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10月第10期（总第39期）



2026年10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 10 月第 10 期（总第 39 期）

2026 年 10 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

顾　问：严　明　公安部第一、第三研究所 原所长、研究员

中国计算机学会计算机安全专业委员会 主任

指导专家：袁旭阳 北京网络行业协会 原会长

公安部网络安全保卫局 原副局长

总 编 辑：黄道丽 公安部第三研究所网络安全法律研究中心 主任

副总编辑：鲍　亮 公安部第三研究所网络安全技术研发中心 副主任

编委会主任：黄丽玲 北京网络空间安全协会 理事长

编委会副主任：（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

黄丽佳 北京网络空间安全协会 会长助理

于永丰 辽宁省信息网络安全协会 秘书长

林勇忠 广东省网络空间安全协会 会长

胡俊涛 郑州市网络安全协会 会长

蔡舒婷 广州网络空间安全协会 秘书长

方满意 揭阳网络空间安全协会 会长

编委会委员：（排名不分先后）

崔华俊 中国电建集团北京勘测设计研究院有限公司 数智院网数部副主任

郭　亮 国富瑞数据系统有限公司 技术战略委员会副主任

陈　雷 北京国际数据跨境服务有限公司 总经理

陈华平 奇安信科技集团股份有限公司 集团副总裁

余慧英 北京长亭科技有限公司 战略发展副总裁

魏钦志 烽台科技(北京)有限公司 董事长

张　帅 北京数风科技有限公司 董事长

林小博 国源天顺科技产业集团有限公司 总经理

张西海 国汀信息科技(北京)有限公司 总经理

林　海 广东电网有限责任公司广州供电局 数字化部副总经理

周宏成 广东省电信规划设计院有限公司 信息集成院（集成院）副院长

朱江辉 广州低空经济产业发展有限公司 正高级工程师

何康鑫 广东南北科技有限公司 总经理

黄　盛 广州华南检验检测中心有限公司 技术总监

成珍苑 网安联认证中心有限公司 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

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 1

（一） 部委层面动向 3

1. 公安部印发《公安机关依法处置涉无人驾驶航空器违法行为行政处罚裁量基准》 3

2. 七部门联合印发《促进数字化绿色化协同转型发展实施方案（2026—2030 年）》 4

3. 国家网信办发布《数据出境安全管理政策法规问答（2026 年 9 月）》 5

4. 三部门联合印发《数字乡村高质量发展行动计划（2026—2030 年）》 5

5. 中央网信办秘书局发布《关于加强涉企侵权信息管理 持续推动营商网络环境优化的通知》 6

6. 民航局、国家数据局联合印发《民航数据治理体系建设实施方案》 7

7. 国家互联网信息办公室发布《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》 8

（二） 地方层面动向 9

1. 湖南省数据局等四部门印发《湖南省公共数据资源授权运营收益分配管理暂行办法》 9

2. 山西省印发《山西省工业互联网高质量发展行动方案》 10

3. 湖北省人民政府印发《数字湖北建设“十五五”规划》 11

4. 广东省政务服务和数据管理局发布《广东省公共数据管理办法（修订草案）》 12

5. 北京市人大常委会通过修订后的《北京市无人驾驶航空器管理规定》 12

6. 四川省发改委等六部门发布《四川省深化智慧城市发展 推进城市全域数字化转型行动计划（2026—2028 年）》 13

7. 江苏省互联网信息办公室发布《江苏省网络数据安全管理办法（草案）》（征求意见稿） 14

8. 四川省人大常委会发布《四川省网络安全条例（草案）》 15

境内前沿观察二：治理实践 17

（一） 公安机关治理实践 19

1. 公安部发布“净网—2026”专项行动阶段成果，侦办网络违法犯罪案件 3.6 万余起 19

2. 公安部发布“净网—2026”专项行动十起典型案例 20

3. 公安部发布“护网—2026”专项工作阶段成果，侦办行政案件 3.8 万起 24

4. 公安部发布“护网—2026”专项工作十起典型案例 25

5. 公安部网安局公布五起网暴运动员典型案例 28

6. 公安部网安局公布两起拒不履行信息网络安全管理义务罪典型案例.....29
7. 辽宁大连警方打掉以“职业打假”为名实施舆情敲诈的涉恶团伙.....31
8. 广东网警发布打击涉企网络谣言十大典型案例.....32
9. 湖南耒阳网警发布打击涉网违法犯罪十五大经典案例....33
10. 吉林公安网安部门打掉一网络暴力违法犯罪团伙，抓获涉案人员 98 名.....33
11. 湖南岳阳网警查处一起高校不履行网络安全保护义务案.....34
12. 湖南雁峰网警侦破一起提供非法控制计算机信息系统程序案.....35
（二） 网信部门治理实践.....36
1. 国家网信办发布十起网络安全、数据安全、个人信息保护等领域执法典型案例.....36
2. 国家网信办通报“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动第二批典型案例.....40
3. 中央网信办通报 30 款 App 个人信息收集使用问题.....42
4. 中央网信办部署开展“清朗·整治短视频虚假人设乱象”专项行动.....42

5. 天津网信办发布“海河安澜 2026”网络执法专项行动典型案例 43
6. 上海市网信办从严处置一批汽车类“自媒体”账号 47
（三） 通信管理部门治理实践 48
1. 安徽、北京、山东等省市通报侵犯用户权益的 APP（SDK）名单 48
（四） 其他部门治理实践 51
1. 最高人民法院发布四起人民法院网络法治典型案例 51
2. 湖南省发布 2026 年“亮剑湖湘·民生领域个人信息保护”专项执法行动取得阶段性成效 52
3. 我国发放首批数据产权登记凭证 52
4. 因数据安全问题，四家银行被央行处罚近五千万元 53
5. 因信息安全管理不到位，国家金融监督管理总局四川监管局对某保险公司处以罚款 15 万元 54
境内前沿观察三：人工智能安全专题 55
1. 2026 中国—东盟人工智能部长圆桌会议举行 57
2. 中美同意建立人工智能对话机制 57
3. 工业和信息化部印发《“人工智能+软件”专项行动实施方案》 58
4. 最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》 59

5. 全国网安标委发布《人工智能安全治理框架 3.0》 60
6. 中央网信办发布“清朗·整治 AI 应用乱象”专项行动第二阶段工作成果 61
7. CNCERT 通报 2026 年人工智能大模型安全众测活动典型漏洞风险 62
8. 江苏省发布《江苏省促进词元经济高质量发展行动方案（2026 年）》 63
9. 北京市印发《北京市加快词元经济发展的行动方案（2026—2028 年）》 64
10. 北京市印发《北京市人工智能+信息通信“京彩智联”行动计划（2026—2028 年）》 65
11. 湖北省印发《湖北省深入实施“人工智能+”三年行动方案（2026-2028 年）》 66
12. 北京市人民政府印发《“十五五”时期数智北京发展规划》 67
13. 江苏省五部门印发《江苏省支持人工智能创新发展有关实施方案的通知》 68
14. 湖北省两部门印发《湖北省算力券实施方案》 70
境外前沿观察：月度速览十则 71
1. 美国 CISA 发布更新版《内部威胁缓解指南》，帮助关键基础设施运营者等主体应对人工智能风险 73

2. 美国联邦调查局发布《网络战略》 73
3. 欧盟《网络弹性法》报告义务条款正式生效 74
4. 美国加州州长签署人工智能安全行政命令，拟要求大型前沿模型开发商在其实验室阶段定期进行审计和评估 75
5. 美国总统签署行政令将人工智能改称超级智能 76
6. 英国 NCSC 发布博客文章，对影子人工智能隐藏风险发出预警 77
7. 美国指控中国人工智能企业对美国前沿模型开展工业级蒸馏作业 78
8. 因违规处理用户位置数据，爱尔兰 DPC 对谷歌处以 4.03 亿欧元罚款 79
9. 澳大利亚总理通报 OpenAI 智能体入侵澳政府网站事件 .79
10. 美科技巨头签署白宫超级智能安全协议 80
行业前沿观察：各地协会动态 81
1. 中关村可信计算产业联盟成功召开《可信计算实训平台框架》等两项团体标准专家评审会 83
2. 海南省计算机学会主办的海南省首届青少年信息学 AI 编程大赛圆满落幕 83
3. 苏州市新媒体联合会携手市社会组织总会，为全市社团宣传工作支招赋能 84

4. 上海市信息网络安全管理协会数智创新系列高级研修班亮相 2026 新耀东方上安会 84

5. 苏州市互联网协会承办的苏州市网络安全进园区太仓专场活动圆满举行 85

6. 北京网络空间安全协会助力高校花式开展网络安全宣传教育活动 85

7. 佛山市信息协会承办“启沅杯”2026 年佛山市工业互联网安全技能竞赛 86

8. 惠州市计算机信息网络安全协会开展 2026 年网络安全宣传周系列活动 86

9. 吉林省信息技术应用协会第三届换届会议圆满召开 87

10. 昆明市网络安全协会联动全省 90 余所高校开展网民网络安全感满意度调查 87

11. 南通市信息网络安全协会成功承办 2026 年南通市网络安全宣传周法治日主题活动 88

12. 金华市网商协会成功举办 AIGC 破局增长——电商·短剧内容创作实战分享会 88

13. 珠海市网络空间安全协会人工智能安全和数据跨境流动工作服务站在斗门揭牌 88

14. 宁波市计算机信息网络安全协会顺利召开六届一次会长办公会议暨走进会员单位活动 89

15. 海南省网络安全和信息化协会开展多领域网络安全专题宣讲活动.....89

16. 汕头市网络空间安全协会承办的鲛城科学大讲堂第五期圆满举办.....90

17. 广东省网络空间安全协会成功举办“智御未来——AI 赋能网络空间安全新范式”论坛.....90

18. 广州网络空间安全协会联合承办的“人工智能安全治理与合规实践”高级研修班成功举办.....91

19. 肇庆市计算机学会协办的 2026 年肇庆市数据知识产权赋能企业宣传培训活动成功举办.....91

20. 上海市信息安全行业协会顺利召开 2026 上海网络安全产业创新推进会.....92

21. 天津市网络空间安全协会顺利召开第二届会员大会第一次会议.....92

22. 西藏自治区互联网协会与西藏自治区通信行业协会联合党支部书记彭坤同志当选西藏自治区互联网行业党委委员.....93

23. 徐州网络公共安防技术协会顺利召开 2026 年徐州市职工 AI+低空无人机应用技术技能竞赛筹备座谈会.....93

24. 湖南省网络空间安全协会顺利开展全省网络系统等级保护定级集中评审工作.....93

境内前沿观察一：政策立法

导读：9 月，网络与数据安全领域政策立法持续推进，中央和地方层面围绕数字化转型、数据治理、网络安全、数据开发利用以及重点场景治理等方面密集出台政策文件，整体呈现出数字化建设与安全治理同步推进、数据开发利用与规范管理并重的特点。

部委层面，数字化转型和数据要素开发利用仍是政策重点。中央网信办等七部门联合印发《促进数字化绿色化协同转型发展实施方案（2026—2030 年）》，推动数字化与绿色化协同转型；中央网信办、农业农村部、工业和信息化部联合印发《数字乡村高质量发展行动计划（2026—2030 年）》，围绕数字基础设施、乡村治理、公共服务和安全保障等作出部署。民航局、国家数据局联合印发《民航数据治理体系建设实施方案》，从数据基础制度、数据资源建设和数据流通利用等方面推进民航领域数据治理。国家网信办发布《数据出境安全管理政策法规问答（2026 年 9 月）》，进一步回应个人信息出境认证与数据出境安全评估衔接等实践问题。

安全治理方面，中央网信办秘书局发布《关于加强涉企侵权信息管理持续推动营商网络环境优化的通知》，进一步明确网站平台对涉企侵权信息的管理责任；国家互联网信息办公室发布《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》，围绕网络服务提供、未成年人模式、信息内容规范和协同治理等作出系统规定。公安部印发《公安机关依法处置

涉无人驾驶航空器违法行为行政处罚裁量基准》，进一步规范相关行政处罚裁量。

地方层面，政策重点主要集中在公共数据开发利用、区域数字化转型以及网络和数据安全制度建设。湖南出台《湖南省公共数据资源授权运营收益分配管理暂行办法》，广东发布《广东省公共数据管理办法（修订草案）》，进一步完善公共数据授权运营和开发利用机制。山西、湖北、四川分别围绕工业互联网、数字湖北和城市全域数字化转型出台行动方案或规划，将数据要素开发、安全保障和数字化治理纳入整体部署。江苏发布《江苏省网络数据安全管理办法（草案）》，对网络数据处理、数据开发利用和数据跨境流动等作出规定；四川发布《四川省网络安全条例（草案）》，进一步完善地方网络安全制度体系。

总体来看，9 月政策立法继续沿着数字化发展和安全治理两条主线推进。一方面，各部门和地方持续推动数据资源开发利用、行业数字化和城市数字化转型；另一方面，围绕网络安全、数据安全、个人信息保护、数据出境等制度安排不断细化，进一步强化数字化发展过程中的安全保障和规范治理。

关键词：数字化转型；数据治理；未成年人网络保护；无人驾驶航空器管理

（一）部委层面动向

1. 公安部印发《公安机关依法处置涉无人驾驶航空器违法行为行政处罚裁量基准》

8 月 26 日，公安部印发《公安机关依法处置涉无人驾驶航空器违法行为行政处罚裁量基准》，包括一般适用规则、具体行为的裁量基准等四部分内容。

一般适用规则方面，《裁量基准》提出，对具有多个裁量情节的，在调节处罚幅度时一般采取同向情节相叠加、逆向情节相抵减的方式，也可以将对整个案情影响较大的情节作为主要考虑因素。违法行为人同时有两个以上应当给予行政处罚的违法行为的，应当分别裁量，依法合并执行，在具体裁量时互不作为从重情节。

具体行为的裁量基准方面，《裁量基准》对未经实名登记实施飞行活动、无民事行为能力人或限制民事行为能力人违规操控民用无人驾驶航空器飞行等五类违法行为分别提出裁量基准。例如，针对未经实名登记实施飞行活动，《裁量基准》根据违法程度的不同，将处罚分为四档，包括责令改正、责令改正并处 200 元以下的罚款、责令改正并处 2000 元以上 1 万元以下罚款、责令改正并处 1 万元以上 2 万元以下罚款。（来源：公安部）

2. 七部门联合印发《促进数字化绿色化协同转型发展实施方案（2026—2030 年）》

9 月 4 日消息，中央网信办、国家发展改革委、工业和信息化部等七部门近日联合印发《促进数字化绿色化协同转型发展实施方案（2026—2030 年）》，围绕推动数智技术与绿色技术融合创新、提升新兴领域用能效率、深化重点领域双化协同应用、夯实双化协同基础支撑四个方面，部署了十四项重点任务。

推动数智技术与绿色技术融合创新方面，《实施方案》提出，发展绿色高效人工智能技术。加强存算一体、高性能存储、数据压缩、分布式训练框架、DB4AI（数据库为 AI 服务）等关键支撑技术研发，加快突破高速互联、高带宽内存、低功耗计算等核心技术，提升数据传输和模型训练效率。加快研究更加高效的模型训练和推理方法，积极推动混合专家、动态稀疏等模型架构优化迭代，加强量化、剪枝等模型压缩技术研究，探索轻量化部署方式，实现超大规模参数模型性能与资源开销平衡。加快构建软硬件全栈协同能力，加强低功耗芯片、算子加速库、通信、编译、框架、算法、多智能体协同等研发适配，支撑人工智能技术快速迭代和普惠易用。构建生成式人工智能全生命周期资源消耗评估体系，指导生成式人工智能服务提供商主动披露大模型资源利用情况，引导人工智能技术绿色高效发展。（来源：网信中国）

3. 国家网信办发布《数据出境安全管理政策法规问答（2026 年 9 月）》

9 月 11 日，国家网信办发布《数据出境安全管理政策法规问答（2026 年 9 月）》，涉及三个问题，分别是（1）通过个人信息出境认证出境个人信息的，应当符合哪些情形？（2）通过个人信息出境认证后，因出境个人信息规模增加需申报数据出境安全评估的，安全评估是否参考认证结果？（3）如何申请个人信息出境认证？

针对第二个问题，文件回应称，已通过个人信息出境认证，但自当年 1 月 1 日起累计出境 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息的，个人信息处理者应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。个人信息处理者申报数据出境安全评估时，可以将通过个人信息出境认证有关情况附后，说明个人信息处理者和境外接收方的个人信息保护水平、个人信息权益保障等情况，网信部门将在安全评估过程中予以参考。（来源：网信中国）

4. 三部门联合印发《数字乡村高质量发展行动计划（2026—2030 年）》

9 月 11 日消息，中央网信办、农业农村部、工业和信息化部近日联合印发《数字乡村高质量发展行动计划（2026—2030 年）》，围绕夯实数字乡村发展基础、提升乡村产业数字化水平、提升乡村建设信息化水平等五个方面，部署二十四项重点任务。

提升乡村治理智慧化水平方面，《行动计划》提出，稳步推进数字赋能乡村治理。集约应用乡村治理数字化工具，推动“数字化+网格”等模式创新应用。依法深入打击农村电信网络诈骗、网络赌博、非法金融活动等违法犯罪行为。持续推进“清朗”专项行动，营造良好网上舆论环境。健全“互联网+公共法律服务”、“智慧公共法律服务”供给机制，畅通农民群体获取优质法律服务渠道。

激发数字乡村发展内生动力方面，《行动计划》提出，守牢安全底线。坚持底线思维，增强风险意识，完善风险评估与预警机制，强化数字乡村重点领域网络安全防护能力建设。健全农村数字基础设施安全管理机制，规范数据采集、存储和使用管理，做好个人信息保护，保障涉农重要数据安全。（来源：网信中国）

5. 中央网信办秘书局发布《关于加强涉企侵权信息管理 持续推动营商网络环境优化的通知》

9 月 15 日，中央网信办秘书局发布《关于加强涉企侵权信息管理 持续推动营商网络环境优化的通知》，旨在压实网站平台主体责任，加大涉企侵权信息处置力度。

《通知》明确网站平台应处置的五类涉企侵权信息：一是个人信息类。包括泄露企业家身份证、护照、户籍档案、家庭住址、电话号码等个人身份及联系信息，以及生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息；二是侮辱贬损类。包括侮辱谩骂企业、企业家，恶搞丑化企业标识、产品和企业家肖像，将企业、企业家与色情低俗话题恶意关联，使用污名化词

汇诋毁企业、企业家或特定品牌用户；三是假冒仿冒类。包括假冒仿冒新闻单位制作发布的涉企监督信息，假借企业或企业家名义发布的信息，在公众账号名称、头像、简介中，擅自使用与企业相同或相似的名称标识或企业家姓名肖像；四是虚假误导类。包括断章取义、歪曲解读企业家过往言论，呈现与事实不符的搜索关键词联想、搜索落地页结果，已经权威辟谣、澄清的不实信息，与企业、企业家在超大平台上的官方账号发布的公开声明不符信息；五是其他类。包括涉企拉踩引战信息，集纳翻炒的企业旧闻旧事、负面信息，已被本平台处置过的涉企侵权信息，机器人账号、网络水军账号发布的涉企评论信息，明显违背公序良俗抹黑诋毁企业、企业家信息。（来源：网信中国）

6. 民航局、国家数据局联合印发《民航数据治理体系建设实施方案》

9 月 16 日消息，民航局、国家数据局近日联合印发《民航数据治理体系建设实施方案》，提出夯实数据基础制度、加强行业数据资源建设、推进数据要素高效流通等六项措施。

筑牢数字基础设施底座方面，《实施方案》提出，统筹推进行业级、各领域数据和算力基础设施建设，构建民航数据流通利用基础设施，全面构建高效互联、绿色低碳的民航数字基础设施底座。推进分类分级分层的行业数据平台集群顶层设计，明确民航行业级及各领域数据基础设施规模、结构、功能和发展模式，加快各类数据基础设施建设。统筹推进民航算力基础设施发展，鼓励行业龙头企事业单位适度集中建设算力基础设施，行业各单位可

通过租建结合的方式高效合理利用算力。推进民航行业可信数据空间以及分领域可信数据空间建设，实现数据按需融通，提升数据可信管控、资源交互、价值共创能力。完善高速泛在网络基础设施，提升跨区域、跨主体数据传输与交换效率，保障行业数据安全可控流通和高效利用。（来源：民航局）

7. 国家互联网信息办公室发布《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》

9 月 18 日，国家互联网信息办公室发布《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》，共二十五条，包括向未成年人提供网络服务、未成年人用户识别和信息内容规范、未成年人模式建设、协同共治要求和法律责任等内容。

规范向未成年人提供网络服务方面，征求意见稿明确网络服务提供者不得向未成年人提供陌生人网络社交服务、虚拟亲属和虚拟伴侣等虚拟亲密关系服务等，并规定了相关例外情形。征求意见稿提出网络服务提供者向未满十六周岁的未成年人提供网络音视频服务、网络直播发布服务以外的其他网络直播服务、网络游戏服务和网络社交服务等，应当通过未成年人模式提供。

未成年人模式建设方面，征求意见稿要求智能终端产品制造者为智能终端产品设置未成年人模式联动、一键切换、退出核验、防绕过等功能，明确应用程序分发平台服务提供者应当落实安全管理责任。规定未成年人模式应当符合国家有关规定和标准，具备有效识别危害或者可能影响未成年人身心健康的网络信息、预防未成年人沉迷网络等功能。明确提供未成年人

模式的智能终端产品制造者和网络服务提供者应当将未成年人模式设置及功能情况向省级网信部门备案等。（来源：网信中国）

（二）地方层面动向

1. 湖南省数据局等四部门印发《湖南省公共数据资源授权运营收益分配管理暂行办法》

8 月 12 日，湖南省数据局、湖南省财政厅、湖南省国资委等四部门联合印发《湖南省公共数据资源授权运营收益分配管理暂行办法》，自 2026 年 8 月 31 日起施行，有效期 2 年。《办法》共四章十七条，包括收益分配程序、监督管理等内容。

收益分配程序方面，《暂行办法》提出，实施机构应会同本级财政、发展改革、数据管理部门及运营机构，按照《国家发展改革委 国家数据局关于建立公共数据资源授权运营价格形成机制的通知》（发改价格〔2025〕65 号）成本核算相关规定，核定在授权运营过程中发生的各项成本。运营机构应建立健全成本管理制度，单独核算并准确记录公共数据资源授权运营经营成本和收入等情况。在提供数据产品与服务过程中，对公共数据资源进行采集、加工、流通、应用等环节中发生的实际支出纳入成本计算，不得将与授权运营无关的费用列入成本。同一成本不得重复计算。（来源：湖南省数据局）

2. 山西省印发《山西省工业互联网高质量发展行动方案》

8 月 24 日，山西省工业和信息化厅、山西省通信管理局印发《山西省工业互联网高质量发展行动方案》，围绕工业互联网基础设施提质行动、工业互联网平台能力提升行动、工业互联网赋能载体壮大行动等四个方面，提出十六项措施。

工业互联网平台能力提升行动方面，《行动方案》提出，加快释放工业数据要素价值。实施工业数据筑基行动，深化企业首席数据官制度建设，开展工业领域数据要素应用场景征集，编制工业场景数据要素应用参考指引，分类指导企业加强数据工程能力建设。推动工业互联网平台提升数据采集与汇聚能力，鼓励龙头企业建立工业数据可信流通空间，促进上下游工业数据共享流通。引导省级产业链、专业镇工业企业联合数据服务商，面向工业模型训练需求和典型应用场景，开展数据清洗、标注、治理与质量评估，打造一批行业高质量数据集。

工业互联网产业生态构建行动方面，《行动方案》提出，健全工业互联网安全保障体系。落实《工业互联网安全分类分级管理办法》，系统推进联网工业企业自主定级、定级核查、分级防护、符合性评测及安全整改工作。建立健全联网工业企业网络安全监测预警和信息通报机制，强化对重点联网工业企业的安全风险感知、分析研判和协同处置，对发现的网络安全问题隐患闭环管理。定期组织开展网络安全教育和应急演练，督促和指导企业持续完善技术防护措施。健全完善联网工业企业网络和数据安全管理体制机

制，压实企业安全主体责任，持续提升工业企业网络和数据安全防范意识和能力水平。（来源：山西省工业和信息化厅）

3. 湖北省人民政府印发《数字湖北建设“十五五”规划》

8 月 28 日，湖北省人民政府印发《数字湖北建设“十五五”规划》，围绕推进数字基础设施前瞻布局、释放数据要素价值、推动数智治理高效协同等十个方面，提出三十一条措施。

构建现代化数字安全治理体系方面，《规划》提出，构建数据安全屏障。落实数据分类分级保护制度，规范数据全生命周期安全防护。建强数据安全监测预警体系，构建审查、研判、通报、处置闭环，常态化开展“数安湖北”攻防演练。推动隐私计算、区块链等安全技术在可信数据空间、算力平台、数据流通交易平台应用。强化数据跨境安全管控，稳妥开展数据跨境试点，制定重点领域数据出境负面清单。

释放数据要素价值方面，《规划》提出，加强数据资源汇聚供给。持续开展全省数据资源调查，健全数据资源目录体系，形成全省数据资源“一本账”，构建省级一体化数据资源池。推动政务数据“应归尽归、一数一源”，实现全量归集、动态更新；引导市场主体规范归集产业感知、生产运营、行业服务等企业数据，拓宽社会数据合规供给渠道。发展专业化数据标注服务。聚焦科学研究、工业制造、医疗卫生等领域，实施高质量数据集协同建设行动，建成 500 个高质量数据集标杆产品。（来源：湖北省政府网）

4. 广东省政务服务和数据管理局发布《广东省公共数据管理办法（修订草案）》

9 月 1 日，广东省政务服务和数据管理局发布《广东省公共数据管理办法（修订草案）》，对 2021 年 10 月版本进行修订。

修订草案共十一章五十九条，包括公共数据目录管理、公共数据的收集、核准与提供等。本次修订亮点主要在于进一步规范公共数据资源目录管理和共享使用要求，建立公共数据授权运营和开发利用机制，促进公共数据赋能人工智能发展。主要涉及压实公共数据资源目录“应编尽编”工作要求、进一步细化“以共享为原则、不共享为例外”数据共享准则、建立公共数据授权运营与开发利用机制、新增公共数据赋能人工智能发展相关制度安排四个方面。

赋能人工智能发展方面，修订草案提出，确立公共数据主管部门、行业主管部门在推动公共数据赋能人工智能发展的主体责任，明确加强公共数据资源高质量供给、推进公共数据资源赋能行业高质量数据集建设以及推动公共数据与社会数据融合赋能人工智能创新应用的支持举措。（来源：广东省政务服务和数据管理局）

5. 北京市人大常委会通过修订后的《北京市无人驾驶航空器管理规定》

9 月 11 日，北京市第十六届人民代表大会常务委员会第二十六次会议通过对《北京市无人驾驶航空器管理规定》的修订，自 2026 年 11 月 15 日起施行。

《规定》提出，北京市行政区域全域为无人驾驶航空器管制空域，禁止在北京市行政区域内实施无人驾驶航空器飞行活动，禁止在北京市行政区域内持有、存放无人驾驶航空器及其核心部件，禁止运输、携带无人驾驶航空器及其核心部件进入北京市行政区域。《规定》强调，北京市禁止非法生产、组装、拼装、改装无人驾驶航空器；禁止非法破解无人驾驶航空器运行控制系统和改变无人驾驶航空器出厂性能、参数。

《规定》指出，属于下列情形之一，确需购买、运输、存放无人驾驶航空器及其核心部件的，经市公安机关会同有关部门进行安全评估后，按照清单化管理的原则予以特殊保障：一是因反恐维稳、抢险救灾、重大活动等需要；二是学校、科研机构、生产企业因教学、技术研发、生产等需要；三是因农林业生产等需要。（来源：北京市人大常委会）

6. 四川省发改委等六部门发布《四川省深化智慧城市发展 推进城市全域数字化转型行动计划（2026—2028 年）》

9 月 11 日，四川省发展和改革委员会、中共四川省委网络安全和信息化委员会办公室、四川省财政厅等六部门联合发布《四川省深化智慧城市发展 推进城市全域数字化转型行动计划（2026—2028 年）》。《行动计划》围绕实施城市智慧高效治理提升行动、实施数字美好生活行动、实施数字经济赋能行动等六个方面，提出二十三项措施。

实施城市智慧高效治理提升行动方面，《行动计划》提出，完善基层数智治理体系。健全“市—县—乡镇、街道—村、社区—网格”数字化治理运行管理体系，实现治理触角延伸至基层网格。推广“一表通”“川善治”等

应用，有效实现基层工作增效减负。以“天网工程”“雪亮工程”为基础，深化综治中心信息平台建设应用，推进视频图像智能化和视图大模型建设，提高重点人群服务管理和基层治理水平。强化“天府消安码”平台应用，实现单位场所赋码管理。依托数字技术进一步畅通公众参与城市治理渠道。拓展“信用+”应用场景，大力推广“信用+惠民便企”服务。

实施适数化改革创新行动方面，《行动计划》提出，推动管理体制机制创新。鼓励各市（州）充分利用城市智能中枢，创新跨部门数据合作机制，构建线下网格与线上网络联动协同机制，支持有条件的城市探索构建数智赋能的城市综合治理体制，推进跨部门、跨层级高效协同联动。省市协同推进有利于城市数字化转型的数据确权规则、数字权证应用、行政审批、项目管理、政府采购等制度改革。（来源：四川省发展和改革委员会）

7. 江苏省互联网信息办公室发布《江苏省网络数据安全管理办法（草案）》（征求意见稿）

9 月 23 日，江苏省互联网信息办公室发布《江苏省网络数据安全管理办法（草案）》（征求意见稿），共七章七十条，包括网络数据安全保护义务、网络数据开发利用安全管理、网络数据跨境流动安全管理等内容。

网络数据安全保护义务方面，征求意见稿提出，网络数据处理者依托自有数据或从第三方取得训练数据开展人工智能训练数据处理活动的，应当对数据来源合法性进行审查并记录，加强对训练数据及其处理活动的安全管理，采取有效措施防范和处置网络数据安全风险；使用自动化工具访问、收集公开的网络数据用于人工智能训练数据处理，应当遵循法律法规及国

家有关规定，符合网络数据相关主体的合理预期及隐私保护需求，不得非法侵入他人网络，不得干扰网络服务正常运行。机关事业单位在政务信息系统中部署人工智能大模型的，在上线前和运行期间应当定期组织大模型应用安全测试，对网络数据安全风险进行评估，加强有关训练数据及其处理活动的安全管理。

网络数据跨境流动安全管理方面，征求意见稿提出，中国（江苏）自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单，或参照适用其他自由贸易试验区已发布实施的负面清单，经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。数据出境负面清单内容发生变化的，应当重新申请备案。（来源：江苏省互联网信息办公室）

8. 四川省人大常委会发布《四川省网络安全条例（草案）》

9 月 24 日，四川省人大常委会发布《四川省网络安全条例（草案）》，共五章四十条，包括网络安全建设、网络安全保障、网络安全监管等内容。

网络安全保障方面，草案提出，本省依照法律、行政法规和国家有关规定对关键信息基础设施予以重点保护。本省在网络安全等级保护制度的基础上，对未列入关键信息基础设施的重要信息系统予以加强保护。省网信部门依法统筹协调重要信息系统安全保护工作，省级行业主管部门、监督管理部门在各自职责范围内负责重要信息系统的安全保护和监督管理工作。重

要信息系统的认定规则、具体范围和安全保护办法，由省网信部门会同有关行业和领域的主管部门、监督管理部门另行制定。

网络安全监管方面，草案规定，本省坚持发展和安全并重、促进创新和依法治理相结合的原则，对人工智能技术研发和应用服务实行包容审慎和分类分级监管，促进人工智能应用和健康发展。人工智能技术和服务提供者应当依法履行安全主体责任，落实人工智能相关管理制度，健全人工智能技术风险防控体系，对数据采集、模型训练、内容生成、拟人互动、对外服务等各环节实施全过程监测预警，常态化排查和处置各类风险隐患。（来源：四川省人大常委会）

境内前沿观察二：治理实践

导读：9 月，公安、网信、通信管理等部门持续推进网络空间安全治理，治理重点主要集中在网络违法犯罪打击、信息内容治理、网络和数据安全监管以及平台责任落实等方面。总体来看，9 月治理实践保持高压态势，专项行动推进、典型案例发布和日常监督检查相结合，网络空间综合治理进一步向常态化、协同化方向推进。

公安机关方面，“净网—2026”“护网—2026”等专项行动持续深入开展。“净网—2026”专项行动今年以来累计侦办网络违法犯罪案件 3.6 万余起，其中侵犯公民个人信息案件 4100 余起、黑客案件 3900 余起、网络谣言案件 1.1 万余起、网络暴力案件 2500 余起，重点打击侵犯公民个人信息、黑客攻击、网络谣言、网络暴力、网络水军以及网络黑灰产等违法犯罪活动。“护网—2026”专项工作累计开展网络和数据安全隐患排查 7900 余次，发现整改各类安全隐患和漏洞 3.8 万个，公开曝光违规收集个人信息的移动应用 652 款，侦办不履行网络安全、数据安全、个人信息保护义务类行政案件 3.8 万起，进一步强化网络运营者安全保护责任落实。

网信部门方面，网络安全、数据安全、个人信息保护和信息内容治理同步推进。国家网信办发布十起网络安全、数据安全、个人信息保护等领域执法典型案例，涉及网页篡改、恶意程序、数据被窃取以及数据和个人信息泄露等问题。中央网信办还在全国范围内部署开展为期 2 个月的“清朗·整治短视频虚假人设乱象”专项行动，重点整治短视频领域通过虚假身份、虚构

经历、摆拍编造等方式打造虚假人设、博取流量的问题，进一步规范短视频内容生态和账号运营秩序。同时，涉企信息治理等专项工作持续推进，平台主体责任和网络生态治理进一步强化。

通信管理部门持续开展移动应用和 SDK 侵害用户权益问题治理。其他部门和司法机关也通过典型案例、专项执法和行政处罚等方式加强网络空间安全治理。最高人民法院发布四起人民法院网络法治典型案例；金融监管领域则对数据安全和信息安全管理不到位问题持续开展处罚，其中四家银行因数据安全相关问题被罚金额合计近 5000 万元。

总体来看，9 月治理实践呈现出打击网络违法犯罪与落实安全保护责任并重的特点。一方面，针对网络谣言、网络暴力、侵犯个人信息、黑客攻击和网络黑灰产等突出问题持续强化打击治理；另一方面，通过监督检查、专项整治和个案查处等方式，进一步压实网络运营者、平台企业及相关主体的网络安全、数据安全和个人信息保护责任。

关键词：护网行动；净网行动；短视频虚假人设乱象；个人信息保护

（一）公安机关治理实践

1. 公安部发布“净网—2026”专项行动阶段成果，侦办网络违法犯罪案件 3.6 万余起

9 月 17 日，公安部发布“净网—2026”专项行动阶段成果。2026 年以来，全国公安机关网安部门持续深化“净网—2026”专项行动，累计侦办网络违法犯罪案件 3.6 万余起。

针对公民个人信息被窃取贩卖、“查档”“开盒”泄露公民个人信息等违法犯罪活动突出情况，公安机关网安部门严打侵犯公民个人信息犯罪活动，累计侦破相关案件 4100 余起。针对网络黑客技术不断升级，犯罪工具智能化、技术对抗白热化、犯罪技术低门槛等情况，公安机关网安部门聚焦危害社会公共秩序、市场税收安全、系统数据安全、生态环境安全和生产交通安全等领域黑客犯罪开展严厉打击，累计侦办黑客案件 3900 余起。

针对涉事故灾害、涉经济民生领域虚构事实、移花接木、AI 生成等网络谣言频发，公安机关网安部门坚持快查快处，侦破相关案件 1.1 万余起，及时开展辟谣宣传、回应舆论关切。同时，深挖幕后 MCN 机构、网络水军，查找整治行业管理漏洞，推进平台算法治理，研究 AI 生成内容监测等技术，着力压缩网络谣言生存空间。针对网络水军团伙充当网络乱象幕后推手，有组织地实施制造话题、蹭炒热点、有偿删帖、刷量控评等行为，公安机关网安部门坚持标本兼治、长效

治理的工作理念，依法严厉打击造谣引流、舆情敲诈、刷量控评、有偿删帖等违法犯罪活动，累计侦破相关案件190余起。

针对网络暴力违法犯罪严重侵犯公民合法权益、严重破坏网络生态秩序，公安机关网安部门聚焦“开盒挂人”、侮辱诽谤、电话短信“轰炸”等网络暴力违法犯罪活动，全面开展打击整治。同时，依法督促指导互联网企业平台加强信息内容审核管理和技术预警防范，全面构建综合整治长效机制，切实维护公民合法权益，累计侦破相关案件2500余起。

针对不法分子通过“以假乱真”手段仿冒官方网站和APP，从事虚假认证、制售假证、网络诈骗、窃取个人信息等违法犯罪活动，公安机关网安部门累计侦破相关案件40余起，封堵关停仿冒网站250余个。针对不法分子利用网站、通讯群组、浏览器、搜索引擎、网盘、社交媒体或利用违禁境外影视剧内嵌字幕、内容、广告等方式，批量发布短视频、链接、二维码、评论，为黄赌诈等各类网络违法犯罪实施推广引流，公安机关网安部门保持高压严打态势，累计侦办相关案件150余起。（来源：公安部网安局）

2. 公安部发布“净网—2026”专项行动十起典型案例

9月17日，公安部发布“净网—2026”专项行动十起典型案例。

案例一：江某某、刘某虚假摆拍“盲人女孩在盲道被撞反被骂”网络谣言案。2026年5月，一名博主发布自己在盲道上被逆行电动车撞击、盲杖掉落的视频，视频中撞人者不仅未道歉，还对被撞的盲

人女孩进行斥责，引发热议。经北京公安机关深入核查，视频中盲人和撞人者分别为江某某、刘某，二人为合作关系，共同运营视频账号，为吸粉引流、博取关注，虚假摆拍“盲人在盲道行走被电动自行车撞击并遭骑车人斥责”内容，通过短视频平台对外发布，误导网民，造成恶劣影响。江某某、刘某等2人已被依法采取刑事强制措施。

案例二：秦某某等人网暴抗洪救灾村干部案。2026年5月，湖南省常德市石门县极端强降雨自然灾害期间，该县某村党支部书记坚守一线参与抗洪救灾工作，因连日劳累，在接受媒体采访时声音嘶哑、神情疲惫，在谈及村庄受灾严重、损失巨大时动情落泪，引发网民共情关注。该报道传播过程中，个别网民无端指责该村支部书记佩戴首饰，发布贬低嘲讽言论，进而实施网暴。湖南、内蒙古、河北等地公安网安部门依法查处网暴行为15起，对秦某某、未某某等人依法处以行政处罚。

案例三：徐某网暴某运动员案。2026年4月，广东省某体育训练中心、国家体育总局某中心先后发布公开声明，称某运动员遭网暴并报警，引发舆论广泛关注。广东公安网安部门依法查明网民徐某系其他运动员“粉丝”，为所谓“维护偶像”，在网上公然发布侮辱该运动员及其“粉丝”言论。徐某已被依法处以行政处罚。

案例四：李某某等人实施舆情敲诈案。浙江、广东、福建等地公安机关侦破多起借“护剧”名义实施舆情敲诈案，查明以李某某、廖某、李某、郑某某为首的4个犯罪团伙，以文化传播有限公司为掩护，通过“大V”账号对新上映影视剧、综艺节目等发布负面信息，有组

织、有预谋、公司化、流程化炮制操控网络负面舆论，进而通过“公关合作”“护剧”名义收取费用，实施敲诈勒索，严重破坏网络舆论生态。目前，已累计抓获嫌疑人24名，其中7名主要犯罪嫌疑人已被依法采取刑事强制措施，案件正在进一步侦办中。

案例五：何某某等人侵犯公民个人信息案。四川成都公安网安部门侦破何某某等人侵犯公民个人信息案，查明四川成都不动产行业工作人员何某某、叶某等人利用职务便利，窃取房屋产权类敏感数据并进行售卖，经余某、李某等中间商层层转手，最终倒卖至房产中介、家装公司，严重危害公民个人信息安全。目前，何某某等14名犯罪嫌疑人已被依法采取刑事强制措施，案件正在进一步侦办中。

案例六：周某等人侵犯公民个人信息案。浙江温州公安网安部门全链条侦破一起电商物流行业“内鬼”侵犯公民个人信息案，查明周某与某电商平台第三方技术人员潘某、某物流公司大客户经理何某等行业“内鬼”相勾结，利用潘、何二人工作便利，获取电商平台内部加密订单数据与物流系统信息后，二次加工非法合成高精度个人信息包，并贩卖给黑灰产犯罪团伙。目前，周某等21名犯罪嫌疑人已被依法提起公诉。

案例七：周某等人非法控制计算机信息系统程序案。江苏盐城公安网安部门成功打掉一个破解停车场系统、非法获取车辆信息的黑产链条。经查，以周某为首的犯罪团伙开发专业黑客软件，破解停车场管理系统的加密传输通道，非法获取目标车辆的出入实时数据，并通

过境外网络黑灰产平台大肆出售，严重危害群众隐私安全。目前，周某等16名犯罪嫌疑人已被依法提起公诉。

案例八：高某某等人非法控制计算机信息系统案。广东广州公安网安部门接到某技术公司工作人员报案，称其大量用户设备被非法控制。经查，以高某某、陆某某为首的犯罪团伙利用该技术公司开发的系统漏洞，实施攻击等犯罪行为。企业发现漏洞进行升级更新时，又遭到该团伙持续实施的攻击，致企业业务中断数小时。公安机关查明，高某某等人非法控制各类计算机设备30余万台。目前，高某某等6名犯罪嫌疑人已被依法采取刑事强制措施，案件正在进一步侦办中。

案例九：尹某某、徐某某提供侵入、非法控制计算机信息系统程序案。山东济南公安网安部门巡查发现，有人在网上公开销售黑客软件。经查，尹某某自主开发具备入侵手机、窃取信息、操控终端等功能的手机端黑客软件，由徐某某等通过网络平台层层分销，累计销售黑客软件4000余套，非法获利100余万元。目前，犯罪嫌疑人徐某某、尹某某已被依法采取刑事强制措施，案件正在进一步侦办中。

案例十：袁某等人非法利用信息网络案。甘肃临夏公安机关网安部门查明，以袁某为首的犯罪团伙通过设立假冒教育培训网站，制售虚假学历、学位证书牟利。公安机关共查获伪印章近6000枚，假教师资格证书、假专业资格证书5000余份，涉案金额超百万元。目前，袁某等4名犯罪嫌疑人已被依法采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

3. 公安部发布“护网—2026”专项工作阶段成果，侦办行政案件 3.8 万起

9 月 17 日，公安部发布“护网—2026”专项工作阶段成果。2026 年，公安机关深入开展“护网—2026”专项工作，围绕网络安全、数据安全、信息安全重点任务，依托国家网络与信息安全信息通报机制，扎实推进网络空间安全保护和综合治理体系建设，集中整治一批突出风险问题，发现清理一批漏洞隐患，侦办一批不履行保护义务的行政案件，有力维护了关键信息基础设施、重要网络系统和数据安全。

一是政策法规体系更加完善。在中央网信委统一领导下，公安部制定出台了《公安机关网络空间安全监督检查办法》，联合有关部门发布了《网络数据安全风险评估办法》《网络安全标识管理办法》等规章，进一步完善网络空间安全法律规范体系，为依法管网治网提供了坚实保障，着力推动构建打防结合、防范为先、源头治理、协同联动的网络犯罪防治格局。

二是联防联控机制日益健全。公安部牵头建立国家网络与信息安全信息通报机制，着力打造通报预警工作体系，网络空间安全治理的联防联控格局初步形成，重要行业单位网络安全防护能力水平得到进一步提升。同时，通过国家网络与信息安全信息通报机制公众号面向公众发布预警，指导网络运营者开展针对性安全防护，促进提升全民网络安全防护意识和能力。

三是“护网”专项工作成效突出。公安机关联合有关行业部门针对 APP 违法违规收集使用个人信息问题、重点领域数据防护措施落

实不到位等突出问题开展集中整治，累计开展网络和数据安全隐患排查 7900 余次，发现整改各类安全隐患和漏洞 3.8 万个，公开曝光违规收集个人信息的移动应用 652 款，侦办不履行网络安全、数据安全、个人信息保护义务类行政案件 3.8 万起。（来源：公安部网安局）

4. 公安部发布“护网—2026”专项工作十起典型案例

9 月 17 日，公安部发布“护网—2026”专项工作十起典型案例。

案例一：江苏某公司不履行数据安全保护义务案。2025 年 11 月，江苏宿迁公安机关接有关部门线索通报，辖区某服务平台数据接口存在访问漏洞。经查，平台建设运维方江苏某公司在开发运维过程中，未采取数据传输及存储保护措施，对发现的安全漏洞未彻底整改，员工擅自访问并下载测评数据用于分析。目前，属地公安机关已依法对该公司予以行政处罚，并监督其销毁擅自留存的个人信息。

案例二：安徽芜湖某单位不履行网络安全保护义务案。2026 年 4 月，安徽芜湖公安机关接有关部门线索通报，辖区某 IP 地址存在异常和安全隐患。经查，该 IP 地址系当地某单位独立使用的通信组网 IP。因该 IP 地址使用的路由器存在漏洞且设备同时开放管理端口等功能，导致被恶意软件控制。由于处置及时，未造成严重后果。目前，属地公安机关已依法责令该单位改正。

案例三：江西南昌某信用中心不履行网络安全保护义务案。2026 年 1 月，江西南昌公安机关工作发现，辖区某中心的短信平台对外发送大量违法短信。经查，该中心运营的某小程序短信接口被不法分子

利用，共向7万余个手机号码发送14万余条涉赌违法短信。但该中心未启动应急预案，也未按规定向有关主管部门报告。目前，属地公安机关已依法对该中心和主管人员予以行政处罚。

案例四：山东济南某科技公司不履行数据安全保护义务案。2026年6月，山东济南公安机关接有关部门线索通报，辖区某科技公司运营的一款微信小程序后台存储数据被泄露。经查，该公司作为建设、运营单位，依托该小程序开展数据处理活动，但未建立相关安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施保障数据安全。目前，属地公安机关已依法对该公司予以行政处罚。

案例五：山东青岛某科技公司不履行网络安全保护义务案。2026年4月，山东青岛公安机关工作发现，辖区某科技公司的某平台被不法分子非法控制，通过该平台向外拨打诈骗电话。经查，该公司在运营平台期间存在多项违法行为：系统未部署防火墙、入侵检测等安全防护设备；未按规定留存网络日志；管理员账号存在漏洞等。上述问题被不法分子利用，造成平台被入侵控制并成为实施电信诈骗的工具。目前，属地公安机关已依法对该公司予以行政处罚。

案例六：广西钦州某运输集团不履行个人信息保护义务案。2026年7月，广西钦州公安机关工作发现，钦州某运输集团运营的一款微信小程序存在不履行个人信息保护义务的行为。经查，该集团在处理个人信息过程中存在多项违法行为：未制定内部管理制度和操作规程；

对存储的用户信息未采取安全技术措施；未定期对从业人员进行安全教育和培训。目前，属地公安机关已依法对该集团予以行政处罚。

案例七：四川宜宾某旅游开发公司不履行网络安全、数据安全、个人信息保护义务案。2026 年 7 月，四川宜宾公安机关接线索通报，兴文县某旅游开发公司的票务系统异常传输数据。经查，该公司票务系统云服务器被植入后门管理账户，导致数据被批量导出，且长期未被发现。经进一步调查，该公司存在多项违法行为：网络安全管理制度不完善，关键共用终端管理不规范，保护措施不到位；未建立相关安全管理制度；采集、存储、处理个人信息未履行告知义务，且未采取个人信息保护措施。目前，属地公安机关已依法对该公司予以行政处罚。

案例八：云南昆明刘某非法获取计算机信息系统数据、控制计算机信息系统案。2026 年 4 月，云南昆明西山公安机关接群众报警称，家中搭建的某品牌服务器出现严重网络堵塞，无法正常访问，疑遭网络攻击。经查，攻击该群众服务器的 IP 地址为刘某的个人家庭宽带。2026 年 2 月初，刘某获悉该品牌服务器存在高危漏洞后，批量获取服务器 IP 地址，并编写自动化攻击脚本，非法获取他人设备中的信息。目前，属地公安机关已依法对刘某予以行政处罚。

案例九:甘肃某游乐园不履行个人信息保护义务案。2026 年 7 月，甘肃公安机关在开展个人信息保护专项执法检查时发现，辖区某游乐园运维管理的智能储物柜、入园闸机仅支持人脸识别一种认证方式，未提供其他替代通行方案。经进一步核查，该游乐园作为个人信息处

理者，存在多项违法行为：采集人脸信息时未向顾客履行告知义务；采集行为不具备特定目的和充分必要性；未落实安全技术措施。目前，属地公安机关已依法对该公司予以行政处罚，并监督其销毁擅自留存的人脸信息。

案例十：宁夏某科技公司不履行数据安全保护义务案。2026 年 7 月，宁夏公安机关工作发现，某全球开源代码托管平台上存在用户以公开仓库形式，完整上传敏感数据的情况。经查，2025 年 4 月，宁夏某科技公司员工张某在负责某系统运维期间，为方便项目组内部协作和工作对接，私自将该系统的敏感信息上传至该托管平台个人仓库，造成张某负责运维系统的网络架构、安全防护体系、单位内部人员信息暴露。目前，属地公安机关已依法对该公司和张某予以行政处罚。（来源：公安部网安局）

5. 公安部网安局公布五起网暴运动员典型案例

9 月 18 日，公安部网安局公布五起网暴运动员典型案例。

案例一：黑龙江绥化公安网安部门查明，网民崔某泽为发泄个人情绪，多次在抖音平台发布针对某乒乓球运动员的侮辱诽谤言论，公然侮辱、诋毁该运动员，损害运动员个人声誉，严重扰乱网络公共秩序。目前，属地公安机关已依法对该崔处以行政处罚。

案例二：福建厦门公安网安部门查明，网民柯某系某乒乓球运动员粉丝，其多次在微博平台发布诋毁、贬损另一乒乓球运动员的帖文，

煽动网民对立情绪，恶意拉踩引战，损害运动员个人声誉，严重扰乱网络公共秩序。目前，属地公安机关已依法对该柯处以行政处罚。

案例三：山东滨州公安网安部门查明，网民贾某霞多次在微博平台发布针对某乒乓球运动员的侮辱诽谤言论，公然侮辱、诋毁该运动员，损害运动员个人声誉，严重扰乱网络公共秩序。目前，属地公安机关已依法对该贾处以行政处罚。

案例四：湖北恩施公安网安部门查明，网民贺某琳多次在微博平台发布针对某乒乓球运动员的丑化图片和侮辱诽谤言论，公然侮辱、诋毁该运动员，损害运动员个人声誉，严重扰乱网络公共秩序。目前，属地公安机关已依法对该贺处以行政处罚。

案例五：广西南宁公安网安部门查明，网民韦某偲系某跳水运动员粉丝，其多次在抖音平台发布侮辱、贬损其他跳水运动员的视频，并组织粉丝群体共同实施网暴活动，恶意拉踩引战，损害运动员个人声誉，严重扰乱网络公共秩序。目前，属地公安机关已依法对该韦处以行政处罚。（来源：公安部网安局）

6. 公安部网安局公布两起拒不履行信息网络安全管理义务罪典型案例

9 月 28 日，公安部网安局公布两起拒不履行信息网络安全管理义务罪典型案例。

案例一：江苏公安机关侦办的卢某斌拒不履行信息网络安全管理义务案。江苏盐城公安网安部门查明，辖区某公司违反《网络安全法》

等相关法律、行政法规规定，在未履行身份信息核验义务的情况下对外提供服务器租赁服务，公安机关依法对其进行行政处罚并责令其限期改正。该公司受到处罚后，仍未按要求进行及时整改，致使多人被骗，且导致刑事案件证据灭失，情节严重。其行为已触犯《刑法》第二百八十六条之一之规定，涉嫌拒不履行信息网络安全管理义务罪。公安机关网安部门依法开展立案侦查。后经法院审理，该公司法定代表人卢某斌因犯拒不履行信息网络安全管理义务罪，对其依法判处有期徒刑八个月，缓刑一年，并处罚金一万元。

案例二：河南公安机关侦办的张某东拒不履行信息网络安全管理义务案。河南三门峡公安网安部门查明，辖区某网络技术服务有限公司违反《网络安全法》等相关法律、行政法规规定，被诈骗团伙雇佣多次发布违法有害信息。公安机关依法对其进行行政处罚并责令其限期改正。该公司受到处罚后，仍未按要求进行及时整改，致使人民群众财产被骗，情节严重。其行为已触犯《刑法》第二百八十六条之一之规定，涉嫌拒不履行信息网络安全管理义务罪。公安机关网安部门依法开展立案侦查。后经法院审理，该公司法定代表人张某东因犯拒不履行信息网络安全管理义务罪，对其依法判处有期徒刑八个月，缓刑一年，并处罚金3000元。（来源：公安部网安局）

7. 辽宁大连警方打掉以“职业打假”为名实施舆情敲诈的涉恶团伙

9 月 10 日消息，辽宁省大连市公安局西岗分局近日成功打掉一个以网络“打假”为幌子、实则进行恶意索赔和舆情敲诈的涉恶团伙，抓获沈某某、董某某等 9 名犯罪嫌疑人，关联大连本地案件 10 起、山东案件 2 起，涉案金额 133 万余元。

2026 年 8 月，大连西岗警方接到群众举报，有人员通过电商平台批量采购地方特色食品，随后频繁发起投诉举报，并通过网络曝光、持续舆情施压等方式对经营企业进行滋扰纠缠、强行索财。警方逐条梳理交易订单、物流轨迹、网络短视频内容及资金流水，层层溯源、交叉印证，迅速锁定以沈某某、董某某为首的作案团伙。该团伙作案目标精准、步骤清晰、分工有序，专门瞄准重视品牌口碑、依赖线上销路的特色产品企业，拿捏企业忌惮负面舆情、担心经营受损的心理，步步施压、借机牟利。

该团伙的敲诈流程具有完整套路。团伙先以小额试购完成试探，锁定目标产品后随即批量囤货，再通过送检刻意挖掘、制造所谓“问题瑕疵”。一旦找到炒作空间，便集中在各大网络平台发布负面视频、捏造不实评价，肆意抹黑企业品牌形象。待舆情发酵、企业迫于声誉压力寻求和解时，团伙顺势提出高额索赔、有偿删帖等无理条件，将正常消费维权异化为敲诈敛财的工具。该团伙肆意曲解行业标准、刻意放大细微瑕疵，甚至张冠李戴、虚构产品问题。即便监管部门核查认定产品符合国家标准、合规可售，他们仍恶意抓取非标指标片面炒

作，拼接剪辑不实素材，持续通过高频投诉、全网扩散负面内容制造恐慌，反复纠缠企业、逼迫破财消灾。

经查，自2022年起，犯罪嫌疑人沈某某依托网络直播打造“打假博主”人设，积累网络热度、获取粉丝信任，随后注册成立传媒公司，招募网络主播、吸纳团伙成员，逐步搭建起组织严密、分工明确的犯罪体系。团伙运营多个网络账号，累计汇聚数百万粉丝，通过多账号联动发声、集中造势，放大负面舆情影响力。团伙内部权责清晰、流程明确，专人负责直播引流、塑造人设，专人负责选品采购、送检炒作，专人对接企业协商索赔、管控资金账目，形成“吸粉塑形象—选品设圈套—舆情造压力—索财分赃款”的完整黑色产业链。（来源：辽宁网警）

8. 广东网警发布打击涉企网络谣言十大典型案例

9月22日，广东公安网安部门发布打击涉企网络谣言十大典型案例，分别是：（1）深圳网民罗某某编造“饮料企业创始人不喝自家品牌饮料”不实文章被刑事拘留；（2）东莞网民肖某捏造虚假投诉信息敲诈勒索企业被刑事拘留；（3）深圳网民季某编造“某企业调整工作时长及福利”虚假短信被刑事拘留；（4）深圳网民王某编造“龙华某工厂一周内多人猝死”虚假信息被行政拘留；（5）东莞网民编造地产开发商虚假信息被行政拘留；（6）中山网民王某编造“工厂老板跑路”的不实信息被行政拘留；（7）惠州网民刘某捏造虚假信息抹黑某车企被行政拘留；（8）广州网民何某冒充某车企名义发

布虚假通告被行政罚款；（9）佛山网民李某恶意造谣抹黑企业及其高管被行政罚款；（10）惠州网民刘某用 AI 生成抹黑企业视频并传播被行政处罚。（来源：广东网警）

9. 湖南耒阳网警发布打击涉网违法犯罪十五大经典案例

9 月 22 日，湖南耒阳网警发布打击涉网违法犯罪十五大经典案例，分别是：（1）刘某某发布涉高考谣言案；（2）吴某用 AI 软件炮制虚假警察照片引流案；（3）罗某发布极端言论编造谣言案；（4）匡某贩卖公民个人信息案；（5）贺某某发布 AI 炮制涉高考虚假图片案；（6）摆拍“僵尸”惊悚视频，两名主播被行政拘留案；（7）雷某某非法获取公民个人信息案；（8）耒阳网安摧毁 5 个赌球团伙案；（9）罗某某用 AI 软件炮制“公交漂移”谣言案；（10）耒阳某电商公司不履行网络安全保护义务案；（11）伍某非法买卖公民个人信息案；（12）贺某某编造“有偿捉奸”虚假视频案；（13）刘某某持玩具枪拍视频蹭流量案；（14）黄某使用抢票外挂牟利案；（15）耒阳某装修公司不履行网络安全保护义务案。（来源：湖南网警）

10. 吉林公安网安部门打掉一网络暴力违法犯罪团伙，抓获涉案人员 98 名

9 月 22 日消息，吉林省吉林市公安网安部门近日成功打掉一个通过“网罗门徒、分级收费、按级授能、按劳返利”方式实施网络暴力的违法犯罪团伙，抓获涉案人员 98 名。

吉林市公安网安部门侦查发现，某网暴团伙效仿传统黑恶违法犯罪模式，对多人实施“污言刷屏式”群体辱骂、“短信轰炸式”恶意滋扰、“隐私揭盖式”曝光施压、“冥物寄送式”精神恫吓等不法行为，社会影响极其恶劣。经查，此网暴违法犯罪团伙面向因网络游戏社交引发矛盾纠纷的特定群体，根据“委托人”需求收取费用、定制“线上报复订单”。其中，冯某负责布置实施网络暴力“任务”，陈某负责团伙运营、接单派单、收益分配，何某、刘某等人从事“人肉开盒”和“短信轰炸”，并为网暴团伙非法行为提供“技术支持”，于某负责统计群组成员活跃度并发放“奖励”，形成“接单—派单—组群—施害—反馈”的“流水线化”作案模式。该网暴违法犯罪团伙对不特定网民实施精神霸凌，导致多名被害人出现抑郁、厌学等后果，工作、学习、生活遭受严重影响。

公安机关在查清不法事实的基础上，组织实施抓捕行动，一举抓获冯某、陈某等多名涉案人员，其中，已依法采取刑事强制措施19人，行政处罚32人。经审讯，该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：吉林网警）

11. 湖南岳阳网警查处一起高校不履行网络安全保护义务案

9月24日消息，湖南岳阳市公安网安部门近日在工作中发现，犯罪分子在辖区内某高校的弱电井房内加装VOIP设备，借此远程操控校园固话对外拨打诈骗电话，目前违法安装VOIP设备的嫌疑人已被抓获。对于该高校网络安全防护不到位的情况，岳阳公安网安部门

同步开展核查，发现该高校网络安全管理存在多项重大漏洞：对机房、弱电井房无巡查巡检制度，弱电井房未明确安全管理责任人且未上锁，未采取网络边界监测、线路异常通话监测等技术防护措施。对于上述问题，岳阳市公安机关依据《网络安全法》相关规定对该高校不履行网络安全保护义务的情形处以行政警告、责令改正。（来源：湖南网警）

12. 湖南雁峰网警侦破一起提供非法控制计算机信息系统程序案

9 月 28 日消息，湖南雁峰公安网络安全保卫大队近日成功侦破一起提供非法控制计算机信息系统程序案，抓获 1 名售卖抢红包外挂的犯罪嫌疑人。

2026 年 9 月，网络安全保卫大队在工作中发现，有人在网上销售秒抢红包的外挂程序。大队立即开展线索研判，查实犯罪嫌疑人谢某在家中，通过网络向多人销售“取*机”、“格*”等未经平台公司授权、擅自调用数据接口的第三方外挂程序。经查明，谢某某从上线处购进红包外挂软件，明知买家会利用该外挂秒抢红包，仍对外转售牟利。

经司法鉴定：“取*机”、“格*”等程序具有外挂程序所具有的特性，可调取平台数据接口获取红包信息、恶意读取红包状态、发送封包实现自动领红包功能，属于抢红包外挂软件。谢某的行为触犯《刑法》第二百八十五条第三款，涉嫌提供侵入、非法控制计算机信息系

统程序、工具罪。目前，犯罪嫌疑人谢某因涉嫌提供非法控制计算机信息系统程序罪已被刑事拘留，案件正在进一步深挖中。（来源：湖南网警）

（二）网信部门治理实践

1. 国家网信办发布十起网络安全、数据安全、个人信息保护等领域执法典型案例

9 月 15 日，国家网信办发布十起网络安全、数据安全、个人信息保护等领域执法典型案例。

案例一：上海某电子有限公司网页篡改案。网信部门核查发现，该企业 2020 年以来，长期忽视门户网站后台系统存在的管理员账号弱口令问题，未及时监测处置相关系统遭暴力破解等安全风险，该后台系统 2026 年 4 月遭攻击，网站源文件被植入恶意代码，通过搜索引擎检索网站相关内容，结果出现大量严重违法和不良信息。该企业未依法履行网络安全保护义务，发生网络安全事件时未及时启动应急预案并采取补救措施，未及时向有关主管部门报告，违反《网络安全法》等法律规定。属地网信办已依法责令其改正，予以罚款处罚。

案例二：北京某网络科技有限公司设置恶意程序案。网信部门核查发现，该企业运营“某助手”应用程序，用户数量约 35 万。该企业员工刘某在职期间曾参与该应用程序开发，后因劳动合同续签问题心生不满，在离职前向该应用程序植入恶意程序以获取推广费用。用户安装该应用程序后，使用浏览器首页及搜索引擎、书签等功能时，

页面跳转至推广链接。该企业未依法履行网络安全保护义务，疏于对所运营应用程序以及员工的管理，未及时发现相关问题并采取补救措施，危害用户网络安全，违反《网络安全法》等法律规定。属地网信办已依法责令其改正，予以罚款处罚，并将刘某涉嫌违法犯罪问题移送公安机关。

案例三：安徽某数据产业有限公司数据被窃取案。网信部门核查发现，该企业在开发“数字档案管理系统”过程中，使用存在未授权访问漏洞的ES开源版本，且在开发测试完成后未及时将测试数据删除，导致其中存储的2400余份审计报告、合同、会议纪要等企业内部文件被窃取，涉及网络安全等级保护测评报告、立项及概算批复文件等敏感内容。该企业未依法履行网络安全和数据安全保护义务，未采取技术措施和其他必要措施保障网络安全、数据安全，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律规定。属地网信办已依法责令其改正，予以警告、罚款，并对直接负责的主管人员予以罚款处罚。

案例四：河南某医院数据泄露风险案。网信部门核查发现，该医院体检系统存在弱口令漏洞，通过该漏洞能获取就诊病例等数据，属地网信办责令医院全面整改后复核发现，该医院网络防火墙、入侵防御系统、漏洞扫描工具、日志审计系统、数据库审计系统、堡垒机等安全设备因授权过期导致失效，网络系统终端仍然存在700个安全漏洞，包括73个可被利用的高危漏洞，数据泄露风险仍未消除。该医院未依法履行网络和数据安全保护义务，违反《网络安全法》《数据

安全法》《网络数据安全管理条例》等法律规定。属地网信办已依法责令其改正，予以警告、罚款，并对直接负责的主管人员予以罚款处罚，同时将相关情况通报属地卫生健康部门。

案例五：广东某软件技术有限公司个人信息泄露风险案。网信部门核查发现，该企业开发的“某盒子”硬件产品存在未授权访问漏洞，可在不经登录验证的情况下，通过网页访问其4000端口控制台业务，查看车辆状态信息。用户绑定微信公众号后，在其盒子产品向公众号传输个人信息、通过公众号查询车辆状态信息等的过程中，均未对信息采取加密措施。该企业未依法履行个人信息保护等义务，未采取身份认证、数据传输加密等必要技术措施保障用户个人信息安全，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律规定。属地网信办已依法责令其改正，予以警告处罚。

案例六：浙江某信息科技有限公司强制收集使用非必要个人信息案。网信部门核查发现，该企业运营的某运动管理App在用户开启跑步功能时，以“防止作弊”为由强制要求一次性授予定位权限、电话权限、存储权限等多种权限，若用户不同意授权，则以用户拒绝提供全部权限为由拒绝提供跑步相关功能。该企业未向不同场景用户提供差异化功能选择，一次性强制索取多个权限，且在有其他替代方式实现处理目的情况下，超范围收集使用非必要个人信息，违反《个人信息保护法》《网络数据安全管理条例》等法律规定。属地网信办已依法责令其改正，予以警告处罚。

案例七：重庆某置业有限公司违法收集人脸信息案。网信部门核查发现，该企业在办公场所安装 10 余处图像采集设备，收集、存储客户人脸信息 5000 余条，用于客户身份信息识别以及与中介机构等的匹配营销。该企业未真实、准确、完整向客户告知收集人脸信息的目的、方式、用途，在未取得客户单独同意的情况下，收集、存储、使用客户人脸信息，违反《个人信息保护法》《网络数据安全管理条例》等法律规定。属地网信办已依法责令其改正，予以警告、罚款处罚。

案例八：上海某科技有限公司超范围收集并违法出境个人信息案。网信部门核查发现，该企业自 2022 年以来，持续通过其 Windows 端应用程序，超范围收集用户使用其硬件产品的主机配置、使用时长、用户系统等信息，并将上述信息和用户注册其相关程序时填写的姓名、手机号、邮箱、生日、密码等信息，传输至境外有关数据中心。该企业超出实现处理目的最小范围收集用户个人信息，且在未依法申报数据出境安全评估情况下，向境外传输个人信息，违反《个人信息保护法》《促进和规范数据跨境流动规定》等法律规定。属地网信办已依法责令其改正，予以罚款处罚。

案例九：四川某科技有限公司运营的小程序未落实生成合成内容标识要求案。网信部门核查发现，该企业运营的微信小程序提供 AI 文本对话、图片生成等服务，但未对人工智能生成合成内容添加显式标识，未在文件元数据中添加包含属性信息、服务提供者名称或者编码、内容编号等制作要素信息的隐式标识，未在提供导出功能时对生

成合成内容添加显式标识，同时未按规定落实安全评估要求，存在内容安全风险，违反《互联网信息服务深度合成管理规定》《人工智能生成合成内容标识办法》《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》等法律规定，网信部门已依法责令下线该小程序。

案例十：江苏某科技股份有限公司提供生成式人工智能服务未按规定进行安全评估案。网信部门核查发现，该企业运营的 2 个网站以“API 中转站”方式调用多个大模型产品接口，提供对话、问答等服务，未按规定开展安全评估工作，存在内容安全风险，违反《生成式人工智能服务管理暂行办法》《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》等法律规定。属地网信办已依法责令其改正、从严处理责任人，予以警告处罚。（来源：网信中国）

2. 国家网信办通报“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动第二批典型案例

9 月 19 日，国家网信办通报“清朗·优化营商网络环境 整治恶意炒作涉企信息”专项行动成效。专项行动对恶意诋毁抹黑企业、集纳炒作涉企负面信息、借监督之名牟取非法利益等问题进行集中整治。同时，有针对性治理企业“内卷式”竞争，从严处置一批散布涉企不实信息、挑动消费群体对立的账号。专项行动期间，各级网信部门和重点商业网站平台清理涉企侵权信息 156 万余条，处置违法违规账号 2.6 万余个。同步发布第二批典型案例。

案例一：“观澜 FinResearch”等账号发布涉企负面不实信息，牟取非法利益。小红书账号“观澜 FinResearch”、今日头条账号“康子”、微博账号“天天观 C”、搜狐号“天下 G 查”发布涉企负面不实信息。在企业与其沟通删除不实信息时，要挟开展商务合作，支付所谓“宣传费”。涉及的账号已被依法依约关闭。

案例二：“赵亦雷”等账号持续散布贬损企业信息，挑动消费群体对立。抖音账号“赵亦雷”、微信视频号“快快变小胖哥”、小红书账号“周章”等账号运营主体在被有关部门行政处罚后拒不改正，仍旧通过上述账号发布攻击贬损企业产品信息，蓄意挑动消费群体对立。涉及的账号已被依法依约关闭。

案例三：“车市博览”等账号发布虚假不实信息，抹黑诋毁企业商誉。今日头条账号“车市博览”、哔哩哔哩账号“1 号车盟”、微博账号“造车局”，频繁在企业新品上市发布等节点，捏造散布企业经营困难、产品质量不佳等虚假信息，抹黑企业形象声誉。涉及的账号已被依法依约采取处置措施。

案例四：“菜乡之剑”等账号恶意集纳企业负面信息，翻炒企业旧闻旧事。新浪微博账号“菜乡之剑”、今日头条账号“糊涂大师”、微信视频号“探索第一现场”，恶意集纳涉企负面信息，频繁炒作企业旧闻旧事，持续唱衰企业发展前景。涉及的账号已被依法依约采取处置措施。（来源：网信中国）

3. 中央网信办通报 30 款 App 个人信息收集使用问题

9 月 20 日消息，中央网信办秘书局近日组织对 App（含小程序）收集使用个人信息行为进行检测，发现 30 款 App 存在个人信息收集使用问题。其中，Flow Fit、滑板车背诵等 6 款 App 未公开个人信息收集使用规则；iNAP Care、中英翻译通等 4 款 App 强制或频繁索要非必要权限；GPS 测亩仪、ROI 计算器等 9 款 App 未完整准确列明收集使用个人信息情况；红卷乐读、道臣智运等 11 款 App 未提供有效账号注销功能。

通报要求，相关 App 运营者应当于本通报发布之日起的 15 个工作日内完成整改，并将整改情况报中央网信办。中央网信办将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。（来源：网信中国）

4. 中央网信办部署开展“清朗·整治短视频虚假人设乱象”专项行动

9 月 30 日消息，中央网信办近日印发通知，在全国范围内部署开展为期 2 个月的“清朗·整治短视频虚假人设乱象”专项行动。专项行动重点整治假扮弱势群体、虚构职业资质、利用 AI 等仿冒人物、鼓吹奢靡迷信、编造冲突剧情五个方面突出问题。

网信部门将采取以下治理措施：一是加大违规账号和平台查处力度。依法从严打击借虚假人设恶意营销牟利、误导网民行为，依法从严打击通过 MCN 机构批量制作、多账号矩阵分发、跨平台搬运扩散

等方式大规模炮制同质化虚假人设行为。对于性质恶劣的账号，坚决予以封禁；二是强化短视频发布环节规范标注。对于未按要求进行内容标注的虚假人设类短视频，依法从严处置；督促网站平台切实履行内容审核义务，不得借已标注虚构演绎、AI 生成、营销、转载、个人观点等内容标签及无不良导向声明规避网络生态治理相关要求，从源头阻遏虚假人设类短视频的上传发布；三是加强重点板块呈现管理。严禁在榜单、推荐等位置推送虚假人设类短视频。强化资质审核管理，对暂缺乏职业分类、资格标准、认证要求且有严重非法牟利空间的领域，分类纳入日常治理重点；四是强化特定群体权益保障措施力度。紧抓内容创设、流量分发、审核管理等关键环节，对虚假打造“AI 霸总”“养生大师”等人设诱骗老年人、散布或集纳谣言贬损农村农民形象、冒充专业领域人士误导网民的短视频，依法依规严格处置。（来源：网信中国）

5. 天津网信办发布“海河安澜 2026”网络执法专项行动典型案例

9 月 28 日，天津网信办发布“海河安澜 2026”网络执法专项行动典型案例。

案例一：某科技发展有限公司不履行网络安全保护义务案。网信部门核查发现，该企业网站系统存在远程代码执行、任意文件读取等漏洞和弱口令问题，具有网页篡改、数据泄露等风险。该企业未依法履行网络安全保护义务，内部安全管理制度不健全，未制定网络安全

应急预案并定期组织开展应急演练，未采取技术措施和其他必要措施保障网络安全，违反《网络安全法》等法律规定。河北区网信办已依法责令其改正，予以警告处罚。

案例二：某科技有限公司未按规定处置、告知、报告安全风险案。网信部门核查发现，该企业主要经营互联网数据中心业务，为用户提供主机托管、互联网接入等服务，收到网信部门的网络安全漏洞通报后，在反馈的整改报告中谎报瞒报涉事系统、数据的相关情况。该企业发现其网络产品、服务存在安全缺陷、漏洞等风险后，既未立即采取有效补救措施，也未按照规定告知其用户并向网信部门报告相关情况，导致大量用户数据长期存在泄露风险，违反《网络安全法》等法律规定。西青区网信办已依法责令其改正，予以警告处罚。

案例三：某测试中心数据泄露风险案。网信部门核查发现，该单位运营的“实验室信息管理系统”开放非必要端口，存在未授权访问漏洞和弱口令问题，导致检测报告等业务数据存在泄露风险。该单位未依法履行网络安全和数据安全保护义务，相关安全管理制度不健全，未采取技术措施和其他必要措施保障网络安全、数据安全，未按规定留存相关网络日志，违反《网络安全法》《数据安全法》等法律规定。天津经济技术开发区网信办已依法责令其改正，予以警告处罚。

案例四：某文化旅游有限公司数据泄露风险案。网信部门核查发现，该企业运营的“票务管理系统”9200 端口的 ES 数据库服务存在未授权访问漏洞，导致大量票务信息等业务数据存在泄露风险。该企业未依法履行网络安全和数据安全保护义务，未制定相关安全管理制

度和操作规程，未采取技术措施和其他必要措施保障网络安全、数据安全，未按规定留存相关网络日志，违反《网络安全法》《数据安全法》等法律规定。北辰区网信办已依法责令其改正，予以警告处罚。

案例五：某医疗供应链管理服务公司数据泄露风险案。网信部门核查发现，该企业运营的“销售数据透视系统”存在任意文件上传、远程代码执行等漏洞和弱口令问题，导致医疗物资采购、仓储、配送等业务数据存在泄露风险。该企业未依法履行网络安全和数据安全保护义务，未采取技术措施和其他必要措施保障网络安全、数据安全，未按规定留存相关网络日志，违反《网络安全法》《数据安全法》等法律规定。武清区网信办已依法责令其改正，予以警告处罚。

案例六：某科技有限公司违法处理个人信息案。网信部门核查发现，该企业运营的体检系统为医院提供在线体检预约、健康管理等服务，存在身份认证绕过、接口未授权访问等漏洞，导致大量体检报告等敏感个人信息存在泄露风险。其在接受某医院委托处理个人信息的过程中，违反双方约定擅自将该医院的个人信息用于其他系统测试。该企业未依法履行网络安全和个人信息保护义务，未采取技术措施和其他必要措施保障网络安全、个人信息安全；作为受托方超出双方约定的目的、方式处理个人信息，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律规定。市网信办已依法责令其改正，予以警告、罚款处罚。

案例七：某健康管理有限公司个人信息泄露风险案。网信部门核查发现，该企业运营的某“医生端”系统提供在线问诊等服务，存在

横向越权漏洞和弱口令问题，导致大量电子处方等敏感个人信息存在泄露风险。该企业未依法履行网络安全和个人信息保护义务，未采取技术措施和其他必要措施保障网络安全、个人信息安全，违反《网络安全法》《个人信息保护法》等法律规定。和平区网信办已依法责令其改正，予以警告处罚。

案例八：某科技有限公司个人信息泄露风险案。网信部门核查发现，该企业运营的体检系统提供职业病体检预约服务，存在硬编码密钥、接口未授权访问、SQL 注入等漏洞和弱口令问题，导致大量体检报告等敏感个人信息存在泄露风险。该企业未依法履行网络安全和个人信息保护义务，未采取技术措施和其他必要措施保障网络安全、个人信息安全，违反《网络安全法》《个人信息保护法》等法律规定。河东区网信办已依法责令其改正，予以警告处罚。

案例九：某科技有限公司个人信息泄露风险案。网信部门核查发现，该企业运营的代驾里程计价系统存在身份认证绕过、越权访问、任意文件上传等漏洞，导致司乘人员的行踪轨迹、支付账户等敏感个人信息存在泄露风险，企业及个人账户资金存在被盗刷窃取风险。该企业未依法履行网络安全和个人信息保护义务，未采取技术措施和其他必要措施保障网络安全、个人信息安全，未按规定留存相关网络日志，违反《网络安全法》《个人信息保护法》等法律规定。红桥区网信办已依法责令其改正，予以警告处罚。

案例十：某科技有限公司提供生成式人工智能服务未按规定进行安全评估案。网信部门核查发现，该企业运营的“AI 创作平台”调用

大模型产品接口向用户提供对话、问答等服务，未按规定开展安全评估工作，存在内容安全风险，违反《生成式人工智能服务管理暂行办法》《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》等法律规定。南开区网信办已依法责令下线该平台。（来源：网信天津）

6. 上海市网信办从严处置一批汽车类“自媒体”账号

9 月 30 日消息，上海市委网信办近日会同市经信委、市商务委、市市场监管局、市公安局网安总队，集中开展汽车行业网上信息传播秩序专项整治行动。截至目前，汽车领域专项整治行动已累计清理违法违规和不良信息 9.68 万余条，处置违规账号 9800 余个。

专项行动重点整治网上汽车交易不实信息、汽车价格虚假信息，以及恶意唱衰车市、煽动非理性维权等违法违规内容。专项行动期间，上海市委网信办专门开设“规范汽车行业网上信息传播秩序”举报入口，委托第三方机构全面巡查，梳理违法违规信息线索。在对问题线索联合会商、综合研判基础上，近期上海市委网信办协调对一批违规汽车“自媒体”账号依法采取禁言 90 天、暂停粉丝增长 90 天、暂停营利权限 180 天等处置措施。（来源：网信上海）

（三）通信管理部门治理实践

1. 安徽、北京、山东等省市通报侵犯用户权益的 APP（SDK）名单

（1）安徽省

9 月 2 日，安徽省通信管理局针对 2026 年第 4 批次整改不到位的 APP 予以公开通报，并要求限期整改。截至目前，尚有 5 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，立即对名单中的应用软件进行下架处理。

此外，安徽省通信管理局近日对省内 APP 进行了拨测检查，检测发现 25 款 APP 存在违法违规收集使用个人信息的问题，2026 年 7 月 24 日对上述违规 APP 开发者下达了责令改正通知书，要求限期完成整改工作。截至目前，尚有 8 款 APP 未完成问题整改，相关 APP 开发者应在 2026 年 9 月 7 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。

（2）北京市

9 月 2 日消息，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”“APP 频繁自启动和关联启动”等侵害用户权益问题。截至通报，尚有 5 款移动互联网应用程序未整改或整改不到位，予以公开通报。

2026 年 8 月 4 日，北京市通信管理局通报北京市部分存在侵害用户权益行为的移动互联网应用程序并要求整改。截至通报，仍有 2 款移动互联网应用程序未整改或整改不到位，现予以全网下架处置。

（3）山东省

9 月 2 日，山东省通信管理局通报 2026 年第 3 批不合格 APP 的整改情况。

截至 9 月 2 日，有 15 款存在问题并被山东省通信管理局通知限期整改的 APP 未按要求在限期内完成整改反馈，现予以通报。9 月 9 日前，上述 15 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 9 月 2 日，有 3 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。

（4）上海市

9 月 11 日消息，上海市通信管理局近日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 6 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。

（5）江苏省

9 月 15 日消息，江苏省通信管理局近日组织核查复检今年以来向社会公示的六批次存在侵害用户权益行为的 APP，发现仍有 10 款 APP 未完成整改，现对上述 APP 进行下架，相关应用商店应立即组织对名单中应用软件进行下架处理。

（6）广东省

9 月 20 日，广东省通信管理局近日开展移动应用程序专项治理工作，发出《APP 整改通知书》责令违法违规 APP 运营者限期整改。截至通报，尚有 21 款 APP 未完成整改。上述 APP 主办者应在 2026 年 9 月 29 日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施。

（7）浙江省

9 月 29 日消息，浙江省通信管理局近日组织第三方检测机构对群众关注的教育领域 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 9 款 APP、小程序未按要求完成整改。相关运营主体于 10 月 14 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。

此外，2026 年 8 月，浙江省通信管理局向社会公开通报了第七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，已有 13 款 APP 已完成通报问题整改；尚有 2 款 APP 未按期完成整改，现依法予以下架处置。

（来源：安徽、北京、山东、上海、江苏、广东、浙江通信管理部门）

（四）其他部门治理实践

1. 最高人民法院发布四起人民法院网络法治典型案例

9 月 16 日，最高人民法院发布四起人民法院网络法治典型案例，分别是：（1）明确适用人格权侵害禁令的考量因素，及时有效遏制网络暴力——李某申请人格权侵害禁令案；（2）明确带货主播侵害他人人格权的责任认定规则，强化网络空间人格权益保护——李某瑾诉某文化公司网络侵权责任纠纷案；（3）厘清搜索引擎服务提供者的侵权责任边界，平衡技术创新与权利保护——某文化公司诉某网络科技公司侵害作品信息网络传播权纠纷案；（4）依法惩处为跨境赌博提供技术支持服务的犯罪，维护网络空间安全——黄某等人开设赌场案。

其中，黄某等人开设赌场案中，菲律宾某跨境赌博集团开发、运营了 14 个赌博网站、6 个第四方支付平台，组织、招揽我国公民参与网络赌博。2016 年至 2020 年，被告人黄某等人根据菲律宾某跨境赌博集团安排，在中国成立某软件科技公司，为该赌博集团提供技术支持服务，包括网络赌博软件开发、编写服务器代码、对服务器和域名进行管理、维护赌博平台等。经查，黄某等人违法所得共计 1216 万余元。重庆市綦江区人民法院经审理认为，被告人黄某等人根据赌博犯罪集团安排，为赌博犯罪活动提供软件开发等技术支持服务，构成开设赌场罪，判处黄某等人有期徒刑五年六个月至六个月不等，并处

罚金。宣判后，部分被告人提出上诉，2023 年 12 月 6 日，重庆市第五中级人民法院作出二审裁定，驳回上诉，维持原判。（来源：最高人民法院）

2. 湖南省发布 2026 年“亮剑湖湘·民生领域个人信息保护”专项执法行动取得阶段性成效

9 月 18 日，湖南省网信办联合省教育厅、省公安厅、省住建厅、省交通厅、省文旅厅、省卫健委、省地方金融管理局、省通信管理局、省邮政管理局等十部门，聚焦交通出行、文化旅游、金融理财、房产物业、教育培训、医疗健康等民生领域违法违规收集使用个人信息等问题，自 2026 年 6 月起组织开展“亮剑湖湘·民生领域个人信息保护”专项执法行动。

本次行动通过远程技术检测、取证固证，会同各行业主管部门实施摸底排查、线索收集、现场检查和执法约谈，依法查处了一批违法违规收集使用个人信息的行为。截至目前，全省共检测发现 155 家单位的应用程序存在违法违规收集使用个人信息的问题，已对 58 家单位开展现场检查，约谈 73 家单位负责人，下达责令整改通知书 42 份，对 14 家单位处以行政处罚。（来源：湖南省网信办）

3. 我国发放首批数据产权登记凭证

9 月 22 日消息，我国首批数据产权登记凭证陆续发放，56 家企业和机构获得相关数据的持有权、使用权和经营权。首批获发数据产

权登记凭证的主体主要包括国有企业、事业单位和民营企业三类，涵盖医疗健康、交通运输、信息技术、科学研究等 10 余个行业领域。在首批发放的 56 份数据产权登记凭证中，与人工智能应用相关场景的登记数据超过 15 份。（来源：新华社）

4. 因数据安全问题，四家银行被央行处罚近五千万元

9 月 24 日，中国人民银行公布行政处罚信息，四家银行因数据安全相关问题被罚，包括一家国有银行、两家股份制银行和一家头部城商行，罚款金额合计近 5000 万元。

一是邮储银行因违反数据安全管理规定等 10 项违法行为，被警告、通报批评，没收违法所得 0.02902 万元，并处罚款 1743.3 万元。同时，行内 8 人被罚，其中运营数据中心王某星对违反数据安全管理规定负有责任，被罚款 1 万元。

二是广发银行因违反数据安全管理规定等 10 项违法行为，被警告，没收违法所得 1.621747 万元，并处罚款 1712.4 万元。

三是渤海银行因违反网络安全管理规定、数据安全管理规定等 11 项违法行为，被警告，没收违法所得 8.510725 万元，并处罚款 534.37 万元。

四是江苏银行因违反数据安全管理规定、网络安全管理规定等 13 项违法行为，被警告、通报批评，没收违法所得 0.17822 万元，并处罚款 937.1 万元。同时，行内 6 人被罚，其中信息科技部、大数据部

王某对违反数据安全管理规定负有责任，被罚款 1 万元。（来源：中国人民银行）

5. 因信息安全管理不到位，国家金融监督管理总局四川监管局对某保险公司处以罚款 15 万元

9 月 24 日，国家金融监督管理总局四川监管局发布处罚信息显示，国宝人寿保险股份有限公司因信息安全管理不到位，被处以罚款 15 万元；对相关责任人欧阳某某、王某某处以警告并合计罚款 2 万元。（来源：国家金融监督管理总局四川监管局）

境内前沿观察三：人工智能安全专题

导读：9 月，我国人工智能相关工作主要围绕国际合作、安全治理、司法规范和产业发展展开。一方面，人工智能治理制度和实践持续完善；另一方面，“人工智能+”、词元经济、算力基础设施等相关政策加快落地，人工智能发展与安全治理同步推进。

国际合作方面，中美同意建立人工智能对话机制，就人工智能相关风险和惠益开展交流，并建立人工智能事件沟通渠道；2026 中国—东盟人工智能部长圆桌会议围绕人工智能发展、安全和风险治理形成多项共识，强调共同应对深度伪造、隐私泄露、算法偏见等问题。

国内治理方面，最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》，对涉人工智能侵权、知识产权、案件审理机制等作出规范；全国网安标委发布《人工智能安全治理框架 3.0》，进一步完善人工智能安全治理框架。中央网信办“清朗·整治 AI 应用乱象”专项行动持续推进，第二阶段累计清理违法违规信息 561 万余条，查处账号 4.9 万余个，处置违规网站、应用程序等 2400 余个。

产业发展方面，工业和信息化部印发《“人工智能+软件”专项行动实施方案》，围绕软件生产变革、智能体软件新业态和安全保障等作出部署。北京、江苏等地围绕词元经济、人工智能与信息通信融合发展出台行动方案，湖北等地也从“人工智能+”和算力支持等方面加快政策布局。

总体来看，9 月人工智能领域一方面持续加强安全治理、司法规范和专项整治，另一方面加快推动产业应用、基础能力和相关新业态发展，人工智能治理与发展并重的政策脉络进一步清晰。

关键词：人工智能治理；AI 应用乱象整治；词元经济；算力基础设施

1. 2026 中国—东盟人工智能部长圆桌会议举行

9 月 17 日，以“共商 AI 治理 共创安全未来”为主题的 2026 中国—东盟人工智能部长圆桌会议在南宁举行。中国国家互联网信息办公室以及文莱、老挝、缅甸、柬埔寨、越南、印度尼西亚、新加坡、马来西亚、泰国等东盟国家有关部门代表，围绕人工智能发展、算法偏见、伦理安全和风险治理交流实践经验。

会议形成五点共识：第一，人工智能带来重大发展机遇，不能因风险而放弃发展；第二，全球对人工智能安全治理仍处于探索阶段，需要加强交流、互鉴与合作；第三，深度伪造、隐私泄露、算法偏见等问题需要各方采取实际行动；第四，应通过监管、治理、合作和互鉴共同应对人工智能安全问题；第五，应在联合国框架下发挥世界人工智能合作组织作用，强化中国与东盟合作。（来源：广西日报）

2. 中美同意建立人工智能对话机制

9 月 23 日至 25 日，中国国家主席习近平对美国进行国事访问。其间，两国元首就中美建设性战略稳定关系及重大国际地区问题深入交换意见，达成八点成果共识，包括双方同意建立中美人工智能对话，交流人工智能相关风险和惠益。下次对话将于今年 11 月举行。双方同意建立人工智能事件的沟通渠道。（来源：新华社）

3. 工业和信息化部印发《“人工智能+软件”专项行动实施方案》

9月2日，工业和信息化部印发《“人工智能+软件”专项行动实施方案》，围绕推进软件生产变革、培养智能体软件新业态、拓展智能体软件服务等六个方面，提出十九项措施。

推进软件生产变革方面，《方案》提出，推动智能编程赋能软件安全。支持企业运用大模型和智能编程工具，对存量软件实施漏洞挖掘、缺陷自动识别和风险分级评估，提升高危安全隐患的发现和修复能力。推动软件企业将智能安全检测嵌入软件开发全流程，实现安全隐患实时发现、及时处置。强化渗透测试、攻防模拟等智能化安全测试手段，提升软件安全验证能力。

优化软件产业发展环境方面，《方案》提出，提升软件领域安全保障能力。加强人工智能生成代码安全审查，防范智能编程工具恶意指令注入等新型攻击，强化开发工具、代码库等访问控制。研究智能体身份标识、可信互联、数据安全、行为管控等安全技术，推动建立覆盖开发、部署、应用等环节的智能体安全管理规范。面向人工智能融合趋势，完善软件产品和服务质量管理与测评规范。加强人工智能生成代码的知识产权合规治理。（来源：工业和信息化部）

4. 最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》

9月7日，最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》，围绕依法规制利用人工智能的侵权行为，依法审理涉人工智能知识产权纠纷案件，探索完善审理程序规则、依法惩治违法犯罪行为，健全完善涉人工智能纠纷案件审理和工作机制等五方面规定24条内容。

依法规制利用人工智能的侵权行为方面，《意见》首先明确了涉人工智能侵权责任的归责原则，其后针对利用人工智能侵害人格权、个人信息权益、消费者权益等不同场景，明确了侵权责任的认定和承担。此外，对生成式人工智能服务提供者的侵权责任、人工智能产品责任、涉自动驾驶汽车和辅助驾驶功能汽车交通事故的赔偿责任等作出了明确。

探索完善审理程序规则、依法惩治违法犯罪行为方面，《意见》主要包括两方面内容：一方面，针对涉人工智能纠纷案件技术性、专业性强等特点，探索完善涉人工智能纠纷案件的事实查明和证据审查规则，同时对利用人工智能不当取证、提供虚假材料等妨害司法秩序行为的依法规制作出了明确；另一方面，对依法惩治利用人工智能实施的各类犯罪行为作出了原则规定。（来源：最高人民法院）

5. 全国网安标委发布《人工智能安全治理框架 3.0》

9 月 14 日，全国网络安全标准化技术委员会发布《人工智能安全治理框架 3.0》。《框架 3.0》分为人工智能安全治理原则、人工智能安全风险分类、人工智能安全风险技术应对措施等五个部分。

《框架 3.0》提出，人工智能安全风险分为内生安全风险、应用安全风险以及衍生安全风险。针对三类人工智能安全风险，《框架 3.0》分别提出对应的应对技术措施。例如，在内生安全风险的应对措施方面，《框架 3.0》针对模型安全风险，提出改进模型架构，扩充训练数据的规模和多样性，引入人类监督机制，提升模型的泛化能力和输出结果可靠性；在训练或微调过程中加入注入攻击样本、网络漏洞信息等高质量训练数据，提升模型防御注入攻击、恶意指令及后门攻击的能力等应对措施。

《框架 3.0》还提出五项人工智能安全风险综合治理措施，包括完善人工智能安全治理顶层设计、提升人工智能安全治理能力水平、构建柔性、动态、可控的沙箱监管环境等。例如，在完善人工智能安全治理顶层设计方面，《框架 3.0》提出，完善人工智能安全法律法规、充分发挥技术标准的引领带动作用、构建人工智能安全风险快速发现与应对体系、加强人工智能科技伦理治理。（来源：全国网安标委）

6. 中央网信办发布“清朗·整治 AI 应用乱象”专项行动第二阶段工作成果

9 月 2 日消息，中央网信办近日组织开展“清朗·整治 AI 应用乱象”专项行动第二阶段工作，聚焦利用 AI 制作发布虚假信息、传播暴力低俗内容、假冒仿冒他人、侵害未成年人权益等突出问题，部署各地网信部门深入推进重点整治任务。截至目前，累计清理违法违规信息 561 万余条，查处账号 4.9 万余个，处置违规网站、应用程序等 2400 余个。

专项行动开展以来，各地网信部门切实履行属地监管责任，因地制宜推出一系列针对性治理措施。北京网信办指导网站平台全面升级审核策略，持续提升违规内容新型变体识别处置能力。上海网信办督促平台深入开展自查自纠，加大违法违规信息和账号查处力度，推出 AI 应用“知识普及包”引导公众识别问题风险。浙江网信办对属地重点平台开展“一企一策”问诊进行合规指导，督促完善内控体系，依法查处一批问题突出的 AI 应用软件。广东网信办召开重点网站平台工作例会，对多款应用违规问题开展点对点督促整改，确保专项行动取得实效。

网站平台积极响应专项行动部署安排，持续健全 AI 内容常态化治理机制。抖音、快手、微博、腾讯、百度、哔哩哔哩、小红书、知乎、豆瓣、淘宝等平台进一步强化技术赋能，优化多模态识别模型，动态扩充人脸库、声纹库和违规样本库，上线人脸实时治理系统等功能措施，提升违规内容智能检测和拦截效率，加大对违规账号、信息

处置力度，畅通线索举报渠道，累计发布各类治理公告 46 期。豆包、元宝、千问、文心一言等平台严把原始语料内容审核关，严格限制违规内容输出，强化 AI 生成合成内容标识要求落地，从源头防范违法违规信息生成传播。华为、小米、OPPO、vivo 等应用商店制定严格的 APP 开发者准入规范和上架要求，对在架 APP 进行抽检复测，有效拦截违规应用入库。

同步发布一批围绕利用 AI“魔改”经典、生成“数字泔水”，AI 制作发布虚假不实信息，AI 假冒仿冒他人，制作发布暴力低俗等信息，AI 侵害未成年人权益，利用 AI“托管”从事网络水军活动，AI 产品服务和应用程序违规方面的典型案例。（来源：网信中国）

7. CNCERT 通报 2026 年人工智能大模型安全众测活动典型漏洞风险

9 月 15 日，国家互联网应急中心 CNCERT 发布《关于 2026 年人工智能大模型安全众测活动典型漏洞风险的通报》。通报指出，众测活动共动员 2467 名白帽子，对国内 25 家 AI 厂商的 54 款大模型及智能体应用产品进行漏洞测试。

众测活动累计发现各类安全漏洞 873 个，其中大模型及智能体应用特有漏洞 608 个，传统漏洞 265 个。通报指出，开源大模型和大模型应用典型漏洞风险包括：提示注入类漏洞普遍，仍是大模型最常见漏洞风险；信息泄露类漏洞多发，存在较大安全风险；部分产品存在不当输出处理类漏洞且危害严重。Claw 类智能体应用典型漏洞风险

包括：代理身份与权限滥用类漏洞频发，存在较大安全隐患；代理目标劫持类漏洞隐蔽，可导致非预期高危操作；部分产品存在非预期代码执行类漏洞且危害严重。

应对处置建议方面，通报指出，应针对大模型面临的各类漏洞风险，持续加强安全防护措施；创新智测融合监测预警，打造 AI 漏洞闭环处置体系。（来源：国家互联网应急中心）

8. 江苏省发布《江苏省促进词元经济高质量发展行动方案（2026 年）》

9 月 11 日，江苏省发展改革委、江苏省数据局发布《江苏省促进词元经济高质量发展行动方案（2026 年）》，围绕推动数据资源高质量供给、推进数字基础设施建设、加强算法模型开发应用等八个方面，提出二十六条措施。

推动数据资源高质量供给方面，《行动计划》提出，深化公共数据开发利用。开展公共数据攻坚行动，推进“一本账”管理，深化公共数据“跑起来”行动。推动省基础库共建共用，建设 10 个左右医疗健康、社会保障、生态环保、信用体系、安全生产等重点领域主题库、专题库。加快建设新一代公共数据平台，推进省市平台统筹运营。

加强词元经济治理方面，《行动计划》提出，强化词元经济监管。统筹推进数据安全、内容安全、模型安全、隐私保护和伦理治理。建立分类分级监管机制，对通用对话等低风险场景包容审慎，对金融、

医疗等高价值敏感场景实施重点监管。严厉打击滥用生成式人工智能、词元套利等非法行为。（来源：江苏省发展改革委）

9. 北京市印发《北京市加快词元经济发展的行动方案（2026—2028 年）》

9 月 15 日，北京市经济和信息化局、北京市发展和改革委员会印发《北京市加快词元经济发展的行动方案（2026—2028 年）》，围绕生产供给、评测分发、消费生态等六个方面，提出十项措施。

完善评测分发体系方面，《行动方案》提出，建立词元质量评测体系。支持软件和信息服务业企业与第三方评测机构合作，探索建设词元测试平台，通过模型智能路由、评测咨询等增值服务形成可持续运营模式。建立客观公正的词元性能与质量评测标准，为词元定价、模型智能路由等提供参考依据。

构建行业知识体系方面，《行动方案》提出，探索数据本体技术范式。将高质量数据集及场景信息、合规要求等关键数据知识有机融合创新，形成大模型可使用的数据产品或服务。支持软件和信息服务业企业、工业企业先行先试，将行业知识、工艺参数、设备数据等封装形成数据产品，探索新型数据生产范式、合作机制及商业模式，加速制造业数字化转型与智能化升级，相关成果纳入高质量数据集奖励支持范畴。（来源：北京市经济和信息化局）

10. 北京市印发《北京市人工智能+信息通信“京彩智联”行动计划（2026—2028 年）》

9 月 17 日，北京市通信管理局、北京市经济和信息化局、北京市发展和改革委员会联合印发《北京市人工智能+信息通信“京彩智联”行动计划（2026—2028 年）》。《行动计划》围绕推动信息通信智能化技术演进发展、夯实人工智能发展底座、增强信息通信行业治理能力等四个方面，提出二十二条措施。

推动信息通信智能化技术演进发展方面，《行动计划》提出，加强网络智能体创新发展与应用。支持研发专业性高、落地性强的网络大模型和智能体，突破大小模型协同、智能体通信等技术。打造自主智能体通信协议，深化网络领域的适配与应用，鼓励探索基于智能体的新型电信业务形态，培育网络智能体自主产业生态。面向信息通信领域模型训练和应用需求，在重点场景打造一批信息通信行业高质量数据集。

增强信息通信行业治理能力方面，《行动计划》提出，强化智能化安全保障。围绕信息通信网络高级威胁攻击、数据异常流转等安全风险，加强人工智能赋能网络和数据安全技术攻关。聚焦信息通信网络安全实战和运营典型场景，构建高质量安全数据集，持续开展人工智能赋能网络和数据安全实效评价。强化人工智能评估评测、风险监测、应急处置等安全保障措施，提升风险防范应对水平。（来源：北京市通信管理局）

11. 湖北省印发《湖北省深入实施“人工智能+”三年行动方案（2026-2028 年）》

9 月 20 日，湖北省人民政府办公厅印发《湖北省深入实施“人工智能+”三年行动方案（2026-2028 年）》，提出实施“人工智能＋”六大专项行动、构建全要素保障体系等内容。

构建全要素保障体系方面，《方案》提出，增加高效率算力供给。构建自主可控的全栈式 AI 芯片供给体系，推进武汉人工智能计算中心、三峡东岳庙智算中心等设施建设，加快建设国家算力互联互通区域节点，持续壮大“武、宜、襄·十”三大算力圈。打造全省算力互联互通平台，推动跨域调度，发放“算力券”，降低中小企业用算成本。完善“云边端”算力多元供给，引导算力资源向产业园区下沉，满足工业场景低时延需求。

强化高质量数据支撑，《方案》提出，实施“模数共振”行动，形成“数据—模型—场景应用”良性闭环。推进数据要素市场化配置改革，依托工业门类齐全优势，建设高质量中文语料库及工业、生物医药、工程建造等垂直领域数据集。搭建可信数据空间，推广隐私计算等安全技术，实现数据合规高效流通。（来源：湖北省人民政府）

12. 北京市人民政府印发《“十五五”时期数智北京发展规划》

9 月 27 日，北京市人民政府印发《“十五五”时期数智北京发展规划》，围绕全面促进数据要素高效配置、加强数智技术创新引领、适度超前布局数智基础设施等五个方面，提出十六条措施。

全面促进数据要素高效配置方面，《规划》提出，健全数据制度标准体系。推动数据产权结构性分置制度落地，打造具有公信力的数据产权登记机构，实现重点行业数据产权登记全覆盖，拓展登记凭证多场景应用。完善数据流通交易制度，建立场内场外结合的交易规则体系。按照“谁投入、谁贡献、谁受益”原则，探索数据要素收益分配机制。健全数据安全治理制度，形成数据流通交易责任界定机制。探索面向人工智能的数据合理使用制度和利益补偿机制。推动数据综合性立法。发挥北京市数据标准化技术委员会作用，完善数据标准体系，率先在数据基础设施、数据技术等方面出台系列标准。

营造创新有序的数智发展环境方面，《规划》提出，筑牢数智发展安全底线。切实维护网络安全。健全网络安全态势感知和综合指挥体系，构建威胁感知、分析研判、通报预警、应急处置全链条协同闭环。强化关键信息基础设施安全保护。完善政务信息系统网络安全管理体系，加强政务共性基础设施网络安全防护和容灾备份，做好首都重大活动网络安全服务保障。强化数据安全保障能力。完善数据分类分级保护制度，加强数据收集、存储、传输、共享、交易、销毁等环节安全管理。建立完善重要数据目录，加强安全保护。常态化开展数

据安全风险评估。完善数据流通利用监管沙盒机制，探索建立包容审慎监管方式。加快隐私计算、安全加密等技术研发与应用，鼓励企业面向市场提供安全合规产品和服务。健全个人信息全链条保护机制，实现收集、使用、共享等环节的合规与安全可控。完善人工智能安全治理。推动建立人工智能内容安全监管制度，强化模型算法、数据资源、基础设施、应用系统等安全能力建设，加强智能体应用安全管理。打造人工智能安全测试靶场，开发安全攻防与测试工具箱。持续推进政务大模型应用备案审查、安全评估、保密管理和检查。（来源：北京市人民政府）

13. 江苏省五部门印发《江苏省支持人工智能创新发展有关实施方案的通知》

9 月 30 日，江苏省发展改革委、中共江苏省委网信办、江苏省工业和信息化厅等五部门印发《江苏省支持人工智能创新发展有关实施方案的通知》，并附《江苏省词元（Token）券实施方案》《江苏省语料券实施方案》《江苏省模型券实施方案》。

词元券是指用于企业、高校院所、研究机构及 OPC 等主体购买智能算力服务（含智能算力租赁）进行模型训练、模型推理、智能体应用等的支持资金。支持对象方面，《实施方案》要求用算主体应同时具备以下条件：一是在江苏省境内正常经营的企业、高校院所、研究机构及 OPC 等主体；二是信用记录良好，近三年内无重大违法违规行为，无安全生产事故记录；三是具备明确的算力应用场景规划和

真实的智能算力服务采购需求，购买智能算力服务费用达1万元（含）以上；四是所购买词元服务，其调用的生成式人工智能模型应已通过国家网信办备案。五是与供算主体无关联关系。

语料券是指用于企业、高校院所、研究机构及OPC等主体购买和建设高质量数据集及行业语料资源的支持资金。支持对象方面，《实施方案》提出支持高质量数据集和语料资源购买、高质量数据集与语料库建设以及具身智能机器人数据采集项目。例如，高质量数据集和语料资源购买方应同时具备以下条件：一是在江苏省境内正常经营的企业、高校院所、研究机构及OPC等主体；二是具备明确的人工智能训练、科学研究、技术研发或场景应用需求；三是信用记录良好，近三年内无重大违法违规行为，无安全生产事故记录；四是承诺按约定范围使用语料资源，不擅自复制、转售或超范围传播。

模型券是指对拥有经国家网信办备案的生成式人工智能服务的省内主体，按大模型应用情况和实际研发投入予以支持的资金。支持对象方面，《实施方案》提出，申报主体应同时具备以下条件：一是在江苏省境内正常经营的企业、高校院所、研究机构及OPC等主体；二是信用记录良好，近三年内无重大违法违规行为，无安全生产事故及重大网络、数据安全事件；三是作为备案主体至少拥有1款经国家网信办备案的大模型，有明确的大模型研发、训练、推理、应用推广或服务能力建设计划。（来源：江苏发展改革委员会）

14. 湖北省两部门印发《湖北省算力券实施方案》

9 月 30 日，湖北省数据局、湖北省财政厅印发《湖北省算力券实施方案》，包括资金及来源、支持对象、支持范围、支持标准等。

支持对象方面，《方案》指出，支持企业、事业单位购买并使用经遴选入库的算力服务机构所提供的智能算力、超级算力服务或基于算力的国产人工智能模型服务。算力服务机构由湖北省数据局发文遴选，一年遴选一次，时效 1 年。同一法人单位不得同时拥有用算单位和算力服务机构身份。

支持标准方面，《方案》指出，企事业单位按实际发生费用的 20%予以补贴，其中购买自主可控算力服务的，按实际发生费用的 30%予以补贴，同一主体年度补贴总额最高不超过 300 万元。OPC（一人公司）按实际发生费用的 30%予以补贴，同一主体年度补贴总额最高不超过 10 万元。单个主体年购买算力服务费用 3 万元（含）以上方可申领算力券补贴。（来源：湖北省数据局）

境外前沿观察：月度速览十则

导读：9月，美国、欧盟、英国、澳大利亚等国家和地区围绕网络安全、人工智能安全和数据保护密集发布政策文件、监管措施和安全动态，集中在内部威胁防范、网络安全执法与协作、产品安全事件报告、人工智能风险治理、数据保护以及人工智能应用安全等方面。

一是传统网络安全治理进一步纳入人工智能风险。美国网络安全和基础设施安全局更新《内部威胁缓解指南》，在原有内部威胁治理基础上，新增人工智能和远程办公相关风险内容，强调防范人工智能系统被内部人员攻击、敏感信息因不当使用人工智能工具而泄露，以及远程办公环境下的安全风险。

二是网络安全执法、协作和事件报告机制持续强化。美国联邦调查局发布《网络战略》，明确从打击网络对手、支持受害者、加强伙伴关系和提升自身能力等方面推进网络安全工作。 欧盟《网络弹性法》相关报告义务正式生效，进一步明确数字产品制造商在发现网络安全漏洞和严重安全事件后的分阶段报告责任。

三是人工智能治理更加重视评估、验证和监督。美国总统签署《开启超级智能时代》行政命令，要求联邦行政部门在官方通信、公开声明和政策文件等非法律文件中，以“超级智能”替代“人工智能”表述。美国加州通过行政命令推动研究强化大型前沿模型监管，重点关注独立验证、安全评估和重大安全事件报告等制度安排。美国三部门联合发布《中国人工智能企业针对美国人工智能公司实施工业规模蒸

馏作业》网络安全公告，围绕人工智能模型知识蒸馏问题提出加强异常行为检测、针对性响应和跨组织情报共享等安全建议。英国国家网络安全中心针对“影子人工智能”发出预警，指出未经组织批准使用人工智能工具，可能带来敏感信息泄露、数据失控以及新的攻击入口等风险。美国多家科技企业还签署相关人工智能安全协议，提出加强企业内部管控、外部评估和董事会监督。

四是数据保护和人工智能智能体安全事件继续成为监管重点。爱尔兰数据保护委员会因谷歌位置数据处理问题作出处罚并要求整改，反映出对个人数据合法、透明处理要求的持续强化。 澳大利亚则通报人工智能智能体未经授权访问政府网站事件，并对事件处置和通报问题表达关切。

总体来看，9 月动态反映出网络安全治理正在加快向人工智能系统及其应用场景延伸。监管关注点已不再局限于传统网络和信息系统安全，而是进一步覆盖模型安全、人工智能工具使用、智能体访问、数据保护以及安全事件报告等问题。同时，风险评估、持续监测、独立验证、信息共享和事件报告等传统网络安全治理手段，也正在更多应用到人工智能安全治理中。

关键词：智能体；数据保护；超级智能；用户位置数据

1. 美国 CISA 发布更新版《内部威胁缓解指南》，帮助关键基础设施运营者等主体应对人工智能风险

9 月 9 日，美国网络安全和基础设施安全局（CISA）发布更新版《内部威胁缓解指南》。该指南是对 2020 年 11 月首次发布的同名指南的首次重大更新，旨在适应内部威胁形势的持续变化，帮助关键基础设施所有者与运营者、联邦及州和地方机构、非政府组织、私营部门等各类组织建立或完善内部威胁缓解计划。

此次更新的重点之一，是新增人工智能相关风险及应对内容。指南指出，内部人员可能通过数据投毒、模型篡改等方式攻击人工智能系统，外部行为者可能利用人工智能生成钓鱼信息、虚假用户资料和深度伪造内容操纵内部人员，员工也可能无意中将敏感信息输入未经批准的人工智能系统。组织应培训员工、保护现有人工智能工具、分类敏感数据，并审查更新保障措施。另一更新重点，是回应混合与远程办公带来的挑战。指南指出，员工在办公室以外工作，涉及组织文件和设备物理安全、家庭网络安全、共享驱动器和服务器文件额外存储等问题，组织应更新安全标准、操作程序和专门培训，并确保远程员工与同事、管理人员保持定期互动，以及时发现潜在异常行为。（来源：美国网络安全和基础设施安全局）

2. 美国联邦调查局发布《网络战略》

9 月 9 日，美国联邦调查局（FBI）发布《网络战略》，确立应对网络安全威胁的四大支柱。第一支柱是“调查、破坏并向网络对手施

加成本”，要求 FBI 运用刑事和国家安全权力调查网络入侵，协调国内外伙伴，并整合情报界、外国伙伴、私营部门监测数据和受害者报告，对恶意网络活动进行归因，以识别和削弱对手的人员、基础设施、资金和工具；第二支柱是“支持受害者”，要求 FBI 将证据收集严格限定于犯罪，使用最低侵入性方法，紧急自动共享网络威胁情报，在事件后快速通知受害者和目标实体；第三支柱是“通过伙伴关系增加影响”，要求 FBI 与美政府、外国盟友及私营部门建立持久关系，共享可操作情报并协调行动；第四支柱是“增强 FBI 网络能力”，聚焦招募和留住顶尖网络人才、扩展网络专业知识、实施新技术工具，并借助人工智能提升行动能力。（来源：美国联邦调查局）

3. 欧盟《网络弹性法》报告义务条款正式生效

9 月 11 日，欧盟《网络弹性法》第十四条报告义务条款正式生效，要求数字元素产品的软硬件制造商发现正在被利用的网络安全漏洞或严重安全事件后，通过欧盟统一报告平台（SRP）向相关国家计算机安全事件响应团队（CSIRT）和欧盟网络安全局（ENISA）通报。

报告分为三个阶段。早期预警须在知悉正在被利用漏洞或严重事件后 24 小时内报告，内容包括对恶意意图的初步怀疑及受影响成员国，无需提供完整技术细节，不得因等待详细分析而延迟。详细通报须在知悉后 72 小时内提交，包含初步严重性评估、事件性质及缓解措施，且在提交 24 小时早期预警后 48 小时内完成。漏洞利用场景下，最终报告须在采取纠正或缓解措施后 14 天内提交；对于严重事

件，须在提交详细通报后一个月内提交，包含完整技术分析、根本原因和已采取的纠正措施。（来源：欧盟委员会）

4. 美国加州州长签署人工智能安全行政命令，拟要求大型前沿模型开发商在其实验室阶段定期进行审计和评估

9 月 18 日，美国加利福尼亚州州长签署第 N-9-26 号行政令，旨在落实加州现有的人工智能安全立法，并制定进一步强化监管的路线图，以应对新出现的风险。

根据行政令，加州政府运营局须与州长紧急服务办公室协商，在 2026 年 11 月 16 日前向州长办公室提交建议，内容涉及修改现有州人工智能安全立法的技术可行性和潜在效果，至少包括四项：一是要求所有大型前沿模型开发商在其实验室阶段嵌入指定的独立验证机构，进行定期审计和评估；二是要求前沿人工智能公司提交的安全框架、透明度报告和风险评估由独立验证机构依据其认定为充分标准进行独立验证；三是要求为前沿模型创建“终止开关”，并由独立验证机构持续验证其有效性；四是更新人工智能公司须报告的重大安全事件定义，纳入一系列失控事件，涵盖大型前沿开发商近期报告的事件。（来源：美国加利福尼亚州州长官网）

5. 美国总统签署行政令将人工智能改称超级智能

9 月 29 日，美国总统特朗普签署行政命令《开启超级智能时代》，指示联邦行政部门以“超级智能”（Super Intelligence，SI）替代“人工智能”（Artificial Intelligence，AI）表述。

行政令规定，联邦各部门和机构须在官方通信、公开声明、网站、报告、政策文件及其他非法定文件中使用“超级智能”和“SI”，不再承认“人工智能”和“AI”的使用。行政令明确，不要求修改此前已发布的法规、总统行动、合同、赠款或其他历史文件。在定义方面，行政令暂时将“超级智能”和“SI”界定为美国法典第 15 编第 9401 条第 3 款所定义的“人工智能”所涵盖的技术和系统，该定义适用至被后续总统行动或国会立法取代为止。

行政令要求总统科技助理在 60 天内，与相关机构负责人协商，向总统提交立法建议，以建立“超级智能”和“SI”的联邦定义，反映行政令所述能力。该建议须包括：评估“超级智能”和“SI”的定义应在多大程度上修改、扩展或取代现行“人工智能”的法定定义；对现有法定条款中“人工智能”和“AI”的引用提出相应修订建议；以及为在整个行政部门实施拟议定义所需的额外总统或行政行动建议。（来源：美国白宫）

6. 英国 NCSC 发布博客文章，对影子人工智能隐藏风险发出预警

9 月 7 日，英国国家网络安全中心（NCSC）发布博客文章，就“影子人工智能”（shadow AI）网络安全风险发出预警。影子人工智能是指，未经组织批准而使用的人工智能技术，属于影子信息技术（shadow IT）的一种形式。

文章指出，影子人工智能的使用十分普遍，有研究发现近四分之三的员工报告使用未经雇主批准的人工智能工具。文章列举了影子人工智能带来的主要网络安全风险：第一，敏感信息可能暴露。影子人工智能访问公司或客户数据，可能增加数据泄露、知识产权损失和未能满足监管要求的风险；第二，组织可能失去对数据的可见性和控制。员工将敏感或专有信息转移到消费级人工智能服务，可能降低组织对该信息的可见性和控制，因为这些信息可能被存储、保留或用于改进服务，超出既定的安全和治理安排，除非存在特定隐私控制；第三，为攻击者提供新机会。人工智能智能体可能存在严重安全漏洞。若攻击者成功利用漏洞，即可获得该智能体合法访问的相同数据、服务和权限。攻击者极可能利用防护较松的智能体，来利用更广泛企业信息技术系统中的漏洞或配置错误。（来源：英国国家网络安全中心）

7. 美国指控中国人工智能企业对美国前沿模型开展工业级蒸馏作业

9 月 8 日，美国国家安全局（NSA）、网络安全和基础设施安全局（CISA）与联邦调查局（FBI）联合发布题为《中国人工智能企业针对美国人工智能公司实施工业规模蒸馏作业》的网络安全公告，指控自 2024 年以来，DeepSeek、月之暗面、阿里巴巴、稀宇科技、阶跃星辰以及智普针对 Anthropic 的 Claude、Open 人工智能的 GPT、谷歌的 Gemini 以及 x 人工智能的 Grok 等美国前沿人工智能模型实施系统性、工业级规模的知识蒸馏，以获取美国尖端模型能力。

公告指控中国人工智能大模型公司的蒸馏作业采用了复杂的战术、技术与操作程序（TTPs），包括通过中转站以远低于官方价格转售美国前沿模型访问权限、对大模型注入越狱提示词、系统收集模型输出以生成训练数据、通过多种手段绕过访问限制等。

对此，公告建议美国人工智能公司采取三项措施：一是实施全面检测与处置。检测异常和恶意提示、账号、网络及行为，重点监控订阅量与使用量比例、新账号是否立即达到最大使用量、企业级吞吐模式；二是部署针对性响应方案。对疑似恶意蒸馏请求，隐蔽地改变模型响应，以降低工业化蒸馏活动的收益；三是建立跨组织情报共享。将模型提供商、云平台和第三方 API 聚合平台上的活动进行关联分析，以识别和揭示分布式蒸馏行动。（来源：美国国家安全局）

8. 因违规处理用户位置数据，爱尔兰 DPC 对谷歌处以 4.03 亿欧元罚款

9 月 21 日，爱尔兰数据保护委员会（DPC）宣布，在对谷歌处理用户位置数据的行为完成为期六年的调查后，决定对其处以 4.03 亿欧元罚款，并责令其在六个月内完成整改。

DPC 认定，在 2018 年 5 月 25 日 GDPR 生效至 2020 年 2 月 4 日 DPC 发起调查期间，谷歌在“网络与应用活动记录”“位置历史记录”及安卓系统“位置精确度”三项功能中，未能合法、公平、透明地处理用户位置数据。调查发现，用户可能并不知晓其位置信息正被用于广告投放或推断个人兴趣，且谷歌保存位置数据的时间超过必要期限，进一步加剧用户个人数据失控风险。（来源：爱尔兰数据保护委员会）

9. 澳大利亚总理通报 OpenAI 智能体入侵澳政府网站事件

9 月 23 日，澳大利亚总理举行新闻发布会，通报一起美国 Open AI 的智能体未经授权侵入澳大利亚政府网站的事件，并就人工智能安全、社交媒体监管等议题阐述澳方立场。

总理披露，2026 年 6 月，OpenAI 的一个智能体未经授权接入了澳大利亚政府部门运营的一个医疗保险统计门户网站，访问了公开与非公开文件。目前调查仍在进行中。总理表示，他当日已与 OpenAI 首席执行官通话，表达澳大利亚对此事的极度关切。OpenAI 直到 9 月 10 日才向澳方公共邮箱发出邮件通知，澳方对 OpenAI 通知的延

误和方式感到失望。澳大利亚政府还将向议会相关委员会寻求紧急建议，确认此事是否存在违法行为以及是否应将此事移交澳警方。

9 月 29 日，据法新社、英国《卫报》等媒体报道，OpenAI 就其一个智能体未经授权访问澳大利亚政府网站一事进行道歉，同时承认“本应更早”向澳方通报有关此次安全事件的情况。（来源：澳大利亚总理官网）

10. 美科技巨头签署白宫超级智能安全协议

9 月 29 日，美国总统特朗普在白宫召集美国主要人工智能企业负责人举行闭门午餐会，会后共同签署了一份名为《白宫超级智能协议：前沿责任联合承诺》的协议。

协议属于自愿性质，明确不具有法律约束力，特朗普将其描述为“具有道德约束力”的承诺。协议提出四层控制与审计机制：一是建立内部管控和监测机制，在训练和部署过程中，围绕网络安全、生物安全和化学威胁等领域，监控其模型的能力与对齐情况，并确保其模型不会以非预期的方式入侵或访问技术系统；二是设立内部团队保障相关机制运行，并对现有问题开展整改；三是引入独立外部审查或评估机构，对机制运行进行独立评估；四是由董事会独立委员会负责监督，确保所有已识别问题得到整改。参与企业还将定期会商，研究制定相关标准和行业规范。

签署协议的企业包括 Google、Anthropic、Meta、OpenAI、xAI 以及 NVIDIA。（来源：福布斯新闻网）

行业前沿观察：各地协会动态

9 月，2026 年国家网络安全宣传周在全国统一开展，各成员单位紧扣“智能时代 网安护航”主题，把竞赛、宣讲、培训送进园区、社区和校园等。网络安全宣传周之外，人工智能安全治理成为本月高频议题，论坛、研修班、服务站点密集落地；技能竞赛与人才培养热度不减，个人信息保护、工业互联网安全等赛道相继开赛；标准评审、等保定级等基础工作稳步推进，多单位完成换届、夯实组织根基。以下活动按举办时间排序，不分先后：中关村可信计算产业联盟成功召开《可信计算实训平台框架》等两项团体标准专家评审会；海南省计算机学会主办的海南省首届青少年信息学 AI 编程大赛圆满落幕；苏州市新媒体联合会携手市社会组织总会，为全市社团宣传工作支招赋能；上海市信息网络安全管理协会数智创新系列高级研修班亮相 2026 新耀东方上安会；苏州市互联网协会承办的苏州市网络安全进园区太仓专场活动圆满举行；北京网络空间安全协会助力高校花式开展网络安全宣传教育活动；佛山市信息协会承办“启沅杯”2026 年佛山市工业互联网安全技能竞赛；惠州市计算机信息网络安全协会开展 2026 年网络安全宣传周系列活动；吉林省信息技术应用协会第三届换届会议圆满召开；昆明市网络安全协会联动全省 90 余所高校开展网民网络安全感满意度调查；南通市信息网络安全协会成功承办 2026 年南通市网络安全宣传周法治日主题活动；金华市网商协会成功举办 AIGC 破局增长——电商·短剧内容创作实战分享会；珠海市网络空间安全协会人工智能安全和数据跨境流动工作服务站在斗门揭牌；宁波市计算机信息网络安全

协会顺利召开六届一次会长办公会议暨走进会员单位活动；海南省网络安全和信息化协会开展多领域网络安全专题宣讲活动；汕头市网络空间安全协会承办的鲲城科学大讲堂第五期圆满举办；广东省网络空间安全协会成功举办“智御未来——AI 赋能网络空间安全新范式”论坛；广州网络空间安全协会联合承办的“人工智能安全治理与合规实践”高级研修班成功举办；肇庆市计算机学会协办的 2026 年肇庆市数据知识产权赋能企业宣传培训活动成功举办；上海市信息安全行业协会顺利召开 2026 上海网络安全产业创新推进会；天津市网络空间安全协会顺利召开第二届会员大会第一次会议；西藏自治区互联网协会与西藏自治区通信行业协会联合党支部书记彭坤同志当选西藏自治区互联网行业党委委员；徐州网络公共安防技术协会顺利召开 2026 年徐州市职工 AI+低空无人机应用技术技能竞赛筹备座谈会；湖南省网络空间安全协会顺利开展全省网络系统等级保护定级集中评审工作；

关键词：国家网络安全宣传周；人工智能安全；技能竞赛；人才研修；等级保护；数据跨境流动；换届

1. 中关村可信计算产业联盟成功召开《可信计算实训平台框架》等两项团体标准专家评审会

2026 年9 月 1 日，中关村可信计算产业联盟（以下简称：可信联盟）在北京成功组织召开了《可信计算实训平台框架》及《自主可信计算实训用例设计指南》专家评审会。本次会议严格遵循团体标准制定程序，邀请了三位在可信计算领域及金融标准领域权威专家组成评审委员会，通过专题汇报、现场质询、集中研讨等环节，对《可信计算实训平台框架》及《自主可信计算实训用例设计指南》团体标准的技术可行性、行业适配性及实践落地性进行全面评审。

2. 海南省计算机学会主办的海南省首届青少年信息学 AI 编程大赛圆满落幕

9 月 5 日上午，海南省首届青少年信息学 AI 编程大赛复赛在海口、三亚、澄迈三个市县的五大考点成功举办，并隆重举行了颁奖典礼。本次大赛由海南省计算机学会主办，海口山高高级实验中学、华东师范大学澄迈实验中学、中国人民大学附属中学三亚学校、西南大学三亚中学、北京师范大学海口附属学校、海南解码未来教育科技有限公司共同承办。

3. 苏州市新媒体联合会携手市社会组织总会，为全市社团宣传工作支招赋能

今天（9 月 7 日）下午，由苏州市社会组织总会与苏州市新媒体联合会联合主办的“精研宣传 严守舆情”暨 2026 年第 3 期秘书长下午茶活动，在苏州大数据产业园新媒 e 家圆满举行。活动吸引了全市各行业领域社团秘书长及核心运营人员近 50 人参加，围绕社会组织新媒体宣传运营与舆情风险防范开展深度交流与研讨。

4. 上海市信息网络安全管理协会数智创新系列高级研修班亮相 2026 新耀东方上安会

9 月 10 日，2026 第五届新耀东方上海网络安全博览会暨沿沪宁“人工智能+安全”产业创新发展推进会在上海跨国采购会展中心顺利开幕。本届博览会设置主研讨会与四场分研讨会，吸引近百家企业参展参会，集中展示网络安全与人工智能融合发展的前沿成果。

在上海市信息网络安全管理协会高研班专区，由协会联合上海交通大学终身教育学院共同推出的数智创新系列高级研修班，凭借权威的课程体系与鲜明的实战导向，吸引了许多企业管理者、信息化负责人及网络安全从业者驻足咨询。此前，高研班前三期已顺利结业，往期学员总数 80 余人，并于交大 130 周年校庆时成立了上海交通大学终身教育学院校友会网络安全联谊会。

5. 苏州市互联网协会承办的苏州市网络安全进园区太仓专场活动圆满举行

9 月 10 日，苏州市网络安全进园区太仓专场活动在智汇谷举行。活动以“网安护企 数智同行”为主题，旨在普及网络安全知识，提升企业网络安全防护能力，助力企业数字化转型，为全市数字经济健康发展营造安全、稳定、可信的网络环境。本次活动由苏州市委网信办主办；太仓市委网信办、苏州市互联网协会、太仓市文化教育投资集团有限公司承办；太仓市互联网协会协办。活动现场，太仓全市重点企业代表齐聚一堂，与行业专家面对面、近距离交流。来自数据合规、网络安全等领域多位专家，分别结合法律法规与真实案例，就数据收集存储、客户信息保护、办公系统防护、AI 工具使用安全等园区企业高频关切的话题展开分享，将知识转化为企业“听得懂、用得上”的“实操指南”。

6. 北京网络空间安全协会助力高校花式开展网络安全宣传教育活动

2026 年国家网络安全宣传周暨全国科普月期间，北京网络空间安全协会联动北京理工大学、北京工业大学、中国矿业大学（北京）、首都经济贸易大学、北京信息科技大学、北京政法职业学院、北京科技职业学院、广安职业技术学院等八所高校，共同推进 2026 年网民网络安全感满意度调查活动“网安校园行”系列。活动自 9 月 12 日至 22 日密集落地，形式覆盖专家讲座、嘉年华闯关、“网络安全第

一课”视频、“网安达人”线上知识竞赛、招聘会反诈科普和志愿摊位宣传等，受众从大一新生延伸到教师群体，地域从北京扩展到京外高校。网安联公益讲师团围绕电信诈骗、信息泄露、大模型认知安全等热点授课，志愿服务队以谐音梗互动、集章打卡等轻量化、年轻化方式引导学生参与调查问卷和知识竞赛，实现多校并行、多点覆盖，让网络安全教育真正走进校园、贴近青年。

7. 佛山市信息协会承办“启沅杯”2026 年佛山市工业互联网安全技能竞赛

9 月 14 日，2026 年佛山市网络安全宣传周正式启动。作为网安周的品牌活动之一，“启沅杯”2026 年佛山市工业互联网安全技能竞赛火热开展。目前，赛事已吸引 63 支参赛队伍踊跃报名，并将于 9 月 18 日进行线上 CTF 初赛。本次大赛由佛山市互联网信息办公室、佛山市工业和信息化局、佛山市公安局、佛山市密码管理局联合主办，南海区发展和改革局、佛山市信息协会、广东东软学院共同承办。

8. 惠州市计算机信息网络安全协会开展 2026 年网络安全宣传周系列活动

9 月 14 日至 20 日，以"网络安全为人民，网络安全靠人民——智能时代 网安护航"为主题的 2026 年国家网络安全宣传周在全国范围内统一开展。惠州市计算机信息网络安全协会在各级监管部门的指导下，紧扣宣传周主题，统筹谋划、多点发力，先后走进惠城区、仲恺

高新区、大亚湾经济技术开发区等开展网络安全专题宣讲，并联合惠州市捡跑协会将网络安全宣传送进社区，推动网络安全意识和防护技能深入基层、深入人心，为构筑全民网络安全防线贡献协会力量。

9. 吉林省信息技术应用协会第三届换届会议圆满召开

近日，吉林省信息技术应用协会第三届换届会议在长春隆重召开，来自全省信息技术应用领域的近 80 位代表、嘉宾齐聚一堂，共同见证协会承前启后、继往开来的重要时刻。本次会议严格依照省委社工部、省民政厅及省科协相关要求规范举行，全体与会代表一致通过了选举办法，并选举产生了以王扬同志为理事长的新一届理事会和领导机构，省科协秘书长方艳红现场指导并为新一届领导班子颁发了证书和牌匾，选举王志军同志为监事，为协会持续发挥行业引领作用奠定了坚实组织基础。

10. 昆明市网络安全协会联动全省 90 余所高校开展网民网络安全感满意度调查

2026 年 9 月 15 日，在国家网络安全宣传周校园日期间，昆明市网络安全协会与云南省高等学校计算机教学研究会教育信息化专委会联动全省 90 余所高校同步开展网民网络安全感满意度调查活动，活动广泛发动高校师生参与调查，倾听网民声音，共筑网络安全防线。

11. 南通市信息网络安全协会成功承办2026年南通市网络安全宣传周法治日主题活动

为深入学习贯彻习近平总书记关于网络强国的重要思想，强化人工智能领域的安全法治意识，根据国家网络安全宣传周总体活动部署，9月17日下午，由南通市公安局主办、南通市信息网络安全协会承办的2026年南通市网络安全宣传周法治日主题活动在张謇企业家学院成功举办。

12. 金华市网商协会成功举办AIGC破局增长——电商·短剧内容创作实战分享会

9月17日下午，AIGC破局增长——电商·短剧内容创作实战分享会在菁英园区举办。80余位电商商家、内容创作者、短剧从业者、OPC创业者到场参会。本次活动由金华市网商协会、婺城区人社局主办，菁英园区、金华市数据运营中心、锦程人才等承办，金华市数据资源协会、金华市网络界人士联谊会、金华名橙信息技术有限公司、杭州白露墨穹科技有限公司等协办。

13. 珠海市网络空间安全协会人工智能安全和数据跨境流动工作服务站在斗门揭牌

9月18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，珠海大横琴科技发展有限公司主办的人工智能安全和数据跨境流动工作服务站揭牌仪式暨网络安全宣传周专题活

动在斗门富山综合服务中心举行。本次活动是2026年珠海市网络安全宣传周的重要专题场次。市委网信办相关领导，斗门区委宣传部常务副部长、区委网信办主任梁剑芬，富山工业园管委会四级调研员陈长球等领导、行业专家及企业代表齐聚一堂，共同见证。

14. 宁波市计算机信息网络安全协会顺利召开六届一次会长办公会议暨走进会员单位活动

2026年9月18日，宁波市网络空间安全协会六届一次会长办公会议在浙江德塔森特数据技术有限公司举办。协会会长、副会长、工作委员会主任、秘书长及相关工作人员参加会议，会议由秘书长王晓东主持。与会人员就协会相关事宜进行商讨，并确认新一届的工作安排，本次会议得到德塔森特大力支持，各项议程圆满完成。

15. 海南省网络安全和信息化协会开展多领域网络安全专题宣讲活动

为扎实开展2026年国家网络安全宣传周活动，深入践行“网络安全为人民，网络安全靠人民”理念，切实提升党政机关、重点行业单位网络安全防护和合规履职能力，近日，海南省网络安全和信息化协会组织行业专家分赴全省多地开展上门专题宣讲，精准对接各领域安全需求，开展定制化网络安全培训。

16. 汕头市网络空间安全协会承办的鲲城科学大讲堂第五期圆满举办

恰逢2026年全国科普月与国家网络安全宣传周，为深入普及前沿通信科技知识，夯实全民网络安全意识，助力数字社会安全健康发展，由市科协、市委网信办和市工信局联合主办，市网络空间安全协会承办，中兴通讯、汕头联通企业科协协办的鲲城科学大讲堂第五期“6G前沿技术与网络安全”专场于9月18日在汕头科技馆顺利举办。

17. 广东省网络空间安全协会成功举办“智御未来——AI赋能网络空间安全新范式”论坛

9月20日，2026年岭南科技创新论坛“AI+网络安全”方向重要平行论坛“智御未来——AI赋能网络空间安全新范式”论坛在广州举行。本次论坛由广东省科学技术协会主办，广东省网络空间安全协会承办，广东新兴国家网络安全和信息化发展研究院、广州网络空间安全协会、广东省航空航天学会协办，汇聚了来自政府机关、高等院校、科研院所、医疗卫生、金融、交通、能源电力、信息安全及信息技术服务等领域的专家学者及企业代表，现场座无虚席，共同探讨人工智能时代网络安全面临的机遇与挑战，旨在推动广东网络安全从“被动防御”走向“主动智御”，为数字经济发展筑牢安全底座。

18. 广州网络空间安全协会联合承办的“人工智能安全治理与合规实践”高级研修班成功举办

9 月 20 日至 24 日，按照广东省人力资源和社会保障厅《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，广东省专业技术人才知识更新工程“人工智能安全治理与合规实践”高级研修班在广州成功举办。本期高级研修班旨在提升人工智能领域安全治理能力与合规实践水平，由广东省人力资源和社会保障厅主办，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。来自全省各地的 62 名专业技术人才齐聚羊城，顺利完成各项研修安排。

19. 肇庆市计算机学会协办的 2026 年肇庆市数据知识产权赋能企业宣传培训活动成功举办

9 月 21 日，由肇庆市市场监督管理局（知识产权局）指导，肇庆市知识产权保护中心主办，广东创智知识产权运营服务有限公司承办，鼎湖区市场监督管理局、肇庆市计算机学会、肇庆市信息协会、麗枫酒店(肇庆东站鼎湖山风景区店）协办的 2026 年肇庆市数据知识产权赋能企业宣传培训活动成功举办。来自肇庆国有企业、事业单位、肇湖区旅游发展协会、肇庆民宿协会等分管领导、业务负责人、财务负责人近 50 人参加。

20. 上海市信息安全行业协会顺利召开 2026 上海网络安全产业创新推进会

9 月 22 日，2026 上海网络安全产业创新推进会在上海大华长风华邑酒店顺利召开。本次推进会由上海市信息安全行业协会、上海市网络安全产业示范园联合主办，市经济信息化委总工程师裘薇、普陀区副区长周如意出席推进会。市委网信办、市公安局、市密码局、市通信管理局、国家金融监督管理总局上海监管局等市区部门领导，以及行业专家、重点企业代表共 200 余人出席活动。

21. 天津市网络空间安全协会顺利召开第二届会员大会第一次会议

近日，天津市网络空间安全协会第二届会员大会第一次会议顺利举行，来自全市各领域的 70 余名会员代表参会。会议依据《社会团体登记管理条例》及协会章程开展，有序完成换届各项既定议程，为协会新阶段高质量发展夯实组织基础、凝聚行业合力。

大会期间，全体代表集中审议通过了第一届理事会工作报告、财务工作报告、监事工作报告，全面总结协会过往工作成效，明确新阶段发展思路和重点任务。大会表决通过修订后的《天津市网络空间安全协会章程》《天津市网络空间安全协会会费标准》等制度文件；选举产生了协会第二届理事会理事和监事。

22. 西藏自治区互联网协会与西藏自治区通信行业协会联合党支部书记彭坤同志当选西藏自治区互联网行业党委委员

9 月 29 日，西藏自治区互联网行业党委 2026 年第二次会议在拉萨召开。自治区党委网信办副主任，自治区公安厅党委委员、副厅长，互联网行业党委书记谢祥萍出席会议并作总结讲话。会议由互联网行业党委副书记尼玛片多主持。自治区互联网行业党委委员参会，直属互联网企业、网络社会组织党建工作指导员及相关企业、协会党员职工代表列席会议。

23. 徐州网络公共安防技术协会顺利召开 2026 年徐州市职工 AI+低空无人机应用技术技能竞赛筹备座谈会

为全力做好 2026 年苏鲁豫皖省际交界地区职工职业技能竞赛筹备工作，进一步擦亮区域特色职工技能赛事品牌，9 月 29 日徐州网络公共安防技术协会无人机专业委员会（以下简称“委员会”）在中国移动徐州分公司召开无人机赛项专项筹备座谈会。会议由委员会主任委员、中国移动通信集团江苏有限公司徐州分公司政企客户部经理杨培培主持。

24. 湖南省网络空间安全协会顺利开展全省网络系统等级保护定级集中评审工作

为切实加强全省网络安全等级保护工作规范开展，湖南省网络空间安全协会等保专委会（以下简称“等保专委会”）在前期组建省级

专家库的基础上，正式开展全省网络系统等保定级集中评审工作。

在省公安厅十一总队业务指导下，本月已组织开展4场集中评审工作，共受理来自7个市州的23个网络系统定级评审申请。结合网络运营者自主定级报告，经专家组认真审慎评审，其中2个系统被认定为定级不准，需重新确定保护级别；21个系统通过评审，涉及三级系统6个，二级系统15个。