推理、全链路攻击溯源、对抗性防御等关键技术，推动以模型替代传统特征匹配、静态规则、固化权限策略的防护模式，加速网络安全推理能力实现行业适配与工程化落地。培育 AI 密码与量子安全，支持神经网络、深度学习等技术集成到密码系统，加快密码大模型的研发与应用，突破高级加密算法、安全密钥生成、密码协议设计等核心技术，构筑面向未来的密码安全底座。（来源：上海市经济和信息化委员会）

5. 山东省工业和信息化厅发布《山东省软件和信息技术服务业高质量发展行动计划（2026—2030 年）（征求意见稿）》

8 月 7 日，山东省工业和信息化厅发布《山东省软件和信息技术服务业高质量发展行动计划（2026—2030 年）（征求意见稿）》，围绕夯实关键技术创新底座、加快人工智能赋能赋智、推动应用场景融合化转型等七个方面，提出二十三项措施。

加快人工智能赋能赋智方面，征求意见稿提出，聚焦人工智能基础理论、核心算法、关键模型等开展创新攻关，加速模型算法和工程化技术创新，做强一批具备自主知识产权的代码大模型、需求分析和

设计大模型等。聚焦超长上下文理解、复杂逻辑推理和跨库代码生成等核心能力，研发多模态代码大模型。构建全栈式大模型工具链，突破分布式训练、高效参数微调、强化学习对齐等关键技术，夯实软件开发智能化底座。鼓励龙头企业联合高校院所开展类脑智能、具身智能等前沿技术研究，抢占未来竞争制高点。（来源：山东省工业和信息化厅）

6. 四川省发展和改革委员会等部门印发《四川省推进算力网建设的若干政策措施（试行）》

8 月 11 日，四川省发展和改革委员会、四川省经济和信息化厅、四川省科学技术厅等五部门印发《四川省推进算力网建设的若干政策措施（试行）》，围绕优化全省算力区域布局、打造集约高效算力产业园区、建设高能级算力中心等六个方面，提出十九项措施。

强化算力赋能“人工智能+”方面，《措施》提出，建设高质量数据集。加快推进成都国家级和宜宾、内江、自贡、遂宁省级数据标注基地建设。推动公共数据、行业数据依法合规向人工智能企业开放。鼓励行业龙头企业开放场景数据资源，形成算力供给、数据支持、场景落地等协同赋能“人工智能+”的良性生态。

推动算力普惠易用方面，《措施》提出，推行词元（Token）普惠化。支持算力园区建设词元（Token）工厂，支持基础电信运营商、云计算企业在川建设模型即服务（MaaS）平台，提供词元（Token）普惠应用技术底座。支持人工智能原生企业和人工智能一人公司

（OPC）主体，聚焦数字文创、装备制造、能源化工、金融科技、软件信息服务等领域，打造一批词元（Token）普惠应用示范标杆。以词元(Token)普惠应用助推产业园区智改数转,打造一批“词元(Token)应用示范园区”。（来源：四川省发改委）

7. 江西省发展改革委（江西省数据局）等三部门印发《关于加快发展数据标注产业建设高质量数据集的若干措施》

8 月 11 日，江西省发展改革委（江西省数据局）、江西省财政厅、江西省人力资源和社会保障厅印发《关于加快发展数据标注产业建设高质量数据集的若干措施》，围绕强化数据资源供给、推进产业集聚发展、强化创新驱动发展等六个方面，提出十八项措施。

强化数据资源供给方面，《若干措施》提出，加强公共数据资源供给。强化公共数据资源登记，编制公共数据资源目录，建立目录动态更新、需求反馈机制，加快构建全省公共数据“一本账”。强化部门供数意识，集约化建设公共数据资源授权运营平台，推动公共数据合规高效流通，尽快打通公共数据资源授权运营全链条。

打造高质量数据集方面，《若干措施》提出，体系化布局高质量数据集。围绕工业制造、医疗卫生、交通运输、金融服务、教育教学、文化旅游、城市治理等重点领域以及具身智能、脑机接口、生物制造等创新领域，征集并系统梳理论证、发布牵引力强的标杆场景，组织行业龙头企业、科研院所等主体，以场景需求和模型应用为导向，编制行业高质量数据集建设图谱。遵循“需求牵引、急用先行、应用验

证、安全保障”的原则，按照“以价值定场景、以场景定模型、以模型定数据”的思路，聚焦图谱，充分发挥链主企业、行业牵头单位、先行先试单位的引领作用，推进建设一批高质量数据集。（来源：江西省发改委）

8. 内蒙古六部门印发《内蒙古自治区促进词元经济高质量发展的若干措施》

8 月 12 日，内蒙古自治区政务服务与数据管理局、内蒙古自治区发展和改革委员会、内蒙古自治区财政厅等六部门印发《内蒙古自治区促进词元经济高质量发展的若干措施》，围绕强化词元供给能力、加强词元科技创新、建设 OPC 生态社区等八个方面提出十八项措施。

加强高质量数据集建设方面，《若干措施》提出强化高质量数据集供给。加大公共数据资源开发利用力度，支持产业链上下游共建数据集，扩大高质量数据集供给规模。鼓励企业积极承接国家先行先试任务，坚持“以模引数、用数赋模”，推动大模型、智能体研发与高质量数据集建设一体布局、同步推进。支持发展人机协同智能化标注和专家型标注服务。

优化词元经济发展环境方面，《若干措施》提出强化词元经济安全治理。提升重点领域词元服务应用安全保障能力，推动词元工厂落实网络安全等级保护要求，督促模型企业依法依规完成生成式人工智能服务备案，建立跨境词元服务安全评估和风险防控机制。（来源：内蒙古政务服务和数据管理局）

9. 安徽省工业和信息化厅发布《安徽省具身智能产业发展行动方案（2026—2028 年）》

8 月 20 日，安徽省工业和信息化厅发布《安徽省具身智能产业发展行动方案（2026—2028 年）》，围绕构建协同发展格局、提升产业创新能力、壮大企业群体等五个方面，提出十六项主要任务。

深化场景应用推广方面，《行动方案》提出，强力推进三类场景落地。为新技术找验证场景，联动企业、高校、院所梳理具身智能前沿新技术，建立待验证技术清单，分类梳理全省验证场景资源，形成场景资源数据库，按需匹配验证点位。为成熟产品找应用场景，面向省内定期征集机器人创新产品，编制产品能力清单，深挖各领域批量应用需求，推动供需匹配落地。为刚需场景找适配产品，聚焦重点领域应用需求，依托平台推动产品精准适配落地；针对难点卡点场景，通过揭榜攻坚模式攻克技术和产品短板。

优化产业发展生态方面，《行动方案》提出，健全标准与治理体系。围绕优势领域标准化需求，鼓励企业参与国家、行业、团体标准制修订，推动技术融入先进标准。依托国家级计量检测平台，建立具身智能产品智能化、可靠性、安全性指标体系与检测方法。加强知识产权服务，为企业提供快速检索、确权、维权全链条服务。推动具身智能伦理与安全治理研究，督导企业落实伦理规范与安全要求。（来源：安徽省工业和信息化厅）

10. 多部门协同联动重拳整治造谣传谣行为，重点网站平台累计处置账号 2.1 万余个

8 月 4 日，国家互联网信息办公室发布 2026 年 7 月至今网络谣言治理情况。网信、气象、公安、应急等多部门协同联动，及时发布权威辟谣信息，依法打击造谣传谣行为。

中央网信办深入推进“清朗·整治 AI 应用乱象”专项行动，违法和不良信息举报中心开设“涉 AI 应用乱象举报专区”，重点受理利用 AI 技术制作发布虚假信息等行为。近两个月来各重点网站平台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。公安部网安局分两批公布近 50 起全国各地涉汛涉灾典型案例，各地公安机关对造谣传谣者刑事拘留 4 人，行政处罚近 50 人，强力震慑了编造传播涉汛涉灾谣言的不法分子，维护防灾救灾良好舆论氛围。

具体来说，7 月，网络谣言主要聚焦于自然灾害、民生政策等领域，造谣者利用 AI 技术炮制虚假信息、拼接旧闻夸大灾情、冒用官方名义杜撰政策，严重误导公众认知，干扰防灾救灾与社会生产秩序。（来源：网信中国）

11. 上海市委网信办部署推进“清朗·整治 AI 应用乱象”专项行动第二阶段工作，下架违规智能体 1065 个

8 月 17 日消息，上海市委网信办近日部署推进“清朗·整治 AI 应用乱象”专项行动第二阶段工作，聚焦 AI 技术生成“数字泔水”、制作发布虚假信息、散播暴力低俗内容、仿冒他人、侵害未成年人权

益、从事网络水军活动、违规提供 AI 产品服务和应用程序 7 类突出问题，统筹推进排查清理、合规指导、普法宣传等各项工作。

第二阶段专项行动期间，上海属地网站平台共清理违法和不良信息 219.3 万余条，处置违规账号 1.8 万余个，下架违规智能体 1065 个。在专项行动期间，上海市委网信办指导小红书、哔哩哔哩、喜马拉雅、Soul 等属地音视频、网络社交平台创新推出 8 期“AI 知识普及包”，以图文、短视频等形式深入剖析 AI 造假手法、黑灰产乱象，普及 AI 内容识别要点，将复杂的专业技术转化为通俗易懂的防范指南。（来源：上海市网信办）

12. 因删库致公司 AI 研发瘫痪，一算法工程师被判破坏计算机信息系统罪

8 月 4 日消息，北京市首例破坏人工智能模型刑事案件近日最终审结，王某因破坏计算机信息系统罪被判处有期徒刑五年十个月，并赔偿所在公司经济损失 20.4 万余元。本案中，某科技公司算法工程师王某，为利用公司算力资源“干私活”腾出存储空间，输入“删库”代码运行逾 17 小时，删除公司 AI 游戏部门 89TB 核心训练数据，导致多个研发项目停摆。

2024 年 1 月，王某应聘进入北京某科技公司 AI 短剧部门担任算法工程师。该部门此前将开发数据存储于自行搭建的 A 服务器集群，因内部架构调整，2024 年 7 月至 8 月，部门先后三次在工作群组通知全体人员将本人负责的公司开发数据及个人数据从 A 集群迁移至

新搭建的B集群，并告知迁移后不再有A集群使用权限。2024年9月，王某使用此前掌握的账号密码登录A集群，查找AI短剧部门文件夹未果后，打开AI游戏部门文件夹试图拉取文件目录，因系统未及时响应便中止操作，随后输入一条“删库跑路”代码，其含义是以最高管理员权限强制删除当前目录下所有文件和子目录，无须逐项确认。输入代码后王某即下班离开，待公司运维人员发现异常并最终定位王某的电脑、中止删除进程时，代码已运行超过17个小时。被删除的AI游戏部门文件夹存储了该部门全部开发文件，包括公司自主研发的多个文生3D和渲染人工智能模型及训练数据，删除行为导致公司模型训练系统功能瘫痪，AI游戏部门相关研发项目全部停摆。2024年9月，公司与王某解除劳动关系，AI游戏部门停止开发活动全力投入数据恢复，经过近20天努力，绝大部分被删除数据得以修复。事件造成公司人工工资支出16万余元，恢复数据消耗的算力资源超过4万元。

2024年10月，该公司向公安机关报案，11月王某被抓获。王某到案后一直辩称系“误删数据”，声称认为A集群已被弃用，不知其中还有其他部门数据。检察机关从王某手机的聊天记录中发现，王某与案外人高某约定利用公司数据和算力资源为高某“训模型”“跑数据”，案发当日上午二人仍在沟通修改模型细节。检察机关认定王某并非误删数据，而是长期与外部人员合谋秘密窃取公司算力资源运行与工作无关项目，其对利用公司资源干私活将被开除具有明确认知，删除数据是为下载个人干私活模型腾出空间，误删辩解不能成立。

2025 年 6 月，东城区检察院以王某涉嫌破坏计算机信息系统罪提起公诉。2026 年 3 月，法院采纳检察机关全部指控意见作出一审判决，判处王某有期徒刑五年十个月，赔偿刑事附带民事诉讼原告人经济损失 20.4 万余元。王某不服提起上诉，6 月二审法院裁定驳回上诉、维持原判。（来源：最高人民检察院）

境外前沿观察：月度速览十则

导读：8 月，境外各国围绕智能体人工智能安全治理、数据和个人信息保护、未成年人网络治理等领域发布相关指南和政策法律。

人工智能安全治理方面，欧盟《人工智能法》关于人工智能系统透明度的相关条款正式生效，要求人工智能系统提供者和部署者承担人工智能生成内容标识、人机交互告知两项透明度义务。澳大利亚两机构联合发布《董事会前沿人工智能网络威胁考量》指南，面向董事会成员和高级管理人员说明前沿人工智能模型发展对组织网络安全威胁的影响，提出加强治理、网络安全准备和韧性的具体建议。澳大利亚工业、科学与资源部发布《多智能体系统的风险与控制——跨组织边界部署 AI 代理的分析框架》，提出多智能体系统的安全治理的层级差异化策略。

个人信息保护方面，韩国国会全体会议通过《个人信息保护法》修正案，为 AI 技术开发过程中的个人信息使用设立新的法律特例。因 Uber 在 2018 年至 2022 年期间使用完全自动化的决策系统对司机账户进行临时或永久性封禁，且在整个决策过程中未引入任何人工审核，荷兰数据保护局对 Uber 处以 8.2499 亿欧元罚款。巴西国家数据保护局对 TikTok 运营方字节跳动处以 1.537 亿雷亚尔罚款，并责令其删除违规收集的数据并实施合规整改计划。

未成年人网络保护方面，法国总统签署《保护未成年人免受社交网络使用风险法》，要求开展针对学生、教职工和家长的屏幕有害影

响及社交网络成瘾性宣传教育。美国 Meta 公司与 47 个州及哥伦比亚特区等属地达成和解协议，同意支付最高 170 亿美元，并在其 Facebook 和 Instagram 平台上实施一系列青少年安全保护强制性措施。

关键词：人工智能安全；个人信息保护；未成年人网络保护

1. 欧盟《人工智能法》透明度规则正式生效，要求履行人工智能生成内容标识及人机交互场景告知义务

8 月 2 日，欧盟《人工智能法》关于人工智能系统透明度的相关条款正式生效。

根据生效条款规定，人工智能系统提供者和部署者须承担两项透明度义务：一是对人工智能生成内容的标记与标识义务。人工智能生成内容必须以清晰可见的方式加注标识，并附带机器可读的标记；二是人机交互情形下的告知义务。明确告知用户交互对象是聊天机器人、人工智能智能体或虚拟形象等人工智能系统。

为协助提供者和部署者履行上述义务，欧盟委员会已陆续发布《人工智能生成内容透明度指南》《人工智能生成内容行为准则》，以及关于《人工智能法》第五十条透明度义务的常见问题解答和人工智能系统透明度规则要点说明。（来源：欧盟委员会）

2. 越南颁布网络安全与个人数据保护统一行政处罚法令

8 月 19 日，越南政府颁布第 330/2026/ND-CP 号法令，针对 2025 年《网络安全法》《个人数据保护法》建立统一的行政处罚框架。

法令适用于在越南境内实施网络安全和个人数据保护行政违法行为的各类主体，包括在越南设立的公司，在越南提供电信、互联网、内容、信息技术、网络安全或跨境数字服务的外国企业分支机构及代表处，以及直接参与或涉及越南公民个人数据处理的相关实体。

法令对罚款上限作出分层次规定。网络安全违法行为方面，组织最高罚款 2 亿越南盾（约合 8000 美元），个人最高罚款 1 亿越南盾（约合 4000 美元）。个人数据保护一般违法行为方面，组织最高罚款 30 亿越南盾（约合 12 万美元），个人最高罚款 15 亿越南盾（约合 6 万美元）。非法买卖个人数据最高可处违法所得 10 倍的罚款。跨境传输个人数据未准备影响评估档案的，最高可处上一年度收入的 5%（组织）或 2.5%（个人）。

除罚款外，法令还设定了警告、暂停或吊销许可证、没收违法工具和物证及对违法外国人的驱逐出境的行政处罚类型。主管机关还可以下令没收用于违法行为的服务器、硬件或软件系统。（来源：越南政府）

3. 韩国国会通过《个人信息保护法》修正案，为合法数据用于 AI 训练开辟新路径

8 月 20 日，韩国国会全体会议通过《个人信息保护法》修正案。修正案核心内容之一是为 AI 技术开发过程中的个人信息使用设立新的法律特例，以突破此前制度下数据利用困境。

此前韩国《个人信息保护法》规定，依法通过信息主体同意或合同等途径收集的个人信息若要用于其他目的，须另行取得信息主体同意或具备其他法律依据，或只能以假名信息、匿名信息形式加以利用，AI 开发因此受到制约。此前允许突破的主要路径是监管沙盒，且仅限于 AI 防范语音诈骗、自动驾驶机器人等部分创新服务可使用含个

人信息的影像或语音数据，而沙盒制度仅在规定期限内提供临时的例外认可。同时，个人信息利用直接关系国民权利，仅凭产业振兴类个别法律中的规制特例难以提供充分保障，需要在统管个人信息保护的专业监督体系基础上另设法律依据。

据此，修正案在既有个人信息处理依据之外新设特例：仅在假名信息或匿名信息不足以完成 AI 开发，且具有公益性、社会必要性的情形下，以强化安全措施并经韩国个人信息保护委员会（PIPC）的审议并作出决议为前提，方可将合法收集的个人信息用于 AI 技术开发。修正案同时设置配套安全保障，包括处理敏感信息或唯一识别信息等对信息主体权利和利益影响较大的情形，须事先评估风险因素并制定改进方案等。（来源：韩国国会）

4. 法国颁布《保护未成年人免受社交网络使用风险法》，规定多项未成年人网络保护措施

8 月 24 日，法国总统签署第 2026-813 号《保护未成年人免受社交网络使用风险法》，8 月 25 日在官方公报公布，8 月 26 日起正式生效。

该法案最初的核心条款规定，自 2026 年 9 月 1 日起禁止 15 岁以下未成年人访问社交网络平台，已经注册的未成年人账户自 2027 年 1 月 1 日起适用禁令。法国议会已于 2026 年 7 月 21 日通过该条款。然而，法国宪法委员会在 8 月 14 日的裁决中认定该禁令构成“对言论自由和私生活的过度侵害”，遂将其从法律中删除。

最终颁布的法律保留了多项未成年人网络保护措施。在教育领域，该法将中小学数字技术使用纳入学校项目，要求开展针对学生、教职工和家长的屏幕有害影响及社交网络成瘾性宣传教育。该法还将此前已在小学和初中实施的手机使用禁令延伸至高中，高中校规须在遵循学校项目的前提下确定禁令的实施方式和例外情形。（来源：法国政府）

5. 澳大利亚两机构联合发布《董事会前沿人工智能网络威胁考量》指南

8 月 5 日，澳大利亚信号局澳大利亚网络安全中心（ASD's ACSC）与澳大利亚公司董事协会（AICD）联合发布指南《董事会前沿人工智能网络威胁考量》，面向董事会成员和高级管理人员说明前沿人工智能模型发展对组织网络安全威胁的影响，并提出加强治理、网络安全准备和韧性的具体建议。

指南提出，董事会应评估组织面对人工智能赋能攻击的脆弱程度，重新审视现有网络安全风险评估所依据的前提和风险容忍度；识别系统和网络供应链中可能被人工智能快速组合利用的薄弱环节；确认组织是否掌握第三方及第四方供应商的安全与韧性状况；审查既有网络安全基础措施在攻击频率更高、针对性更强和自动化程度更高的情况下是否仍然有效；同时确认在严重网络安全事件发生时，组织能否持续提供关键业务，并及时检测和响应由前沿人工智能加速的攻击。

指南建议，组织建立并持续执行安全配置基线，删除不必要的服务和不安全配置；持续开展漏洞扫描和评估，及时修复或缓解软件及配置弱点；定期审查用户和系统访问权限，按照最小权限原则配置账户；定期审查并演练网络安全事件响应、业务连续性和灾难恢复计划。组织也可以采用适当的人工智能模型辅助软件开发、漏洞识别和修复、安全评估、漏洞扫描以及安全监测和事件分类，但相关应用仍应置于适当的治理和监督机制之下。

指南提出，董事会应持续要求管理层就上述措施的实施情况进行报告并提供保证，以确保组织能够在前沿人工智能不断改变网络威胁环境的情况下，具备预防、检测、响应和恢复网络安全事件的能力。（来源：澳大利亚信号局）

6. 澳大利亚工业、科学与资源部发布《多智能体系统的风险与控制——跨组织边界部署 AI 代理的分析框架》报告

8 月 10 日，澳大利亚工业、科学与资源部（DISR）发布《多智能体系统的风险与控制——跨组织边界部署 AI 代理的分析框架》。报告指出，多智能体系统的安全治理需依据部署层级采取差异化策略，系统级风险无法通过单代理评估识别，最终安全有赖于部署机构、政策制定者与标准研究界的多方协同。

报告将代理交互环境划分为单一治理、联邦治理和开放环境三个层级。报告强调，在多智能体系统中，归因、授权、监督和评估四类治理工作尤为突出。代理间的交互链条冗长，责任追溯复杂；权限在

层层委托中难以有效管控；代理行动速度远超人类审核能力，沟通过程又不易理解，实质性监督难以落地；而单代理测试无法覆盖系统整体涌现的风险。随着共同治理基础的弱化，这些困难将进一步加剧。核心基础设施、全局性熔断机制和群体规模监控等能力，在系统发展早期建设成本较低，一旦代理群体大规模运行后再行改造，则代价高昂甚至难以实现。标准制定、法规完善和评估方法论研究等工作超出单个组织的能力范围，需要行业、法学研究机构和监管机构协同推进。（来源：澳大利亚工业、科学与资源部）

7. 美国第九巡回上诉法院撤销针对 Perplexity AI 初步禁令

8 月 4 日，美国第九巡回上诉法院就亚马逊旗下 Amazon.com Services, LLC 诉人工智能公司 Perplexity AI, Inc.案作出裁决，撤销联邦地区法院此前发布的初步禁令，裁定亚马逊依据《计算机欺诈与滥用法》（CFAA）及加州《综合计算机数据访问与欺诈法》（CDAFA）提出的主张难以在实体审理中胜诉。

本案争议源于 Perplexity 于 2025 年推出的 AI 赋能的 Comet 浏览器及其内置的可选 AI 助手“Assistant”。该助手在用户指令下可执行浏览 Amazon.com 等网站并搜索商品的任务。当用户指示助手在亚马逊平台查找商品时，助手截取浏览器视图的屏幕截图，从用户计算机发送至 Perplexity 服务器，并接收来自 Perplexity 服务器的导航指令。在此过程中，Perplexity 服务器未直接与亚马逊服务器交互。亚马逊在 Comet 发布前后均告知 Perplexity 其 AI 产品不得访问亚马逊平台，

争议核心在于 Perplexity 未使用“用户代理字符串”机制向亚马逊表明用户已激活 AI 代理。2025 年 11 月，亚马逊提起诉讼并同时申请初步禁令，指控 Perplexity 违反 CFAA 及 CDAFA。2026 年 3 月，联邦地区法院作出初步禁令裁决，认定亚马逊在诉讼中具有胜诉可能性且将遭受不可弥补的损害。Perplexity 随即提起上诉。

第九巡回上诉法院在分析中指出，CFAA 惩罚的是“任何人”“故意访问”受保护计算机的行为。最高法院已在 Van Buren 案中阐明，“访问”指进入计算机系统本身或其中特定部分的行为。上诉法院认为，无论 Assistant 当前如何先进，其在法律上仍属于工具而非“人”。关键在于判断 Perplexity 是否通过该工具“访问”亚马逊服务器。基于本案事实，法院认定是用户借助 Assistant 在 Amazon.com 上执行特定行为，而非 Perplexity 本身。关于加州 CDAFA 主张，法院认为尽管该法对“访问”的定义可能比 CFAA 更宽泛，但调查的核心仍在于“人”是否访问或导致访问。据此，第九巡回上诉法院裁定撤销地区法院的初步禁令，并将案件发回重审。（来源：美国第九巡回上述法院）

8. 因自动化封禁司机账户，荷兰数据保护局对 Uber 罚款 8.2499 亿欧元

8 月 21 日消息，因 Uber 在 2018 年至 2022 年期间使用完全自动化的决策系统对司机账户进行临时或永久性封禁，且在整个决策过程中未引入任何人工审核，违反 GDPR 关于自动化决策的禁止性规定，荷兰数据保护局近日宣布对 Uber 处以 8.2499 亿欧元罚款。

本案源于法国人权联盟代表 171 名法国 Uber 司机向法国数据保护机构提出的集体投诉。由于 Uber 的欧洲总部设在荷兰阿姆斯特丹，根据 GDPR 的“一站式”机制，荷兰数据保护局成为该案的主管调查机构。荷兰数据保护局经调查认定，Uber 使用软件监控司机驾驶行为与客户评分，一旦检测到涉嫌欺诈或客户评分过低，相关账户即被自动停用。封禁决策完全缺乏人工介入，而账户被停用意味着司机无法通过 Uber 平台接单并获得收入。Uber 对本次罚款表示异议，相关诉讼程序仍在进行中。（来源：荷兰数据保护局）

9. 因违法处理儿童青少年数据，巴西国家数据保护局对 TikTok 处以 1.537 亿雷亚尔罚款

8 月 25 日，巴西国家数据保护局（ANPD）在联邦公报公布制裁决定，对 TikTok 运营方字节跳动（ByteDance Brasil Tecnologia Ltda.）处以 1.537 亿雷亚尔罚款，并责令其删除违规收集的数据并实施合规整改计划。此次处罚源于 ANPD 监管监察过程中发现的 TikTok 在儿童和青少年个人数据处理方面的多项违规行为。

ANPD 监察总署通过第 50/2024 号技术报告认定，TikTok 在“无账号信息流”和“注册账号信息流”两种访问模式下，均存在处理儿童和青少年个人数据而缺乏有效法律依据的违规行为。具体违规事项共计五项：在无账号信息流模式下，允许儿童和青少年访问信息流并处理其个人数据而缺乏有效法律依据，且未采取措施预防此类数据处理；在注册账号信息流模式下，为儿童和青少年办理注册而处理其个

人数据而缺乏有效法律依据，且未采取有效措施预防该群体注册；在两种访问模式下，均未能证明已采取有效且可验证的措施以确保数据保护规范的遵守与执行。（来源：巴西国家数据保护局）

10. Meta 就未成年人成瘾诉讼达成 170 亿美元和解协议

8 月 26 日，美国 Meta 公司与 47 个州及哥伦比亚特区、波多黎各、美属萨摩亚、北马里亚纳群岛、关岛和美属维尔京群岛等属地达成一项法律和解协议，同意向提起诉讼的各州支付最高 170 亿美元，并在其 Facebook 和 Instagram 平台上实施一系列青少年安全保护强制性措施。

2023 年，以加利福尼亚州、科罗拉多州、肯塔基州和新泽西州为首的 29 个州在加州北区联邦地区法院对 Meta 提起诉讼，随后扩展至 47 个州及多个属地。各州指控 Meta 在 Facebook 和 Instagram 平台中设计使青少年成瘾的功能。各州还依据《儿童在线隐私保护法》（COPPA）提出诉讼，指控 Meta 明知平台存在 13 岁以下用户，未经可验证的家长同意收集和使用其个人信息。各州还指控 Meta 在 2016 年大选前与剑桥分析公司等第三方共享 Facebook 用户的非公开信息。

根据和解协议，Meta 将在 10 年内支付至少 121 亿美元，若 TikTok 和 YouTube 等其他社交媒体公司未来达成类似和解，总金额可升至 171 亿美元。德克萨斯州未加入多州和解，而是单独与 Meta 达成约 10 亿美元的独立和解协议。除财务赔偿外，Meta 同意实施一系列安

全措施，包括为 13 至 17 岁青少年账户在 Instagram 和 Facebook 两个平台合计设定每日 2 小时使用上限，连续使用 15 分钟后强制暂停，60 分钟和 90 分钟时再次暂停；午夜至早上 6 时默认封锁访问；上学日 8 时至 15 时消除推送通知；采取更严格的年龄验证措施，包括身份或面部识别技术；提供更完善的家长监督工具等。（来源：综合媒体信息）

行业前沿观察：各地协会动态

各单位围绕生态协同、人才培育、技能竞赛、公益科普等积极作为。院士大讲堂、高级研修班、网络安全大赛、低空经济研修、数据跨境研讨等活动多点开花，行业协同活力持续释放。以下按活动举办日期先后排序。佛山市信息协会2026年度生态协同对接会圆满举行：打破内卷，共建良性产业新生态；中关村可信计算产业联盟成功举办2026院士大讲堂----“院士中国行”第一站（内蒙古）；抗量子密码安全芯片在汉发布 安创会华中网络安全生态峰会顺利举办 武汉市网络安全协会提供支持；以案为鉴筑牢安全防线 守护医疗数据“生命线” 茂名市计算机信息网络安全协会承办省运会医疗专项安全培训；肇庆市计算机学会主办的专利产品备案培训暨专利密集型产品宣传活动在广东邦科电子股份有限公司圆满举行；北京网络空间安全协会国家级高研班办出“生态圈”：人社部“大模型驱动的具身智能应用与安全高级研修班”在京成功举办；天津市网络空间安全协会举办互联网应用程序个人信息保护合规公益培训；惠州市计算机信息网络安全协会承办的第七期惠州网信沙龙在惠阳具身智能产业园举行；南通市信息网络安全协会举办人工智能平台合规与用户信息安全研讨会；海南省计算机学会主办的“AI智能体教育应用与教学创新实战工坊”圆满收官；澳门国际科技产业发展协会主办的“澳门网络数据与AI安全峰会暨网络攻防精英培训计划开幕式”圆满举行；广东省网络空间安全协会承办的低空经济网络安全保障与风险管理高级研修班在广州成功举办；苏州市

互联网协会承办的苏州市网络安全进园区大模型专场活动顺利举办；珠海市网络空间安全协会主办的“数据跨境流动政策推进座谈会”顺利举行；广州网络空间安全协会商用密码公益大讲堂（第四期）圆满举办；宁波市计算机信息网络安全协会主办的2026年宁波市第九届网络安全大赛圆满收官；西藏自治区互联网协会“情暖雪域e起行”关爱西藏儿童察隅县公益行活动圆满举办；湖北省网络和数据安全协会扎实推进国家网络与信息安全职业技能人才等级认定工作。

关键词：生态协同、人才培育、技能竞赛、公益科普、低空经济、数据跨境

1. 佛山市信息协会 2026 年度生态协同对接会圆满举行：打破内卷，共建良性产业新生态

8 月 5 日，佛山市信息协会 2026 年度生态协同对接会在鹰创园隆重举行。本次大会以“聚力共生·生态共荣”为主题，汇聚了近 50 家会员单位代表及生态伙伴参加。面对“再造一个新佛山”的产业攻坚关口，会议旨在通过政策解读、生态倡议及深度资源对接，引导行业携手构建良性和可持续的产业生态。

2. 中关村可信计算产业联盟成功举办 2026 院士大讲堂----“院士中国行”第一站（内蒙古）

中关村可信计算产业联盟（以下简称：可信联盟）诚邀内蒙古工业大学联合主办的“院士中国行”第一站（内蒙古）--2026 可信计算院士大讲堂，2026 年 8 月 7 日在呼和浩特内蒙古工业大学成功举行，内蒙古工业大学副校长张杰、教育部教育信息管理中心原副主任、研究员曾德华、中关村可信计算产业联盟监事长马帅致辞，中国工程院沈昌祥院士莅临，以《构建安全可信智能网络新生态，促进数字经济高质量发展》为题做主旨报告，教育部及首都高校相关领导、国家部委信息中心领导、相关领域专家、内蒙古属地网信、公安、教育、保密局相关领导和可信联盟会员单位代表，近百人在现场参会，直播平台线上在线参会人数约 2600 人。

3. 抗量子密码安全芯片在汉发布 安创会华中网络安全生态峰会顺利举办 武汉市网络安全协会提供支持

2026 年 8 月 14 日，由中关村科技企业家协会指导、北京中关村科技企业家协会网络安全创新企业分会（以下简称，安创会）主办的“安创会 2026 年华中网络安全生态峰会”在武汉举行。活动以＂数安聚力 •鄂启新程＂为主题，汇聚该组织北京、重庆、陕西等地 20 余家专精特新网安企业及武汉本地百余家相关企业，聚焦网络安全生态共建与资源对接。中国船舶集团有限公司第七二二研究所、武汉市网络安全协会、国家网络安全人才与创新基地产业联盟为活动提供支持。

4. 以案为鉴筑牢安全防线 守护医疗数据“生命线” 茂名市计算机信息网络安全协会承办省运会医疗专项安全培训

网络安全没有旁观者，人人都是守护者。8 月 13 日上午，“以案为鉴 守护生命线 护航省运会”——2026 年广东省运会网络安全保障医疗专项安全培训活动在中国联通茂名市分公司举行。

本次培训由茂名市卫生健康局主办，茂名市公安局网络安全保卫支队指导，茂名市计算机信息网络安全协会及医疗分委会承办，中国联合网络通信有限公司茂名市分公司、天津云安科技发展有限公司、北京数字认证股份有限公司、广东深界科技有限公司协办。中国联通茂名市分公司党委委员、副总经理蔡丽霞，茂名市卫生健康局规信科科长谭勇强，茂名市网络安全保卫支队二大队教导员谭艺，茂名市计算机信息网络安全协会医疗专委会主任委员陈鹤鸣等出席活动。全市

各级医疗卫生机构，包括医院、疾控中心、卫监所、血站等相关负责同志，以及医疗行业网络安全技术专家80余人参加培训。

5. 肇庆市计算机学会主办的专利产品备案培训暨专利密集型产品宣传活动在广东邦科电子股份有限公司圆满举行

8月14日，由肇庆市市场监督管理局（知识产权局）、高要区市场监督管理局（知识产权局）、高要区工业信息化局联合指导，肇庆市计算机学会主办，广东邦科电子股份有限公司与肇庆市信息协会协办的专利产品备案培训暨专利密集型产品宣传活动在理事单位广东邦科电子股份有限公司圆满举办。高要区市场监督局、高要区工信局有关领导及股室负责人出席会议。活动吸引了天龙油墨、晟辉科技、羚光新材、恒兴水产、力合技术、广东嘉拓、斯塔文化、永达辉、华峰电子、动力金属、博士芯等优秀企业参与。

6. 北京网络空间安全协会国家级高研班办出“生态圈”：人社部“大模型驱动的具身智能应用与安全高级研修班”在京成功举办

按照《人力资源和社会保障部办公厅关于印发专业技术人才知识更新工程2026年高级研修项目计划的通知》（人社厅函〔2026〕35号）部署，由人力资源和社会保障部主办、北京市人力资源和社会保障局协办，北京网络空间安全协会承办，北京市机器人产业协会、北京关键信息基础设施安全保护中心联合承办的“大模型驱动的具身智

能应用与安全高级研修班”，2026 年 8 月 17 日至 21 日在北京成功举办。来自全国政、产、学、研、金、服、用 7 大领域的 97 名学员齐聚北京·中国锦，完成 5 天研修，圆满完成各项研修任务。

7. 天津市网络空间安全协会举办互联网应用程序个人信息保护合规公益培训

为深入推进 2026 年个人信息保护系列专项行动，加强个人信息保护政策法规宣贯，推动我市互联网应用程序规范有序发展，8 月 18 日，互联网应用程序个人信息保护合规公益培训成功举办。我市 80 余家互联网应用程序运营者参会。

本次培训由天津市互联网信息办公室指导，天津市网络空间安全协会、国家互联网应急中心天津分中心、天津市网络数据安全和技术保障中心主办，恒安嘉新（天津）网络科技有限公司、北京梆梆安全科技有限公司承办，天津公交易通科技有限公司、天津市启阳优信科技有限公司协办。

8. 惠州市计算机信息网络安全协会承办的第七期惠州网信沙龙在惠阳具身智能产业园举行

8 月 19 日下午，以“惠聚美好 E 路同行”为主题的第七期惠州网信沙龙在惠阳具身智能产业园举行，惠阳区、大亚湾区有跨境经贸业务需求的机构和企业代表近 70 人参加活动。本次活动由惠州市委

网信办主办，惠州市计算机信息网络安全协会、惠州联通承办，惠阳区、大亚湾区网信部门协办。

9. 南通市信息网络安全协会举办人工智能平台合规与用户信息安全研讨会

为深入学习贯彻习近平在2026世界人工智能大会暨人工智能全球治理高级别会议开幕式上的讲话精神，落实人工智能安全治理工作要求，筑牢网络信息安全防线，搭建行业交流对接平台，南通市信息网络安全协会于8月20日下午在崇川区东部智谷举办人工智能平台合规与用户信息安全研讨会。

10. 海南省计算机学会主办的“AI智能体教育应用与教学创新实战工坊”圆满收官

2026年7月至8月，由海南省计算机学会主办、纳瓠蓝图（海南）科技有限公司承办的“2026年AI智能体教育应用与教学创新实战工坊”在海口连续举办四期，于8月20—21日第四期结课后全面收官。系列培训紧扣“人工智能+教育”落地难题，以“实战为主、学以致用”为核心原则，帮助一线教师打通从“不敢用、不会用”到“用得顺、用得巧”的转化路径，为海南自贸港智慧教育建设夯实人才根基。

11. 澳门国际科技产业发展协会主办的“澳门网络数据与 AI 安全峰会暨网络攻防精英培训计划开幕式”圆满举行

由澳门国际科技产业发展协会主办、澳门基金会资助的“澳门网络数据与 AI 安全峰会暨网络攻防精英培训计划开幕式”（以下简称峰会）于 8 月 21 日上午 10 时 30 分在澳门科学馆会议厅圆满举行。峰会汇聚政府代表与业界专家，共同探讨如何通过合规遵循、技术突破与产业协同，携手构建安全、可信、可持续的数字未来。

12. 广东省网络空间安全协会承办的低空经济网络安全保障与风险管理高级研修班在广州成功举办

8 月 25 日至 29 日，按照《人力资源社会保障部办公厅关于印发专业技术人才知识更新工程 2026 年高级研修项目计划的通知》部署，国家专业技术人才知识更新工程“低空经济网络安全保障与风险管理”高级研修班（2026 年第一期）在广州成功举办。

本期研修班旨在深入贯彻落实国家关于发展低空经济的战略部署，提升低空经济领域网络安全保障能力与风险管理水平，由人力资源和社会保障部主办，广东省人力资源和社会保障厅组织实施，广东省网络空间安全协会承办，广州网络空间安全协会联合承办。来自全国各地的 70 名专业技术人才齐聚羊城，顺利完成各项研修安排。作为承办单位，广东省网络空间安全协会全程组织教学、研讨与对接服务，搭平台、促交流、谋共建，让 70 名学员同窗研修、同题共答。

13. 苏州市互联网协会承办的苏州市网络安全进园区大模型专场活动顺利举办

为提升网络和数据安全治理水平，防范人工智能风险，强化监测预警，筑牢网络安全底线。8 月 25 日，苏州市网络安全进园区大模型专场活动在中国移动江苏公司苏州分公司成功举办。

本次活动由市委网信办、工业园区网信办主办；市互联网协会、工业园区人工智能产业协会承办；中国移动江苏公司苏州分公司、苏州国际科技园协办。活动以“AI 绘新程 安全筑未来”为主题，聚焦大模型安全治理，搭建政企交流对接平台，全市大模型企业、AI 企业及网络安全企业代表齐聚现场共商人工智能安全发展路径。

14. 珠海市网络空间安全协会主办的“数据跨境流动政策推进座谈会”顺利举行

8 月 26 日上午，由珠海市网络空间安全协会主办的“数据跨境流动政策推进座谈会”在金湾区市民服务中心 C1 栋 6 楼 601 会议室顺利举行。本次活动旨在搭建政企沟通桥梁，帮助企业精准把握数据跨境传输的最新政策导向，深入探讨合规落地的具体路径，切实解决企业在国际化经营中面临的实际问题。

15. 广州网络空间安全协会商用密码公益大讲堂（第四期）圆满举办

8 月 27 日下午，由广州市密码管理局指导，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，广东新兴国家网络安全和信息化发展研究院承办，广州华南检验检测中心有限公司、领信数科信息技术有限公司协办的商用密码公益大讲堂（第四期）在广州广电平云广场成功举办。

本期大讲堂以“深化商密应用 赋能数字安全”为主题，首次将课堂搬进产业一线，采取“实地观摩＋专题分享”相结合的方式举行。广州市密码管理局商用密码处处长邱辉祥、副处长刘昌劲、一级主任科员刘欣怡，广州网络空间安全协会会长黄丽玲、秘书长蔡舒婷，广州市商用密码产业联盟副秘书长、领信数科信息技术有限公司副总经理戴远程，来自广州市党政机关、企事业单位及科研院所的信息化负责人、安全管理员、技术骨干，以及网安协会员单位、联盟成员单位代表等 100 余人参加活动。

16. 宁波市计算机信息网络安全协会主办的 2026 年宁波市第九届网络安全大赛圆满收官

8 月 29 日，宁波市第九届网络安全大赛决赛圆满收官。本次大赛历经前期预赛选拔、成绩复核及社会公示，最终 42 支精英队伍晋级线下决赛，各路网安能手同台竞技、巅峰对决，圆满完成全部赛事比拼。

大赛由宁波市公安局、宁波市数据局、浙江省网络空间安全协会指导，宁波数字产业集团有限公司、宁波市计算机信息网络安全协会主办，中国联通网络通信有限公司宁波市分公司、宁波市宁数安全科技有限公司承办。共有近20个省的代表队报名参赛，参赛队伍达到203支。参赛队伍涵盖党政机关、金融、通信、国企等行业从业者，以及省内外多所高校优秀学子，兼具专业性与广泛性，全方位展现了国内网络安全人才的过硬素养。

17. 西藏自治区互联网协会“情暖雪域e起行”关爱西藏儿童察隅县公益行活动圆满举办

近日，由西藏自治区互联网协会、西藏自治区通信行业协会联合中国网络社会组织联合会、中国牙病防治基金会、丁香园共同发起的“情暖雪域e起行”——关爱西藏儿童察隅县公益行活动顺利结束。活动深入贯彻习近平总书记关于网络强国和未成年人保护的重要指示精神，落实《中华人民共和国未成年人保护法》《未成年人网络保护条例》要求，以法治温情与公益力量，为高原孩子送去实实在在的关怀。

18. 湖北省网络和数据安全协会扎实推进国家网络与信息安全职业技能人才等级认定工作

数字经济时代，网络和信息安全人才，是支撑国家网络安全事业行稳致远的核心动力。作为湖北省人力资源和社会保障厅核准备案的

省级社会培训评价组织，湖北省网络和数据安全协会已连续6年成功开展网络与信息安全管理员职业技能等级认定工作，该职业涵盖网络安全管理员、信息安全管理员等工种，主要承担网络及信息安全的管理、防护、监控等核心职责，协会坚持每月常态化组织考核评价，6年累计参考人数近万名，为湖北数字产业培育输送大批实战型网安技能人才，积极践行社会组织服务产业、服务技能人才的社会责任。