



网络与数据安全治理

FRONTIERS OF REGULATORY OVERSIGHT IN CYBERSECURITY AND DATA GOVERNANCE

前沿洞察 (月刊)

2025年1月第1期 (总第18期)



2025年1月16日

目 录

境内前沿观察一：安全事件	3
1. 国务院开展第十一次专题学习，关注行政执法规范化水平提升	4
2. 中央网信办召开全国网络辟谣联动机制第二次全体会议 .	5
3. 国家互联网应急中心发现处置两起美国对中国大型科技企业机构网络攻击事件	5
4. 国家数据局举行专题新闻发布会，介绍“关于推动数据产业高质量发展和促进企业数据资源开发利用”相关情况	6
境内前沿观察二：政策立法	8
（一） 国家层面动向	10
1. 国务院审议通过《公共安全视频图像信息系统管理条例（草案）》	10
2. 国务院办公厅印发《关于严格规范涉企行政检查的意见》	10
3. 中共中央办公厅、国务院办公厅发布《关于推进新型城市基础设施建设打造韧性城市的意见》	12
（二） 部委层面动向	13
1. 四部门印发《中小企业数字化赋能专项行动方案（2025—2027年）》	13
2. 三部门印发《制造业企业数字化转型实施指南》	14

3. 市场监管总局发布《网络交易执法协查暂行办法》	14
4. 财政部发布《数据资产全过程管理试点方案》	15
5. 国家数据局等五部门发布《关于促进企业数据资源开发利用的意见》	16
6. 国家金融监督管理总局印发《银行保险机构数据安全管理办法》	17
7. 国家发展改革委等六部门发布《关于促进数据产业高质量发展的指导意见》	18
8. 国家数据局发布《数据领域常用名词解释（第一批）》	19
9. 三部门发布《国家数据基础设施建设指引》	20
10. 全国网安标委发布《网络安全标准实践指南—— 一键停止收集车外数据指引》	21
（三） 地方层面动向	21
1. 广州市政务服务和数据管理局发布《广州市公共数据授权运营管理暂行办法》	21
2. 甘肃省人民政府办公厅（甘肃省数据局）发布《甘肃省公共数据资源登记管理实施细则（试行）》（公开征求意见稿）《甘肃省公共数据资源授权运营管理办法（试行）》（公开征求意见稿）	22
3. 西藏自治区经济和信息化厅发布《西藏自治区公共数据资源开发利用实施方案》	23

4. 浙江省网信办发布《浙江省互联网信息服务安全评估指南》	24
5. 浙江省人大常委会批准《杭州市数据流通交易促进条例》	25
6. 杭州市财政局、数据资源局发布《关于加强杭州市公共数据资产管理的试行意见》	26
7. 黑龙江省人大常委会通过《黑龙江省数字经济促进条例》	27
8. 上海市人民政府办公厅发布《关于人工智能“模塑申城”的实施方案》	27
9. 上海浦东新区人民政府发布《浦东新区公共数据授权运营管理若干规定（试行）》	28
10. 天津市数据局发布《天津市公共数据资源登记管理实施细则（试行）》（征求意见稿）	29
11. 海南省人民政府办公厅发布《海南省国土空间基础数据管理办法》	30
12. 福建省网信办发布《福建省个人信息出境标准合同备案实施办法》	30
13. 贵州省人民政府办公厅印发《贵州省推动人工智能高质量发展行动方案（2025—2027年）》	31
境内前沿观察三：治理实践	33
（一） 公安机关治理实践	35

1. 公安部公布打击整治“网络水军”违法犯罪工作情况：侦破案件 900 余起.....	35
2. 上海警方通报 2024 年打击各类涉网违法犯罪成果：侦破涉网案件 8000 余起.....	35
3. 因数据库存在安全漏洞，浙江台州公安机关对浙江某软件科技公司作出行政处罚.....	37
4. 山东警方破获一起利用制作、安装木马程序等手段盗窃网民游戏账号及虚拟装备案.....	37
5. 山西警方破获一起架设“手机口”实施电信诈骗案.....	39
6. 甘肃警方依法查处一起侵犯公民个人信息案.....	40
7. 上海警方全链条捣毁一个“网络水军”犯罪团伙.....	40
8. 上海警方侦破一起利用共享充电宝侵犯公民个人信息案.....	41
9. 上海黄浦警方破获一起非法获取计算机信息系统数据案.....	44
10. 北京海淀警方发布整治涉网犯罪典型案例.....	44
(二) 网信部门治理实践.....	46
1. 国家网信办集中整治网上金融信息乱象.....	46
2. 中央网信办发布打击网上侵害未成年人合法权益典型案例.....	47
3. 中央网信办举报中心依法受理处置 518 个仿冒诈骗类网站平台.....	49
4. 海南省网信办开展互联网移动应用程序违法违规收集使用个人信息专项治理.....	50

5. 江西南昌网信办依法处置违规从事生成式人工智能服务企业	51
6. 湖南湘潭联动开展医疗行业个人信息权益保护执法检查	51
7. 因存在个人信息泄露风险, 湖南怀化网信办集中约谈 15 家单位	52
8. 因未履行数据安全保护义务, 重庆市网信办对属地公司作出行政处罚	53
9. 因系统页面被篡改为博彩页面, 江西南昌网信办对属地某软件销售公司作出行政处罚	53
(三) 通信管理部门治理实践	54
1. 工信部、多地通信管理局通报侵害用户权益行为 APP	54
2. 湖北省通信管理局组织开展工业领域网络和数据安全风险监测处置专项行动工作	56
3. 上海市通信管理局组织开展 2024 年度云服务安全专项治理工作	57
4. 浙江省通信管理局组织开展 2024 年“数安铸盾”数据安全应急演练	57
5. 青海、贵州、宁夏通信管理局组织开展 2024 年基础电信企业网络与信息安全责任考核年终检查	58
(四) 其他部门治理实践	59

1. 最高检、公安部联合挂牌督办第四批特大跨境电信网络诈骗犯罪案件	59
2. 因违反数据安全管理制度等问题，江苏灌南农村商业银行股份有限公司被处罚	60
境外前沿观察：月度速览十则	61
1. 欧盟《网络弹性法》正式生效	63
2. 韩国国会全体会议通过《旨在构建人工智能发展与信赖基础的人工智能基本法案》	64
3. 联合国通过首个全球打击网络犯罪公约	64
4. 美国总统签署《2025 财年国防授权法》	65
5. 欧盟网络安全局发布《2024 年欧盟网络安全状况报告》	66
6. 美国政府首席信息官办公室发布《2024 影响评估报告》	67
7. 美国 Fortinet 公司发布《2025 年网络威胁趋势预测报告》	68
8. 美国财政部工作站遭遇网络攻击	68
9. 苹果同意支付 9500 万美元和解苹果公司 Siri 窃听诉讼	69
10. 因数据泄露影响约 2900 万 Facebook 账户，爱尔兰对 Meta 处以 2.51 亿欧元罚款	70
行业前沿观察一：倾听 324 万份网民意见心声——2024 “安满周”盛大举办；国家网信办就《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》公开征求意见；《互联网平台企业涉税信息报送规定》向社会公开征求意见	71

1. 倾听 324 万份网民意见心声——2024 “安满周” 盛大举办！发布《2024 年全国网民网络安全感满意度调查统计总报告》等数据成果	72
2. 国家网信办就《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》公开征求意见	75
3. 《互联网平台企业涉税信息报送规定》向社会公开征求意见	81
行业前沿观察二：各地协会动态	84
1. 广东省网络空间安全协会举行信创赋能（第五期）——“信创适配技术交流与推广：共筑数字经济安全基石”活动	85
2. 北京网络空间安全协会召开人工智能专委会（筹）专家咨询会议	85
3. 甘肃省商用密码行业协会捐款 4 万余元驰援西藏抗震救灾	86
4. 重庆信息安全产业技术创新联盟成功举办 2025 年网络安全技术沙龙暨联盟两长工作会议	87
5. 可信联盟基础平台专业委员会召开换届工作会议	87
6. 海南省网络安全和信息化协会与海口市广告协会联合举办网络安全与法律培训活动	88

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

广东关键信息基础设施保护中心

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 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）

林小博 北京网络空间安全协会 秘书长

朱方园 上海市信息安全行业协会 副秘书长

于永丰 辽宁省信息网络安全协会 秘书长

闫东 辽宁省网络安全保障工作联盟 秘书长

孙甲子 黑龙江省网络安全协会 会长

吴文涛 安徽省网络安全协会 秘书长

刘长久 湖北省网络和数据安全协会 副秘书长

邓庭波 湖南省网络空间安全协会 秘书长

林勇忠 广东省网络空间安全协会 党支部书记

冯伟 广西网络安全协会 秘书长

李春报 海南省网络安全和信息化信协会 常务副理事长

戴勇 贵州省网络安全和信息化协会 副理事长

孙大跃 陕西省信息网络安全协会 会长

卢建宙 甘肃省商用密码行业协会 会长

郑方 甘肃烽侦网络安全研究院 院长

李学锋 新疆维吾尔自治区互联网协会 秘书长

胡俊涛 郑州市网络安全协会 秘书长
乔 奇 武汉市网络安全协会 副秘书长
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
邓开旭 成都信息网络安全协会 副秘书长
陈建设 贵阳市信息网络协会 秘书长
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 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
贾辉民 榆林市网络安全协会 会长

编委会委员：（排名不分先后）

黄汝锡 广东关键信息基础设施保护中心 党支部专职副书记
方满意 广东网络空间安全协会副会长
王 嫣 上海市信息网络安全管理协会 部长
贺 锋 广东中证声像资料司法鉴定所 主任
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 胡柯洋
李培刚 薛 波 孙翊伦 林 晴 徐瑞雪

发行部主任：周贵招

发行部：林永健 张 彦 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。

境内前沿观察一：安全事件

导读：12月，国务院以“加快落实行政裁量权基准制度，进一步提升行政执法规范化水平”为主题进行第十一次专题学习。国务院总理李强指出现在一些领域和地方滥用行政裁量权、执法不公正的现象仍然存在。2025年将开展规范涉企执法专项行动，持续优化营商环境，促进稳预期强信心。

国家互联网应急中心发现处置两起美国对中国大型科技企业机构进行网络攻击窃取商业秘密事件。具体来说，中国某先进材料设计研究单位、某智慧能源和数字信息大型高科技企业均疑似被美国情报机构利用安全漏洞植入木马或后门程序，窃取商业秘密信息等数据。

国家数据局举行专题新闻发布会介绍“关于推动数据产业高质量发展和促进企业数据资源开发利用”相关情况。发布会指出，数据产业尚处于发展初期，全国4成数据仅被存储而未使用，数据资源开发利用质效有较大提升空间，数据产业生态还不完善，需尽快破题起势，加快释放数据要素价值潜力。

中央网信办召开全国网络辟谣联动机制第二次全体会议，总结联动机制建立一年多来的工作成效及下一步工作计划。会议表示将把握规律、守正创新、压实责任、狠抓落实。

关键词：行政执法规范化、网络攻击窃密、数据开发利用、网络辟谣

1. 国务院开展第十一次专题学习，关注行政执法规范化水平提升

12月16日，国务院以“加快落实行政裁量权基准制度，进一步提升行政执法规范化水平”为主题进行第十一次专题学习。

国务院总理李强指出，行政执法是政府依法履职、管理经济社会事务的重要方式，推进严格规范公正文明执法是建设法治政府的重要内容。现在一些领域和地方滥用行政裁量权、执法不公正的现象仍然存在。要从群众和企业反映强烈的问题入手，进一步完善行政裁量权基准制度，规范权力运行。针对基准覆盖不全面问题，抓紧完善许可、征收、强制、检查等裁量权基准。针对裁量幅度不合理问题，考虑经营主体违法情况和可承受能力，按照“过罚相当”原则确定处罚限度。针对地方标准不统一问题，加强统筹指导，及时督促调整。

李强指出，2025年要开展规范涉企执法专项行动，持续优化营商环境，促进稳预期强信心。要规范执法程序，全面落实行政执法公示、执法全过程记录、重大执法决定法制审核制度，畅通申诉渠道，依法保障监管对象申诉权利。要优化执法方式，对情节比较轻微、没有主观故意、对社会危害性较低的违法行为，可采取柔性执法措施。要强化执法监督，关注罚没收入异常增长、大量异地执法、大额顶格处罚等情况，审查核实相关执法行为，有问题的要及时纠正。强化信息技术运用，提升执法监督效能。

李强强调，规范行政执法需要常抓不懈，必须坚持问题导向、完善制度规则、强化执行约束，不断提高执法能力水平，切实维护群众和企业的合法权益，维护公平竞争的市场秩序。（来源：国务院）

2. 中央网信办召开全国网络辟谣联动机制第二次全体会议

12月18日，中央网信办召开全国网络辟谣联动机制第二次全体会议。会议总结全国网络辟谣联动机制建立一年多来的工作成效。各单位认真落实全国网络辟谣联动机制部署要求，构建联动辟谣体系，工作格局不断完善；主动回应社会关切，权威辟谣正本清源；积极探索创新举措，难点问题有效解决；广泛凝聚智慧力量，推动网络辟谣工作社会影响日益凸显。

会议强调，网络辟谣是维护网上政治安全和意识形态安全的重要举措，是开展网上群众工作的重要抓手，是深化网络综合治理的重要内容。做好下一步工作，必须把握规律、守正创新、压实责任、狠抓落实。要注重夯基垒台，推进机制高效运转；要强化属地责任，提升谣言应对能力；要压实主体责任，守好网上“第一关口”；要坚持利剑高悬，严处造谣传谣行为；要加强社会参与，筑牢联动辟谣防线。（来源：网信中国）

3. 国家互联网应急中心发现处置两起美国对中国大型科技企业机构网络攻击事件

12月18日消息，国家互联网应急中心近日发现处置两起美国对中国大型科技企业机构进行网络攻击窃取商业秘密事件。

2024年8月起，中国某先进材料设计研究单位遭疑似美国情报机构网络攻击。经分析，攻击者利用中国境内某电子文档安全管理系统漏洞，入侵该公司部署的软件升级管理服务器，通过软件升级服务向该公司的270余台主机投递控制木马，窃取该公司大量商业秘密信息和知识产权。

2023年5月起，中国某智慧能源和数字信息大型高科技企业遭疑似美国情报机构网络攻击。经分析，攻击者使用多个境外跳板，利用微软Exchange漏洞，入侵控制该公司邮件服务器并植入后门程序，持续窃取邮件数据。同时，攻击者又以该邮件服务器为跳板，攻击控制该公司及其下属企业30余台设备，窃取该公司大量商业秘密信息。（来源：国家互联网应急中心）

4. 国家数据局举行专题新闻发布会，介绍“关于推动数据产业高质量发展和促进企业数据资源开发利用”相关情况

12月31日，国家数据局举行专题新闻发布会，介绍“关于推动数据产业高质量发展和促进企业数据资源开发利用”相关情况，重点就国家数据局近日发布的《关于促进数据产业高质量发展的指导意见》《关于促进企业数据资源开发利用的意见》《可信数据空间发展行动计划（2024—2028年）》的背景、主要内容和后续工作安排进行通报。

发布会指出总体而言，数据产业尚处于发展初期，全国4成数据仅被存储而未使用，数据资源开发利用质效有较大提升空间，数据产业生态还不完善，需尽快破题起势，加快释放数据要素价值潜力。国家数据局近日

发布的三份文件的政策主线、主要内容和预期目标总体可概括为“三个紧紧围绕”，一是紧紧围绕经济高质量发展的政策目标，二是紧紧围绕数据要素市场化配置改革的工作主线，三是紧紧围绕企业关切诉求和市场期盼。

在培育多元化数据企业方面，国家数据局有关同志应记者提问表示，数据企业是推动数据产业高质量发展的关键主体。根据数据产业的业务形态将数据企业分为数据资源、数据技术、数据服务、数据应用、数据安全和数据基础设施企业等六类。国家数据局将会同有关部门创新支持政策，建立数据企业培育库，支持数据企业做强做优做大，推动构建大中小企业融通发展、产业链上下游协同创新的产业生态体系。

在数据出境管理方面，中央网信办有关同志应记者提问表示，国家网信办会同相关部门依法依规开展数据出境安全评估和个人信息出境标准合同备案工作。截至2024年12月，国家网信办共完成安全评估项目285个，个人信息出境标准合同备案1071个。其中安全评估项目未通过评估的27个，占整体比例不到10%。除个别项目因重要数据出境必要性不足或存在安全风险未通过评估，其余大多数未通过的主要原因是数据处理者未按照法律规定征得个人信息主体同意。《促进和规范数据跨境流动规定》出台后，数据出境安全评估项目数量同比下降约60%，个人信息出境标准合同备案数量同比下降约50%。（来源：国家数据局）

境内前沿观察二：政策立法

导读：12月，数据资源开发利用和数据产业发展、公共数据授权运营仍是国家部委和地方政策立法的关注重点，凸显重要地位。同时，视频图像信息系统管理、行政执法规范化相关制度文件也取得重要进展。

视频图像信息系统管理方面。行政法规《公共安全视频图像信息系统管理条例（草案）》经国务院常务会议审议通过，旨在规范公共安全视频系统建设和使用，更好维护公共安全、保护个人隐私。

行政执法规范化方面。国务院办公厅印发《关于严格规范涉企行政检查的意见》，指出行政检查是行政执法主体履行行政管理职责的重要方式，对引导规范企业合法经营、预防纠正违法行为具有重要作用。意见围绕明确行政检查主体，严禁不具备主体资格的组织实施行政检查；清理并公布行政检查事项，从源头上遏制乱检查等方面提出十项具体要求。市场监管总局发布《网络交易执法协查暂行办法》，指出市场监督管理部门开展网络交易执法协查工作，应当遵循合法、合理、高效原则，向平台经营者调取的信息应当遵循“必要且适当”原则，不得超出履行法定职责所必需的范围和限度。

数据资源开发利用方面。从中央到地方，各级部门重视数据安全的管理规制，发布相关政策文件。五部门发布《关于促进企业数据资源开发利用的意见》，围绕健全企业数据权益实现机制、培育企业数字化竞争力、营造开放透明可预期的发展环境等提出十三项要求。六部门发布《关于促

进数据产业高质量发展的指导意见》，围绕加强数据产业规划布局、培育多元经营主体、加快数据技术创新等方面提出九项意见。

同时，国家金融监督管理总局印发《银行保险机构数据安全管理办法》，强化数据治理顶层设计、落实分类分级管理要求、强化数据安全管理体系、加强个人信息保护、完善风险监测处置机制。财政部发布《数据资产全过程管理试点方案》，提出在有关中央部门、中央企业、地方财政部门，围绕数据资产台账编制、登记、授权运营、收益分配、交易流通等重点环节，开展数据资产全过程管理试点。

地方层面围绕公共数据授权运营制度建设取得多项进展。广东省广州市、西藏自治区、上海浦东新区先后发布《广州市公共数据授权运营管理暂行办法》《西藏自治区公共数据资源开发利用实施方案》《浦东新区公共数据授权运营管理若干规定（试行）》；甘肃、天津也聚焦公共数据资源登记等环节发布相关征求意见稿，推动本地区公共数据资源开发利用。

此外，浙江省网信办发布《浙江省互联网信息服务安全评估指南》，指导浙江省内企业开展互联网新技术新应用安全评估、区块链信息服务备案、互联网信息服务算法备案、生成式人工智能（大语言模型）上线备案。福建省发布《福建省个人信息出境标准合同备案实施办法》，指导和帮助个人信息处理者规范备案个人信息出境标准合同。

关键词：数据资源开发、公共数据、视频图像信息系统管理、行政检查执法规范化

（一）国家层面动向

1. 国务院审议通过《公共安全视频图像信息系统管理条例(草案)》

12月16日，国务院总理李强主持召开国务院常务会议，会议审议通过《公共安全视频图像信息系统管理条例（草案）》，指出要规范公共安全视频系统建设和使用，更好维护公共安全、保护个人隐私。

目前，草案正文尚未公布，根据4月发布的《公共场所视频图像信息系统管理条例（征求意见稿）》，条例所称“公共场所视频图像信息系统”是指通过安装图像采集设备及相关设施，对公共场所进行视频图像信息收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动的系统。

（来源：司法部、公安部）

2. 国务院办公厅印发《关于严格规范涉企行政检查的意见》

12月30日，国务院办公厅印发《关于严格规范涉企行政检查的意见》。意见指出，行政检查是行政执法主体履行行政管理职责的重要方式，对引导规范企业合法经营、预防纠正违法行为具有重要作用。意见提出十项具体要求，包括：明确行政检查主体，严禁不具备主体资格的组织实施行政检查；清理并公布行政检查事项，从源头上遏制乱检查；合理确定行政检查方式，最大限度减少入企检查频次；严格行政检查标准、程序，杜绝随意检查等内容。

意见指出，要明确行政检查主体，严禁不具备主体资格的组织实施行政检查。实施行政检查的主体必须具备法定资格。具有行政执法权的行政机关必须在法定职责范围内实施行政检查；法律、法规授权的具有管理公共事务职能的组织必须在法定授权范围内实施行政检查；受委托组织必须在委托范围内实施行政检查。除上述主体外，任何组织和个人不得实施行政检查。行政检查主体资格要依法确认并向社会公告。严禁政府议事协调机构以各种名义实施行政检查；严禁检验检测机构、科研院所等第三方实施行政检查；严禁外包给中介机构实施行政检查；严禁未取得执法证件的执法辅助人员、网格员、临时工等人员实施行政检查。

意见强调，要规范行政检查行为，防止逐利检查、任性检查。涉企行政检查要做到“五个严禁”、“八个不得”。严禁逐利检查，不得接受被检查企业的任何馈赠、报酬、福利待遇，不得参加被检查企业提供的宴请、娱乐、旅游等活动，不得由被检查企业支付消费开支或者将检查费用转嫁给企业，不得强制企业接受指定的中介机构提供服务。严禁干扰企业正常生产经营，不得刻意要求法定代表人到场。严禁任性处罚企业，不得乱查封、乱扣押、乱冻结、动辄责令停产停业。严禁下达检查指标，不得将考核考评、预算项目绩效与检查频次、罚款数额挂钩。严禁变相检查，不得以观摩、督导、考察等名义行检查之实。（来源：国务院）

3. 中共中央办公厅、国务院办公厅发布《关于推进新型城市基础设施建设打造韧性城市的意见》

12月5日，中共中央办公厅、国务院办公厅发布《关于推进新型城市基础设施建设打造韧性城市的意见》，旨在深化城市安全韧性提升行动，推进数字化、网络化、智能化新型城市基础设施建设，打造承受适应能力强、恢复速度快的韧性城市，增强城市风险防控和治理能力。

意见共提出十一项重点任务，包括实施智能化市政基础设施建设和改造、推动智慧城市基础设施与智能网联汽车协同发展、发展智慧住区、提升房屋建筑管理智慧化水平、开展数字家庭建设、推动智能建造与建筑工业化协同发展、保障网络和数据安全等内容。

保障网络和数据安全方面，意见提出，要严格落实网络和数据安全法律法规和政策标准，强化信息基础设施、传感设备和智慧应用安全管控，推进安全可控技术和产品应用，加强对重要数据资源的安全保障。强化网络枢纽、数据中心等信息基础设施抗毁韧性，建立健全网络和数据安全应急体系，加强网络和数据安全监测、通报预警和信息共享，全面提高新型城市基础设施安全风险抵御能力。（来源：新华社）

（二）部委层面动向

1. 四部门印发《中小企业数字化赋能专项行动方案（2025—2027年）》

12月12日，工信部、财政部、中国人民银行、金融监管总局印发《中小企业数字化赋能专项行动方案（2025—2027年）》，围绕深入实施“百城”试点、分类梯次开展数字化改造、推进链群融通转型、推动人工智能创新赋能等七方面提出十八项重点任务。

推动人工智能创新赋能方面，方案提出发布中小企业人工智能应用指引、加强中小企业人工智能应用推广、强化中小企业人工智能应用基础三项重点任务。其中，将编制发布中小企业与人工智能融合应用推进指南，明确中小企业人工智能应用实施的主要模式、典型路径，为中小企业提供可落地、易操作的参考指引。

提高数字化转型公共服务能力方面，方案将构建中小企业数字化转型标准体系、完善中小企业数字化转型服务载体、全面增强中小企业数据与网络安全防护能力。其中，将引导中小企业建立健全网络和数据安全管理制度，促进态势感知、工业防火墙、入侵检测系统等安全产品部署应用。支持中小企业开展网络和数据安全演练，提升中小企业网络风险防御和处置能力。鼓励中小企业通过购买网络安全保险等方式降低安全风险。（来源：工信部）

2. 三部门印发《制造业企业数字化转型实施指南》

12月17日，工信部、国务院国有资产监督管理委员会、中华全国工商业联合会印发《制造业企业数字化转型实施指南》。指南提出分四步推动制造业企业数字化转型：一是制定转型规划，二是组织落地实施，三是开展成效评估，四是推进迭代优化。指南进一步提出，要聚焦场景突破，强化分类推进，强化政策保障。

其中，指南要求加强安全保障。健全工业企业网络安全管理制度，深入实施工业互联网安全分类分级管理，建立健全定级防护、评估评测、监测预警、信息通报、成效评价等工作机制，指导企业落实《工业控制系统网络安全防护指南》相关要求，开展重要工业控制系统识别认定，构建工控安全评估体系。督促企业落实《数据安全法》《工业和信息化领域数据安全管理办法（试行）》等法律政策要求，加强重要数据识别与备案，做好数据分类分级保护和安全风险评估，强化风险监测预警和应急处置能力，切实提升工业数据安全防护水平。（来源：工信部）

3. 市场监管总局发布《网络交易执法协查暂行办法》

12月18日，市场监管总局发布《网络交易执法协查暂行办法》，自2025年1月20日起施行。

办法共十八条，明确“执法协查”是指市场监督管理部门开展案件调查、事故处置、缺陷消费品召回、消费争议处理等执法活动时，依法要求网络交易平台经营者提供有关平台内经营者信息及相关交易信息，对协查

事项进行核实确认并回复结果，协助市场监督管理部门开展执法工作的行为或活动。

办法要求，市场监督管理部门开展网络交易执法协查工作，应当遵循合法、合理、高效原则，向平台经营者调取的信息应当遵循“必要且适当”原则，不得超出履行法定职责所必需的范围和限度。

办法明确，县级以上市场监督管理部门在执法过程中，根据工作需要，可以依法要求平台经营者协助调查。涉及特定时段、特定品类、特定区域的商品或者服务的价格、销量、销售额等数据信息，由国家市场监督管理总局及其授权的省级市场监督管理部门要求平台经营者协助提供。平台经营者应当在收到市场监督管理部门限期提供信息通知书之日起，十五个工作日内完成协查工作并复函。（来源：市场监管总局）

4. 财政部发布《数据资产全过程管理试点方案》

12月19日，财政部发布《数据资产全过程管理试点方案》，提出在有关中央部门、中央企业、地方财政部门，围绕数据资产台账编制、登记、授权运营、收益分配、交易流通等重点环节，开展数据资产全过程管理试点，规范数据资产管理流程，形成数据资产管理全过程工作指引，打造数据资产应用标杆和典型案例，为后续完善数据资产管理制度，加强数据资产管理积累经验。试点时间为2025年1月1日至2026年12月31日。

编制数据资产台账方面，方案要求基于数据资源目录，加强数据资源汇集、治理，提升数据资源质量，按照数据资产定义，组织梳理试点单位

符合数据资产范围和确认条件的数据资源，形成规范化的数据资产管理台账，摸清数据资产底数。

完善授权运营机制方面，方案要求建立并完善数据资产授权运营管理制度和工作机制，明确授权运营条件，确保具备相应条件的主体，依法合规开展授权运营工作。公共数据资产对外授权运营，要严格按照资产管理权限，探索规范的资产使用和处置审批程序。结合实际探索采取整体授权、分领域授权、依场景授权等不同模式，开展数据资产的使用权和经营权授权。强化授权运营事中事后监管，建立定期评估和动态调整机制，根据市场运营效果，调整或收回授权运营事项。（来源：财政局）

5. 国家数据局等五部门发布《关于促进企业数据资源开发利用的意见》

12月20日，国家数据局、中央网信办、工信部等五部门发布《关于促进企业数据资源开发利用的意见》，围绕健全企业数据权益实现机制、培育企业数字化竞争力、营造开放透明可预期的发展环境等提出十三项要求。

培育企业数字化竞争力方面，意见提出，要提高数据治理能力。鼓励企业建立首席数据官制度，健全数据资源管理机制。推动数据管理相关国家标准贯标，规范开展数据治理能力评估，强化企业数据治理和质量管理能力建设。大力推广云计算、边缘计算、大数据分析等平台服务，支持企业开发和使用智能化工具，建立覆盖研发、生产、销售、服务、管理等各环节的数据资源体系。落实国家数据分类分级和个人信息保护政策法规要求，在防范实质性风险前提下，鼓励企业针对不同敏感级别的数据和数据

处理场景，采取差异化的数据安全与合规管理措施，优化对同类型数据处理行为的内部合规审批流程，加强数据流转分析和风险监测。鼓励企业采用可信数据空间、区块链、隐私计算、匿名化等技术模式，促进数据安全流动和开发利用。

营造开放透明可预期的发展环境方面，意见提出，要提升数据安全合规治理效能。完善数据联管联治机制，强化部门协调和央地协同，推动包容审慎监管。针对新技术应用和新模式新业态，探索建立“沙盒监管”机制，构建鼓励创新、弹性包容的治理环境。健全政企沟通机制，稳定企业合规预期。推动制定行业数据分类分级标准，健全数据资源开发利用安全技术规范。健全数据安全管理体系、个人信息保护认证制度。强化行业自律建设，营造公平竞争、规范有序的市场环境。（来源：国家数据局）

6. 国家金融监督管理总局印发《银行保险机构数据安全管理办法》

12月27日，国家金融监督管理总局印发《银行保险机构数据安全管理办法》，自公布之日起施行。办法共九章八十一条，包括数据安全治理、数据分类分级、数据安全管理体系等内容。

办法主要包括以下内容：（1）强化数据治理顶层设计。要求银行保险机构建立与业务发展目标相适应的数据安全治理体系，落实数据安全责任制，按照“谁管业务、谁管业务数据、谁管数据安全”的原则开展数据安全保护工作；（2）落实分类分级管理要求。要求对业务经营管理过程中获取、产生的数据进行分类管理。根据数据的重要性和敏感程度，将数据分为核心、重要、一般三个级别，并将一般数据进一步细分为敏感数据和其

他一般数据，并采取差异化的安全保护措施；（3）强化数据安全管理体系。要求银行保险机构建立健全数据安全管理制度，对委托处理、共同处理、转移、公开、共享等相关数据处理活动开展安全评估，采取相应技术手段保障数据全生命周期安全，保障数据开发利用活动安全稳健开展；（4）加强个人信息保护。按照“明确告知、授权同意”的原则处理个人信息，按照金融业务处理目的的最小范围收集个人信息。共享和向外部提供个人信息，应履行个人告知及取得同意的义务；（5）完善风险监测处置机制。将数据安全风险纳入全面风险管理体系，明确数据安全风险监测、风险评估、应急响应及报告、事件处置的组织架构和管理流程，有效防范和处置数据安全风险。（来源：国家金融监督管理总局、中国政府网）

7. 国家发展改革委等六部门发布《关于促进数据产业高质量发展的指导意见》

12月28日，国家发展改革委、国家数据局、教育部等六部门发布《关于促进数据产业高质量发展的指导意见》。

意见指出，数据产业是利用现代信息技术对数据资源进行产品或服务开发，并推动其流通应用所形成的新兴产业，包括数据采集汇聚、计算存储、流通交易、开发利用、安全治理和数据基础设施建设等。意见围绕加强数据产业规划布局、培育多元经营主体、加快数据技术创新、提高数据领域动态安全保障能力等方面提出九项意见。

提高数据领域动态安全保障能力方面，意见要求创新数据安全产品服务、加强动态数据安全保障。其中，要推动基础设施安全、数据安全、应

用安全协同发展，加强身份认证、数据加密、安全传输、合规检测等技术创新，培育壮大适应数据流通特征和人工智能应用的安全服务业态。建立健全数据安全风险识别、监测预警、应急处置等相关规范，落实数据流通利用全过程相关主体的安全责任。健全数据分类分级标准，加强对涉及国家安全、商业秘密、个人隐私等数据的保护。

发展数据流通交易方面，意见要求促进数据合规流通交易、大力发展第三方服务。其中，要建立健全数据交易规则，鼓励探索多元化数据流通交易方式，优化数据交易机构布局，支持数据交易机构、数据流通交易平台互认互通。支持企业贴近市场需求，开发数据产品和服务，实现数据合规高效流通。构建数据跨境便利化服务体系，强化数据跨境相关基础设施建设和互联互通，推动数据跨境安全有序流动。（来源：国家发展改革委）

8. 国家数据局发布《数据领域常用名词解释（第一批）》

12月30日，国家数据局数据领域名词解释起草专家组发布《数据领域常用名词解释（第一批）》。本次发布的名词解释与此前10月份的征求意见稿相比，保留征求意见稿大部分内容，对个别名词进行删改，主要有：

（1）将数据交互名词删除；（2）将数据资源的定义修改为“具有价值创造潜力的数据的总称，通常指以电子化形式记录和保存、可机器读取、可供社会化再利用的数据集合”；（3）将数据要素的定义修改为“投入到生产经营活动、参与价值创造的数据资源”；（4）将元数据的定义修改为“定义和描述特定数据的数据，它提供了关于数据的结构、特征和关系的信息，有助于组织、查找、理解、管理数据”；（5）将数据分析的定义修改为“通

过特定的技术和方法，对数据进行整理、研究、推理和概括总结，从数据中提取有用信息、发现规律、形成结论的过程”；（6）将数据挖掘的定义修改为“是数据分析的一种手段，是通过统计分析、机器学习、模式识别、专家系统等技术，挖掘出隐藏在数据中的信息或者价值的过程”；（7）将区块链的定义修改为“是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，具有多中心化、共识可信、不可篡改、可追溯等特性，主要用于解决数据流通过程中的信任和安全问题”。（来源：国家数据局）

9. 三部门发布《国家数据基础设施建设指引》

12月31日，国家发展改革委、国家数据局、工信部发布《国家数据基础设施建设指引》。指引提出数字基础设施基本内涵，明确建设数字基础设施的目标和推进路径。同时，指引就国家数据基础设施的总体功能、总体框架、重点建设方向、算力建设、安全防护等方面提出具体意见。

安全防护方面，指引提出构建多层次、全方位、立体化的国家数据基础设施安全保障框架。贯穿数据生命周期全流程，帮助各参与方提升数据安全保障能力，确保数据的可信性、完整性和安全性。

其中，国家数据基础设施安全保障层面，实现可信接入、安全互联、跨域管控和全栈防护等安全管理，建立网络安全风险和威胁的动态发现、实时告警、全面分析、协同处置、跨域追溯和态势掌控能力，提供应对芯片、软件、硬件、协议等内置后门、漏洞安全威胁的内生防护能力。加强对合作伙伴、运维人员、平台用户等数据安全内部风险的防范应对。加强

对入侵渗透、拒绝服务、数据窃取、勒索投毒等外部威胁的应急响应。（来源：国家发展改革委）

10. 全国网安标委发布《网络安全标准实践指南—— 一键停止收集车外数据指引》

12月19日，全国网安标委发布《网络安全标准实践指南 —— 一键停止收集车外数据指引》。指引对装有车载摄像头、雷达等传感器的智能网联汽车上设置一键停止收集车外数据功能提出具体建议。

指引适用于汽车制造企业、自动驾驶研发企业以及相关零部件或服务提供商设计、研发、制造具有车外数据收集功能的智能网联汽车（不包括主驾无人的高级别自动驾驶汽车）；也适用于重要敏感区域的管理机构对进入该区域内汽车的数据收集状态进行判断；还可为第三方测评机构开展智能网联汽车车外数据停止收集功能的有效性和安全性测试评估提供参考。

（来源：全国网络安全标准化技术委员会）

（三）地方层面动向

1. 广州市政务服务和数据管理局发布《广州市公共数据授权运营管理暂行办法》

12月6日，广州市政务服务和数据管理局发布《广州市公共数据授权运营管理暂行办法》，自印发之日起施行，有效期三年。暂行办法共八章三十九条，包括职责分工、数据供给、运营管理等内容。

办法规定，公共数据授权运营是指参与本市公共数据运营工作的企事业单位（以下简称公共数据运营机构）按照法律法规和相关要求获得市人民政府授权后，面向数据商公平提供服务，对公共数据进行加工使用，为数据商提供安全可信的数据开发利用环境，以及数据商开发利用形成公共数据产品和服务并向社会提供使用的行为。

办法提出，市公共数据主管部门联合数源部门、区公共数据主管部门、市政务大数据管理机构、公共数据运营机构建立公共数据授权运营全流程可追溯的安全监管体系，建立网络安全、数据安全、个人信息保护、商业秘密保护的协同监管机制。公共数据授权运营过程中落实“谁管理谁负责、谁使用谁负责”的数据安全责任制。定期开展风险评估，排查可能影响网络安全、数据安全、个人信息保护、商业秘密保护等关键监管点的风险隐患。排查中发现有影响数据安全的行为，市公共数据主管部门有权暂停向公共数据运营平台提供公共数据，并待问题整改完成后，重新恢复提供公共数据。（来源：广州市政务服务和数据管理局）

2. 甘肃省人民政府办公厅（甘肃省数据局）发布《甘肃省公共数据资源登记管理实施细则（试行）》（公开征求意见稿）《甘肃省公共数据资源授权运营管理办法（试行）》（公开征求意见稿）

12月10日，甘肃省人民政府办公厅（甘肃省数据局）发布《甘肃省公共数据资源登记管理实施细则（试行）》（公开征求意见稿）《甘肃省公共数据资源授权运营管理办法（试行）》（公开征求意见稿）。

《甘肃省公共数据资源登记管理实施细则（试行）》（公开征求意见稿）共十一章四十七条，包括登记内容、管理机构、登记机构、登记主体等内容。征求意见稿规定，登记内容主要包括数据基本信息、委托代理信息、数据存储信息、数据应用场景说明、数据共享开放信息、共有数据信息、数据合法合规性来源及承诺、数据目录信息等。征求意见稿强调，自然人、法人或非法人组织对公示中或登记后的登记信息有异议的，应实名提出异议，并提供真实、必要的证明材料。

《甘肃省公共数据资源授权运营管理办法（试行）》（公开征求意见稿）共六章四十三条，包括工作机制、授权管理、运营实施等内容。征求意见稿规定，公共数据资源授权运营模式包括整体授权、分领域授权或依场景授权等。县级以上地方各级人民政府结合本地实际确定公共数据资源授权运营模式。（来源：甘肃省人民政府）

3. 西藏自治区经济和信息化厅发布《西藏自治区公共数据资源开发利用实施方案》

12月16日，西藏自治区经济和信息化厅发布《西藏自治区公共数据资源开发利用实施方案》，提出九项工作任务，包括建立健全制度规范体系、规范公共数据授权运营、加强数据安全等内容。

建立健全制度规范体系方面，方案提出，要建立健全西藏自治区公共数据资源流通共享、开发利用实施完善的配套规范制度和体系建设，制定相关政策、法规和技术保障措施，确保公共数据资源流通共享、开发利用过程中的合法性、安全性和可持续性，明确数据流通共享、开发利用过程

中数据流向、使用主体、调用频次等基本要素，并建立监督管理审核机制。制定数据传输技术通道建设规范，明确跨部门、跨网络数据传输技术通道的部署要求、功能要求、性能要求和安全要求，全力推动数据全生命周期高质量建设发展。

加强数据安全方面，方案提出，要加强数据全生命周期安全管理，强化数据安全和个人信息保护，加强对数据资源生产、加工使用、产品经营等开发利用全过程的监督和管理，确保数据资源安全运行管理边界清晰、职责明确、落实到位。建立健全数据安全信息共享、应急响应处置机制。指导督促运营机构履行数据安全主体责任，采取加密、备份、访问控制、安全认证等技术措施，加强动态监控、主动防御，形成数据安全规范管理闭环，提升安全防护水平。在公共数据开放平台等数据基础设施建设中落实商用密码“三同步一评估”要求，加强数据资源在产生、流通、存储、利用等各环节密码防护，推动数据交易过程商用密码应用。依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场。（来源：西藏自治区经济和信息化厅）

4. 浙江省网信办发布《浙江省互联网信息服务安全评估指南》

12月18日，浙江省网信办发布《浙江省互联网信息服务安全评估指南》，指导浙江省内企业开展互联网新技术新应用安全评估、区块链信息服务备案、互联网信息服务算法备案、生成式人工智能（大语言模型）上线备案。

其中，生成式人工智能（大语言模型）上线备案方面，指南指导浙江省内企业三步走：一是确定适用范围。互联网信息服务提供者利用生成式

人工智能（大语言模型）技术面向公众提供信息服务的，且具有舆论属性和社会动员能力的，需进行生成式人工智能（大语言模型）上线备案；二是填写备案材料。互联网信息服务提供者在提供服务之前通过省网信办领取《生成式人工智能（大语言模型）上线备案表》，按照《备案表》所列项目，填写生成式人工智能服务的基本情况、模型研制、服务与安全防范、安全评估等情况，并附相关附件材料和证明材料等；三是提交申报材料。整理完成申报材料后，线下向浙江省互联网信息办公室提交备案材料。（来源：网信浙江）

5. 浙江省人大常委会批准《杭州市数据流通交易促进条例》

12月19日，浙江省第十四届人民代表大会常务委员会第十四次会议批准《杭州市数据流通交易促进条例》，自2025年3月1日起施行。条例共六章三十七条，包括数据权益、数据开放与授权、数据要素市场培育、保障措施等内容。

条例规定，杭州市建立公共数据授权运营机制，对不承载个人信息、不影响公共安全、法律法规未禁止开放的公共数据加大供给力度，提高公共数据社会化开发利用水平。开展授权运营活动，不得滥用行政权力或者市场支配地位排除、限制竞争，不得利用数据和算法、技术、资本优势等从事垄断行为。依法获得公共数据运营权的市场主体加工公共数据形成的数据产品、数据服务，应当按照国家和省有关数据要素市场规则流通交易。

条例强调，对承载个人信息的数据，数据处理者应当按照个人授权范围依法规范开展个人信息处理活动，不得采取“一揽子授权”、强制同意

等方式过度收集个人信息，不得擅自变更授权范围。法律、行政法规另有规定的，从其规定。鼓励市场主体提供个人数据代理服务，受托管理个人数据，监督个人数据处理行为，记录和汇总个人数据使用情况，代为主张个人数据权益。（来源：杭州网）

6. 杭州市财政局、数据资源局发布《关于加强杭州市公共数据资产管理的试行意见》

12月26日，杭州市财政局、杭州市数据资源局发布《关于加强杭州市公共数据资产管理的试行意见》，自2025年2月1日开始施行。意见共提出十二项要求，包括明确公共数据资产范围、推进公共数据资产登记和入表、加强公共数据资产使用管理、推动公共数据资产开发利用等内容。

加强公共数据资产使用管理方面，意见提出，公共管理和服务机构应明确管理责任，推进公共数据资产安全有效使用。公共管理和服务机构应依据《数据安全法》等规定，做好公共数据资产加工处理工作，提高公共数据资产质量和管理水平。结合数据采集加工周期和安全等级等实际情况及要求，对公共数据资产定期更新维护。在确保公共安全和保护个人信息的前提下，积极推动公共数据资产开放共享，充分释放公共数据资产价值。

加强公共数据资产安全和监督管理方面，意见提出，按照分类分级管理要求，公共管理和服务机构应建立健全公共数据资产管理内控制度，加强对公共数据资源生产、加工使用、产品经营等开发利用全过程的监督管理，采取适当安全防护技术措施，规范实施资产评估，严防虚增公共数据资产价值，落实安全审查、风险评估、资产评估、监测预警等管理机制。

依法依规予以保密的数据资产不予开放。自觉接受人大监督、审计监督、财会监督等各类监督，确保数据资产安全完整。（来源：杭州市人民政府）

7. 黑龙江省人大常委会通过《黑龙江省数字经济促进条例》

12月19日，黑龙江省第十四届人民代表大会常务委员会第十九次会议通过《黑龙江省数字经济促进条例》，自2025年3月1日起施行。条例共七章八十六条，包括数字经济发展支撑、数字产业化、数字化治理等内容。

条例强调，县级以上人民政府应当加强数字政府建设，推进政府履职和政务运行数字化转型，推动数字技术在经济调节、市场监管、社会治理、公共服务、生态环境保护、政府自身运行等领域的应用，建设以数据要素驱动、数字智能技术支撑、数字网络覆盖的现代化数字政府体系。

条例规定，县级以上人民政府及有关部门和处理数据的主体应当履行有关数字经济发展的安全责任，加强重要领域数据资源、重要网络、信息系统和硬件设备安全保障，建立健全安全管理制度和安全风险评估、报告、信息共享、监测预警、应急处置机制，采取必要安全措施，保护数据、网络、设施等方面的安全。（来源：黑龙江省人民政府）

8. 上海市人民政府办公厅发布《关于人工智能“模塑申城”的实施方案》

12月20日，上海市人民政府办公厅发布《关于人工智能“模塑申城”的实施方案》，共提出二十二项措施，包括打造超大规模自主智算集群、构建多层次语料供给体系、加快行业基座大模型体系创新等内容。

方案提出，要构建多层次语料供给体系。建立一批通用和专用语料库，打造多层次语料体系，支撑基础大模型研发和垂直应用。聚焦前沿大模型训练需求，推动打造基础大模型训练语料库。聚焦金融、制造、教育、医疗、文旅、城市治理等行业需求，打造一批行业开放语料库与测试数据集。建设语料公共服务平台，构建语料处理、生产、运营等工具链平台。培育一批开箱即用的语料服务产品。探索建立新型语料开放共享收益分配机制。

方案强调，要构建人工智能测试评估体系。加快建设大模型测评标准，支持本市创新主体参与或主导国内外大模型测评标准研制。建设人工智能大模型测试验证平台，面向智能体、具身智能等重点应用，提供测试验证服务。依托优质企业和测评机构等，围绕通用和垂直领域应用，加快大模型测评语料库体系建设。（来源：上海市人民政府）

9. 上海浦东新区人民政府发布《浦东新区公共数据授权运营管理若干规定（试行）》

12月30日，上海浦东新区人民政府发布《浦东新区公共数据授权运营管理若干规定（试行）》，自2025年2月1日起施行，有效期至2027年1月31日。规定共二十条，包括职责分工、参与主体、授权运营协议等内容。

规定指出，浦东新区公共数据授权运营的实施机构为区大数据中心，在区数据主管部门指导下，具体负责组织开展授权运营活动。运营机构是指按照规定程序获得授权，对授权范围内的公共数据进行开发运营的法人或者非法人组织，按需对本区公共数据进行基础治理、开发，为其他经营主体提供安全开发场地、开发利用管理、服务能力支撑、市场生态培育和

安全保障等便利化支撑服务。其他经营主体是指在安全可信环境下对运营机构提供的公共数据产品进行再开发、再利用的法人或者非法人组织，根据市场需求推动多源数据融合，提升数据产品价值，赋能产业经济发展。

规定强调，运营机构应当定期向实施机构报告公共数据授权运营情况和公共数据使用情况。运营过程中发现涉嫌侵犯国家秘密、工作秘密、商业秘密和个人信息权益的，应当立即停止相应的数据处理活动，并及时向区数据主管部门和实施机构报告。实施机构应当定期向社会披露授权对象、内容、范围和期限等公共数据授权运营情况。（来源：上海市人民政府）

10. 天津市数据局发布《天津市公共数据资源登记管理实施细则（试行）》（征求意见稿）

12月23日，天津市数据局发布《天津市公共数据资源登记管理实施细则（试行）》（征求意见稿），共六章三十二条，包括职责分工、登记要求、登记程序等内容。

征求意见稿规定，登记主体可以委托具备相关资质、相应管理和技术能力的第三方专业服务机构参与公共数据资源登记活动。第三方专业服务机构应严格按照委托事项依法客观、独立公正开展相关服务，不得与登记机构、登记主体之间存在重叠、隶属或其他利益关联关系，在服务过程中不得存在虚假记载、误导性陈述、信息泄露等违法违规行为。

征求意见稿提出，涉及公共数据资源授权运营的，登记主体在申请登记前应当自行或委托第三方专业服务机构，通过技术手段在保障安全的前

提下对公共数据资源进行存证，确保来源可查、加工可控。（来源：天津市数据局）

11. 海南省人民政府办公厅发布《海南省国土空间基础数据管理办法》

12月24日，海南省人民政府办公厅发布《海南省国土空间基础数据管理办法》，共七章二十八条，包括采集汇交、共享应用、安全保障等内容。

办法规定，“国土空间基础数据”是指与国土空间位置及其时态有关的，可以为多个行业、多项业务提供支撑的自然、经济、社会等信息，包括基础测绘数据，基础地质数据，土地、矿产、森林、草原、水、湿地、海域、海岛等基础调查数据，以及各政务部门和公共服务组织的行业专题国土空间基础数据。

办法提出，国土空间基础数据的采集和生产应当遵循一种数据一个来源的原则，各有关单位应当按照职责开展采集汇交工作。各单位对基础测绘数据、基础地质数据、基础调查数据有采集需求的，有关部门在年度计划审核或批准立项前应按数据类型充分征求同级相关行业主管部门的意见，避免重复采集、多头采集。（来源：海南省人民政府）

12. 福建省网信办发布《福建省个人信息出境标准合同备案实施办法》

12月24日，福建省网信办发布《福建省个人信息出境标准合同备案实施办法》，共二十四条，规定福建省内个人信息处理者通过与境外接收方

订立个人信息出境标准合同的方式向中华人民共和国境外提供个人信息的要求。

办法规定，以下情形属于个人信息出境行为：（1）个人信息处理者将在境内运营中收集和产生的个人信息传输至境外；（2）个人信息处理者收集和产生的个人信息存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；（3）符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他个人信息的活动。

办法提出，中国（福建）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，经省委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。中国（福建）自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免于备案个人信息出境标准合同。（来源：网信福建）

13. 贵州省人民政府办公厅印发《贵州省推动人工智能高质量发展行动方案（2025—2027年）》

12月28日，贵州省人民政府办公厅印发《贵州省推动人工智能高质量发展行动方案（2025—2027年）》，围绕智算能力提升行动、数据资源建设行动、行业大模型发展行动、智能产业培育行动、数字生态优化行动提出十四项重点任务。

实施数据资源建设行动，保障高质量数据供给方面，方案提出，要推进公共数据开发利用。制定公共数据授权运营管理办法，建设完善贵州省

公共数据平台，建立公共数据目录“一本账”体系，围绕自然资源、交通、民政、住建、人社、医保、市场监管、教育等重点领域，开展公共数据授权运营。发挥公共数据牵引作用，推动行业、企业数据依法依规授权使用。

实施数字生态优化行动，激发改革创新活力方面，方案提出，要统筹发展与安全。落实国家关于人工智能监管要求，引导企业建立完善安全评估、风险防范机制。针对人工智能不同发展阶段、不同应用场景、不同服务对象实施分类管理。开展人工智能风险研判，推动协同治理、强化问题处置。加强网络、信息和数据安全。管理。（来源：贵州省人民政府）

境内前沿观察三：治理实践

导读：12月，公安、网信、工信等部门持续发力，对网络安全进行全方位、多层次有效治理，提升网络安全防护能力，构建更加安全、健康、有序的网络生态。

公安机关方面，公安部公布打击整治“网络水军”违法犯罪工作情况，2024年以来依托“净网2024”专项行动，公安机关打击整治“网络水军”违法犯罪，共侦破案件900余起，抓获嫌疑人5000余名。上海警方通报2024年打击各类涉网违法犯罪成果。2024年以来，上海公安机关侦破涉网案件8000余起；其中，侦破黑客类犯罪案件同比上升35%，侦破网络黑灰产案件2500余起，查处非法APP、网站300余个，侦破网络谣言案件1100余起。同时，浙江、山东、山西、上海等地方公安机关发布多起典型案例，围绕打击治理“网络水军”、侵犯公民个人信息、电信诈骗等违法犯罪行为。

网信部门方面。国家网信办集中整治网上金融信息乱象，会同相关部门处置一批在抖音、快手、微博、微信等平台上从事非法荐股、非法金融中介等活动的账号，清理金融领域引流类及诱导性违规信息，加大对无资质从事金融相关业务的网站及账号的处置处罚力度。中央网信办还发布一批打击网上侵害未成年人合法权益典型案例。同时，海南省网信办持续开展互联网移动应用程序违法违规收集使用个人信息专项治理，组织对省内用户量大、群众投诉反映集中等涉网络社交、网络游戏、生活服务类等领域移动应用程序进行巡查，发现10款App存在违法违规收集使用个人信息

行为，责令整改。湖南湘潭网信部门开展医疗行业个人信息权益保护执法检查。个案方面，因系统页面被篡改改为博彩页面，南昌市网信办对某企业作出行政处罚；因未履行数据安全保护义务，重庆市网信办对某网络科技有限公司作出罚款处罚。

通信管理部门方面，湖北省通信管理局组织开展工业领域网络和数据安全风险监测处置专项行动工作，以工业企业、工业互联网平台企业等为监测对象，以强化风险监测、深入分析研判等作为重点任务；浙江省通信管理局组织开展2024年“数安铸盾”数据安全应急演练，采用场景模拟方式开展，分为事件研判分析、事件上报等环节，各企业参与人员涉及云网运维团队、安全团队等；上海市通信管理局组织开展2024年度云服务安全专项治理工作，重点检查企业网络运行及云服务安全制度建设落实、风险隐患清单管理、平台监控及系统冗余保护能力建设、运行事故应急演练等方面工作情况；青海、贵州、宁夏等地通信管理局根据工信部工作部署，对本地区基础电信企业开展网络与信息安全责任考核年终检查。

关键词：网络水军、涉网违法犯罪、金融信息乱象、应急演练、基础电信企业年终检查

（一）公安机关治理实践

1. 公安部公布打击整治“网络水军”违法犯罪工作情况：侦破案件 900 余起

12月12日，公安部公布打击整治“网络水军”违法犯罪工作情况。据统计，2024年以来依托“净网2024”专项行动，公安机关打击整治“网络水军”违法犯罪，共侦破案件900余起，抓获嫌疑人5000余名。

同期公布十起典型案件，分别是：（1）山东枣庄公安机关侦破某传媒公司编造谣言引流案；（2）广东广州公安机关侦破叶某某等人编造谣言引流案；（3）浙江温州公安机关侦破许某某等人编造谣言引流案；（4）江西抚州公安机关侦破邹某某等人网络敲诈勒索案；（5）河南南阳公安机关侦破宋某某等人网络敲诈勒索案；（6）浙江台州公安机关侦破范某等人刷单炒信案；（7）江苏宿迁公安机关侦破宗某等人刷量控评案；（8）四川内江公安机关侦破赵某某等人刷量控评案；（9）江苏镇江公安机关侦破肖某等人有偿删帖案；（10）辽宁锦州公安机关侦破西某等人有偿发布虚假信息删帖案。（来源：公安部网安局）

2. 上海警方通报 2024 年打击各类涉网违法犯罪成果：侦破涉网案件 8000 余起

12月19日，上海警方通报2024年打击各类涉网违法犯罪成果。2024年以来，上海公安机关深入开展“净网2024”和“砺剑”系列专项行动，

聚焦人民群众关心的网络安全问题，紧盯新特点新趋势，重拳严打网络黑灰产、网络黑客、网络谣言等各类涉网违法犯罪，共侦破涉网案件 8000 余起。同时，持续深化网络空间治理，指导互联网企业健全未成年人安全上网优化保护机制，护航青少年上网安全，切实维护清朗有序网络环境。

具体而言，严厉打击涉网违法犯罪方面，网络黑灰产、网络黑客、侵犯公民个人信息和网络谣言四类案件比较突出。2024 年，上海警方侦破黑客类犯罪案件同比上升 35%；侦破网络黑灰产案件 2500 余起，查处非法 APP、网站 300 余个；侦破网络谣言案件 1100 余起，目前全市网络谣言案件发案数明显下降，打击整治网络谣言违法犯罪取得阶段性成效。

强化管理引导企业合规发展方面，2024 年，本市互联网平台主动加强平台内容管理，累计针对“毒视频”“开盒挂人”等内容，清理违法有害信息 213 万余条，封禁账号 10.4 万余个。公安机关累计对互联网企业开展释法培训、以案说法等法律宣贯千余场，发送公安风险提示函 8000 余份。

建立健全保护机制、护航未成年人安全上网方面，上海公安网安部门与市委网信办、市人民检察院和市文旅局健全完善本市未成年人网络保护四方协同机制，指导互联网企业建立健全预防网络游戏沉迷、优质信息推送、账号实名认证等多项未成年人安全上网优化保护机制。（来源：上海网警）

3. 因数据库存在安全漏洞，浙江台州公安机关对浙江某软件科技公司作出行政处罚

12月24日消息，浙江台州公安机关近日工作中发现，浙江某软件科技公司受托搭建的数据库存在安全漏洞，数据库中承载的大量电子政务数据存在泄露风险。

经查，该公司主要为政府部门提供软件开发、信息系统建设和运维等服务。在与台州当地部分政府部门合作期间，该公司未对受托维护、处理的电子政务数据履行应尽的数据安全保护义务，未依法建立全流程数据安全管理制度，导致电子政务数据存在严重泄露风险，相关行为违反《数据安全法》。

台州公安机关依法对该公司和该公司负责人进行行政罚款，并责令其依法依规履行数据安全保护义务。同时，依法约谈涉事政府部门相关负责人，通报委托处理电子政务数据活动中存在的安全问题，责令进一步加强数据安全管理和保护，严防数据泄露。（来源：浙江网警）

4. 山东警方破获一起利用制作、安装木马程序等手段盗窃网民游戏账号及虚拟装备案

12月8日消息，山东济宁曲阜警方近日破获一个利用制作、安装木马程序等手段，盗窃网民游戏账号及虚拟装备案，涉案金额高达三千多万元。

2024年初，曲阜警方接到某网络公司报案称，其旗下许多玩家游戏账号在不知情的情况下，被登录并盗取虚拟资产，曲阜男子陈某某曾在网上大量倒卖被称为“黑号”的游戏账号和虚拟资产。警方迅速锁定陈某某并

将其抓获，并发现从 2023 年年初至案发时一年的时间内，陈某某倒卖游戏“黑号”和虚拟资产共非法获利 20 万元。警方发现陈某某在犯罪链条中处于比较底层的‘号商’角色，主要从事低于市场价购入非法盗取来的黑号，加价后高价卖给发卡平台、租号平台和一些玩家，从中赚取差价。陈某某的上线‘号商’为张某某，警方于 3 月份将张某某抓获，并得知张某某是通过叫杨某的上线人员获取的‘登录态’数据。

警方调查发现，嫌疑人通过盗取“登录态”数据再侵入他人游戏账号，进而窃取虚拟资产。该手法比以往更加隐蔽，不仅游戏玩家难以觉察，网络游戏公司同样难以发现。在抓获张某某后，办案民警在其电脑里发现大量的各类游戏登录缓存，“缓存”即不法分子用来侵入他人游戏账号的“登录态”数据。张某某按照游戏账号的等级、种类以及游戏账号所含虚拟资产的价值、数量进行筛选分类，然后出售给下游“号商”。一些游戏玩家账号内的“点券”等虚拟资产被盗后，造成数万元的经济损失。民警先后将贩卖编写、制作“上号器”等黑客程序，编译、制作盗号木马程序、盗取和倒卖“登录态”数据和他人游戏虚拟资产的邹某某、许某某、程某、杨某等 10 多名犯罪嫌疑人抓获。

在广东中山，盗取“登录态”数据的杨某和编译制作木马程序的许某某同时落网。他们就是张某某的上线，张某某的他人游戏账号都是从杨某手中购买的。在杨某的电脑里，民警查获“登录态”数据 400 多万条。经查，杨某通过倒卖、盗取的“登录态”数据共获利 140 多万元。在许某某电脑里，民警查获木马程序 11 个。行动中，警方缴获涉案电脑、手机等一

批作案工具，查扣各类黑客程序 23 件以及犯罪嫌疑人盗取的公民个人信息 3700 多万条。

目前，17 名犯罪嫌疑人已被警方依法采取刑事强制措施，案件还在进一步深挖扩线中。（来源：公安部网安局）

5. 山西警方破获一起架设“手机口”实施电信诈骗案

12 月 11 日消息，山西警方近日破获一起架设“手机口”实施电信诈骗案件。“手机口”是指将两部手机同时打开外放，其中一部手机通过网络社交软件与境外诈骗分子通话，另一部则插入本地电话卡拨打受害人电话，实现语音中转，成功掩饰诈骗电话归属地，来降低受害人的警惕。

公安网安部门工作发现，有人利用“手机口”新型诈骗方式，协助境外电信网络诈骗团伙频繁拨打电话，涉嫌帮助信息网络犯罪。经查，犯罪嫌疑人杜某为获取利益应聘“高薪聘请话务员”。杜某在境外诈骗人员指引下，其中一部手机添加诈骗分子即时通讯账号接听语音电话，另一部手机拨打诈骗分子提供的被害人手机号码，在免提状态下让诈骗分子与被害人通话实施诈骗，上线后按小时为其结算获利。

杜某在发现有利可图之后，将自己身边的 9 名同学发展成自己的“帮手”，让他们也通过该方式进行电信诈骗，事后由杜某将“报酬”分发给他们。目前，公安机关已依法对相关人员进行处罚。（来源：公安部网安局）

6. 甘肃警方依法查处一起侵犯公民个人信息案

12月12日消息，甘肃武威公安机关网安部门近日在对辖区内某房屋装修公司例行检查时发现，该公司业务员正手持某新建小区业主信息登记表，逐一拨打业主电话，推销其公司装修业务。经仔细检查询问，民警在该公司办公电脑及业务员的手机内，发现大量包含业主公积金信息、贷款信息、个人征信记录以及房屋价格等敏感个人信息。

民警发现，该房屋装修公司从新建小区销售人员处非法购买到购房者的个人留存信息，让其业务员通过拨打电话的方式推销装修业务，之后又将非法获取到的个人身份信息转卖给其他家具经销商、材料供销商，导致大量业主的个人信息泄露，严重干扰辖区居民日常生活。

公安机关网安部门寻线追踪，持续深挖调查，发现3个非法获取、出售或提供公民个人信息的犯罪团伙。公安机关网安部门开展集中收网行动，抓获主要犯罪嫌疑人3名，查获非法获取公民个人信息的违法行为人19名。同时，对不履行个人信息安全保护义务的多家地产企业、装修公司等进行行政处罚。（来源：公安部网安局）

7. 上海警方全链条捣毁一个“网络水军”犯罪团伙

12月14日消息，上海警方近日经过缜密侦查，全链条捣毁一个有偿组织网络写手，撰写、发布不实贴文的“网络水军”犯罪团伙，抓获犯罪嫌疑人11人，涉案金额达200余万元。

上海市公安局金山分局在工作中发现，张某所开设的上海某文化有限公司通过发布虚假正面贴文来沉降负面贴文、美化搜索下拉词等方式违规

优化某连锁品牌房屋中介公司负面评论，即在市公安局网安总队的指导下成立专案组开展侦查。

经专案组调查发现，该公司对外声称其业务为企业品牌形象优化，实则提供处置虚假贴文信息服务。经查证，张某系公司法人代表兼实际经营者，公司架构清晰、职责分明。经查，2022年5月以来，该公司在未获取《互联网增值电信业务经营许可证》的情况下，先后与某生物技术公司、某房屋中介公司、某游轮服务公司等十余个品牌运营方签署品牌网络优化服务协议，并根据品牌方要求，在未实际体验过或接触过相关产品的情况下，组织“写手”黄某撰写虚假正面文字稿150余篇（部分文章由AI生成），交由吴某经营的某文化传媒有限公司在互联网平台上批量发布，意图稀释负面舆情、下沉负面贴文，虚增指定产品的影响力、曝光度、好评度、美誉度，涉嫌违法犯罪。

专案组分赴多地集中收网，全链条捣毁由运营公司、写稿人、发稿人组成的“网络水军”团伙11人，现场扣押作案手机30部、电脑11台、相关合同11份，涉案金额达200余万元。目前，张某等11名犯罪嫌疑人已被警方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）

8. 上海警方侦破一起利用共享充电宝侵犯公民个人信息案

12月19日，上海警方近日成功侦破一起侵犯公民个人信息案，抓获以犯罪嫌疑人董某为首的涉案公司相关人员，并在公安部指导下在全国范围内组织多波次集群战役，先后抓获涉案宾旅馆负责人110余人。

2023年8月，上海宝山某酒店负责人向上海市公安局宝山分局高境派出所反映线索称，一个自称经营共享充电器的公司表示能在共享充电器投入酒店使用后给予免费“刷好评”服务，怀疑涉嫌违法犯罪遂向警方举报。获悉后，宝山警方迅速展开调查，发现辖区内有一家旅馆刚刚与该公司达成合作协议但尚未实施。在研究合作协议和客服话术后，警方初步掌握该公司的合作模式，即宾旅馆在达成合作协议后，免费将共享充电器投入每个客房，住户使用后产生的费用公司按比例分成，在此基础上公司根据合作酒店提供的住户信息提供“刷好评、删差评”的所谓增值服务。

经调查，警方确认该公司在运营共享充电器过程中，以提供“刷评服务”为诱饵，非法获取大量公民个人信息，从而实现迅速抢占全国市场资源和扩大品牌影响力的目的。据此，在市公安局网安总队的指导下，宝山警方成立专案组，对该公司及相关合作宾旅馆的资金端、信息端进行调查取证，对本市个别已经涉嫌侵犯公民个人信息的宾旅馆进行逐个查证打击。

随着调查的深入，上海警方发现涉案公司总部位于吉林省某地，公司分部则分散在吉林、四川等多地，已经合作的宾旅馆散布全国各地。在精准梳理掌握该公司负责人董某及另外9名业务骨干的具体分工和犯罪证据后，2024年4月，上海警方会同吉林、四川警方展开集中收网行动，将犯罪嫌疑人董某及其公司涉案员工全部抓捕归案。之后，自6月起至今，上海警方在公安部指导下，在全国各地发起多轮次集群战役，循线先后抓获涉嫌非法提供住客信息的宾旅馆负责人110余人。

经查，该公司分工严密，共设置销售部、技术部、好评部、差评部、售后部等5个部门，并对员工进行系统的话术培训。其中前端部门销售部

负责推广和签订合作协议，再根据推广成功的宾旅馆和客房数量按比例获得收入提成；技术部负责共享充电器投放后的运维；售后组负责汇总充电器使用数据后向相关宾旅馆返利。

合作宾旅馆每月通过制表、手抄、翻拍等方式向涉案公司提供住客姓名、入住时间等信息后，公司好评部、差评部一方面安排客服以宾旅馆或服务平台名义对住户进行海量回访，引导住户在相关服务平台订单内给予好评；另一方面，客服会根据相关平台内的差评关键词、图片、时间等，使用自行研发的非法插件加人工分析，结合宾旅馆提供的入住信息，倒推出实际入住人，并采取电话骚扰和修改评价给予返利等方式进行软磨硬泡，以此实现“删差评刷好评”的最终目的。

据涉案公司骨干成员供述，由于星级酒店、连锁酒店等管理比较规范，为提高合作成功率，他们把推广重点锁定在房间均价 200 元左右的小旅馆，许诺能够在其他共享充电器品牌 85%返利的基础上进一步提高返利额度至 98%，并定期给予一定数量的刷好评和删差评服务。2022 年 7 月至今，涉案公司已经与全国众多宾旅馆达成合作协议，通过非法获取公民个人信息帮助合作宾旅馆删除差评 10 万余条。

目前，犯罪嫌疑人董某因涉嫌侵犯公民个人信息罪已被检察机关依法批准逮捕，其余犯罪嫌疑人已被警方依法采取刑事强制措施。警方初步查明，涉案相关公民信息仅被用于所谓“刷评服务”，并未对外泄露。下一步，警方将对相关涉案宾旅馆开展进一步调查，并会同相关部门强化行业监管。（来源：上海网警）

9. 上海黄浦警方破获一起非法获取计算机信息系统数据案

12月23日消息，上海黄浦警方近日破获一起非法获取计算机信息系统数据案。

2024年2月，上海警方接到某互联网企业报案称，旗下一款社交平台在进行安全检查的过程中，发现大量账号近期发布涉诈、涉赌、色情等信息。与此同时，平台接到大量相关账号登录异常的投诉举报。上海警方迅速开展侦查工作，成功锁定某高校计算机专业在读大学生、年仅19岁的犯罪嫌疑人蒋某鹏。经查明，自2023年10月起，蒋某鹏利用平台登录机制漏洞，使用自制的黑客软件伪造用户的“登录凭证”，从而获取登录权限，并搭建网站出售账号。截至案发，蒋某鹏利用黑客技术手段非法获取账号4万余个，通过售卖账号累计获利7万余元。

2024年3月，网安部门将犯罪嫌疑人蒋某鹏抓获。经警方进一步深挖涉案线索发现，相关被盗账号背后暗藏着一个黑灰产团伙。史某辉购买涉案账号，林某毅等4人通过购买账号，发布涉诈、涉赌、色情等信息。

目前，蒋某鹏因非法获取计算机信息系统数据罪，被黄浦区人民法院判处有期徒刑三年，缓刑三年，并处罚金人民币三万元。史某辉以涉嫌侵犯公民个人信息罪被立案侦查。林某毅等4人被处以行政处罚。警方已督促该企业修复系统漏洞，完善落实平台安全机制，对发布违法信息的账号进行封停或禁言。（来源：上海网警）

10. 北京海淀警方发布整治涉网犯罪典型案例

12月27日，北京海淀警方发布三起整治涉网犯罪典型案例。

案例一：侵犯公民个人信息案件

近期，海淀警方接到辖区某院校报警称有人在网上贩卖公民个人信息牟利。接警后，海淀分局警务支援大队迅速行动，对线索抽丝剥茧、深挖扩线，发现一个以邓某为首出售个人信息牟利的团伙，成功斩断网上贩卖公民个人信息犯罪链条。海淀警方在掌握相关证据后组织 40 名警力，奔赴全国多地将邓某等 17 人抓捕归案。经审讯，邓某等人通过违法手段获取大量个人信息，出售、提供给从事“代刷课时”“代为考试”人员。警方现场起获实施违法犯罪设备 60 余台。邓某等人对侵犯公民信息的犯罪事实供认不讳，目前邓某等 17 人已被海淀警方依法刑事拘留。

案例二：网络水军非法经营案

海淀警方成功破获一起网络水军案件，起获数十台实施违法犯罪设备，刑事拘留 1 人，涉案金额 20 余万元。海淀分局警务支援大队在日常网络巡检中发现有人在短视频平台发布虚假评论并对部分用户进行虚假举报，通过串并分析疑似为有组织有目标的“水军”。经深度排查梳理，发现犯罪嫌疑人岳某有重大作案嫌疑，海淀警方果断出击，将岳某抓获归案。经审查，岳某通过违法手段控制数百个账户，对各大互联网短视频平台、电商平台用户，提供虚假评论、恶意举报，严重扰乱了网络平台市场经济秩序。目前，岳某因涉嫌非法经营罪被海淀警方依法刑事拘留。

案例三：非法获取计算机信息系统数据案

近期，海淀警方接辖区某企业报警称员工办公电脑存在异常，疑似被植入木马病毒。海淀分局警务支援大队随即赶赴现场开展勘验取证工作，通过初步调查，锁定该企业员工鲁某具有重大作案嫌疑。侦查人员顺线深

挖，成功发现以刘某为首的犯罪团伙。该团伙组织成员对互联网企业投放木马程序，获取用户数据。掌握相关证据后，海淀警方雷霆出击，一举抓获刘某等 12 名犯罪嫌疑人。经工作，刘某等 12 名嫌疑人通过违法手段，在目标公司大量植入具有远程控制功能的木马程序，窃取公司用户数据并出售牟利的犯罪事实供认不讳。目前，刘某等 12 人因涉嫌侵犯公民个人信息罪、非法获取计算机信息系统数据罪被海淀警方依法刑事拘留。（来源：公安部网安局）

（二）网信部门治理实践

1. 国家网信办集中整治网上金融信息乱象

12 月 11 日消息，2024 年以来，国家网信办深入贯彻落实党中央、国务院工作部署，对网上金融信息乱象保持高压严打态势，会同相关部门处置一批在抖音、快手、微博、微信等平台上从事非法荐股、非法金融中介等活动的账号，清理金融领域引流类及诱导性违规信息，加大对无资质从事金融相关业务的网站及账号的处置处罚力度。对从事助贷业务的网站平台，要求其规范营销信息展示和营销功能设置，加强信息风险披露。下一步，国家网信部门将继续加强对网上金融信息乱象的打击整治力度，规范网上金融信息传播秩序，着力维护人民群众财产安全。

网信部门提示，当前非法金融活动呈现形式多样、隐蔽性强的特点，有的打着“拼单团购”“社交电商”“消费返利”“网络兼职”“虚拟养殖”“电子币交易”等旗号开展网络传销活动，有的以“债务重组”“债

务优化”为名收取“砍头息”加重债务人负担，有的以“零门槛”“零利息”“到账快”等话术诱导盲目借贷。特别是随着近期资本市场交易活跃度提升，一些账号以“分享炒股技巧”“大佬看盘”“高手指导”为噱头，通过直播、短视频、图文等形式从事非法荐股活动并骗取高额费用，对投资者特别是中小投资者造成财产损失。（来源：网信中国）

2. 中央网信办发布打击网上侵害未成年人合法权益典型案例

12月19日，中央网信办发布打击网上侵害未成年人合法权益典型案例。

案例一：恶意炮制发布“沙雕动画”短视频。巡查发现，短视频平台部分账号集纳“沙雕动画”，包含大量血腥、惊悚等负面内容。部分账号恶意改编经典动画，发布“暴力海绵宝宝”“惊悚米奇”等内容。部分短视频内容借动画形式，模拟校园欺凌情节，美化自杀自残行为，严重危害未成年人身心健康。网信部门对相关平台予以行政处罚，关闭一批集纳发布“沙雕动画”的违规账号。

案例二：隐匿传播涉未成年人软色情内容。专项行动期间发现，有用用户在未成年人分享日常生活内容页面的评论区，恶意发布低俗表情包和“找同城”等不良交友信息，企图对未成年人实施性引诱。在一些未成年人集中的频道版块、兴趣圈子等环节，部分用户使用分隔符、替代词等方式，发布传播低俗色情内容。网信部门指导网站平台持续加大对各类违规暗语的识别打击力度，深入清理涉未成年人违规外链信息。相关违法线索已转公安机关。

案例三：利用“网红儿童”违规牟利。根据网民举报线索，部分账号频繁发布涉未成年人不良导向内容，炮制所谓“网红儿童”，违规引流牟利。包括让未成年人摆拍校园霸凌视频，售卖所谓“小混混鞋”等商品；以未成年人结婚怀孕等为噱头，发布“07年宝妈在婆家带娃的一天”等内容；让未成年人演绎“做一个绿茶的自我修养”“良心没了可以挣更多”等不良价值观内容，引流售卖商品。网信部门对相关账号依法采取清理粉丝、取消营利权限、关闭等处置措施，坚决打击借“网红儿童”牟利行为。

案例四：诱导未成年人参与“直播拆卡”。巡查发现，部分直播间售卖动漫、游戏等卡牌盲盒，鼓动诱导未成年人过度消费。个别商家使用“蜜桃”“欲望”“女神”等暗示词汇，诱导网民购买加热或遇水后显示低俗内容的“温感卡”“水感卡”。有主播在直播时刻意遮挡、快速闪现卡牌封面，违规售卖展示动漫人物敏感部位、挑逗姿势的低质盗版卡牌。网信部门指导直播和电商平台优化未成年人消费风险提示功能，对盲盒类产品强化年龄确认，平台主动开展店铺商家合规指导，累计处置违规直播1700余场，下架商品2.8万余个。

案例五：利用新技术新应用生成涉未成年人不良内容。专项行动期间发现，部分用户利用AI绘图技术，恶意将未成年人图片转换成儿童怀孕状态、身穿裸露服装等恶俗低俗漫画。一些“AI恋人”类APP存在涉未成年人不良人物角色，通过AI对话服务变相传播低俗信息。网信部门依法从严处置处罚问题突出的平台和账号，督促此类AI服务平台开展自查自纠，及时下线存在涉黄风险的AI人物，健全未成年人网络保护机制。

案例六：青少年模式下呈现违法不良信息。巡查发现，个别社交平台开启青少年模式后，在搜索框搜索“正能量”“吃瓜”“福利”等关键词，搜索结果呈现色情引流信息，诱导未成年人添加群组、下载 APP，传播涉黄涉赌内容。个别平台开启青少年模式后，存在擦边图片或低俗评论内容。网信部门依法从严处置处罚问题突出平台。同时，督促平台积极推进模式建设升级，强化评论、弹幕、留言等互动环节管理，严防信息内容风险。

案例七：儿童智能设备存在违法违规内容。根据网民举报线索，部分儿童智能手表通过产品搭载的语音问答服务，传播危害未成年人身心健康的信息。个别学习平板电脑的应用商店提供短视频 APP 下载服务，下载后呈现低俗擦边舞蹈视频，评论区等环节存在色情赌博网站引流信息。网信部门及时约谈有关儿童智能设备企业，督促全面排查设备自带及第三方 APP 内容安全，并对违规企业予以行政处罚。（来源：网信中国）

3. 中央网信办举报中心依法受理处置 518 个仿冒诈骗类网站平台

12 月 27 日消息，一段时期以来，有不法分子打着“金融投资”“退费补贴”“消费充值”“证件办理”“期刊征稿”等幌子，仿冒有关部门、单位官方网站平台，实施诈骗活动，严重影响部门公信力，侵害人民群众合法权益和财产安全，社会危害大，群众反映强烈。

2024 年，中央网信办举报中心持续深化涉仿冒诈骗类网站平台受理处置工作，广泛收集举报线索，积极协调核查认证，有效回应网民关切，共受理处置违法违规网站平台 518 个。其中，涉及仿冒教育部、财政部、人力资源和社会保障部等政府机关类网站平台 279 个，仿冒中国石化、中国

一汽、国家电网等国有企事业单位类网站平台 83 个，仿冒腾讯、抖音、TCL 等民营企业类网站平台 41 个，仿冒《现代大学教育》《暨南学报》《铁道科学与工程学报》等期刊杂志类网站平台 115 个。

中央网信办举报中心梳理发现，仿冒诈骗类网站平台存在以下特点：一是迷惑性强。通过镜像、复制相关部门官方网站等形式进行伪装，令网民难以分辨真伪，极易受骗。二是诱惑性强。常以宣传“高额利息”“退费补贴”“有偿发稿”等内容为噱头，诱导网民落入诈骗陷阱。三是隐蔽性强。绝大多数服务器在境外，网址域名经常跳转，以此逃避监管。（来源：网信中国）

4. 海南省网信办开展互联网移动应用程序违法违规收集使用个人信息专项治理

12 月 30 日消息，海南省互联网信息办公室近日组织对省内用户量大、群众投诉反映集中等涉网络社交、网络游戏、生活服务类等领域移动应用程序进行巡查，重点围绕移动应用程序违法违规收集使用个人信息等突出问题进行集中采集检测，结果显示 10 款 App 均存在不同程度的非法获取、超范围收集、过度索权等违法违规收集使用个人信息行为，集中向社会通报并责令相关运营单位限期整改。同时，对上一批次通报中整改工作表现良好的 28 款移动应用程序予以肯定。

近年来，海南省高度重视互联网个人信息保护工作，对这一领域的违法违规行为保持高压态势。2024 年，海南省网信办共采集检测 APP、小程序等类型移动应用程序达 600 余款，通报整改 90 款，现场执法检查 9 款，

依法下架 2 款，覆盖社交平台、网络直播、网络游戏、生活应用等 10 余个社会民生重点领域；联合省市场监督管理局、省商务厅开展为期 6 个月的商场超市消费领域个人信息保护专项执法行动，覆盖 9 家企业主体旗下门店 61 家，涉及消费者人数达 342.82 万，下达责令限期整改通知书 9 份，全部督促整改。（来源：网信海南）

5. 江西南昌网信办依法处置违规从事生成式人工智能服务企业

12 月 2 日消息，在江西省委网信办的指导下，南昌市网信办近日依法对属地网站“阿水 AI”的运营主体南昌阿水科技有限公司存在内容审核管理不严、主体责任落实不到位等问题进行处置。

经查，该企业运营的“阿水 AI”网站违规生成法律法规禁止的信息，未尽内容审核的主体责任，违反《网络安全法》《生成式人工智能服务管理暂行办法》等相关法律法规。南昌市网信办依据《网络安全法》《生成式人工智能服务管理暂行办法》等法律法规，对南昌阿水科技有限公司下达《责令限期改正通知书》，责令立即关停相关服务，并对照相关法律法规开展自查整改，加强信息内容审核，健全信息内容安全管理相关制度。

（来源：网信南昌）

6. 湖南湘潭联动开展医疗行业个人信息权益保护执法检查

12 月 6 日消息，在湖南省网信办的指导下，湘潭市网信办近日针对医疗行业在日常工作中收集使用个人敏感信息、个人医疗和普通医疗信息等数据问题，联合市卫健委等部门开展执法督导检查。

检查中发现，属地2家医疗机构存在个人信息保护工作制度不健全、未完全告知用户应告知事项等问题。根据《个人信息保护法》第六十六条第一款规定，检查组现场下达责令限期整改通知书，并围绕《网络安全法》《个人信息保护法》等相关法律法规，结合案例开展普法宣讲。针对网民反馈的“某医院体检中心存在过度收集个人信息”问题，检查组通过走访体检中心、约谈负责人及查验相关平台等方式，核实到收集用户个人信息是基于向已婚人士提供特定医疗检查项目的工作需要，不属于过度收集范畴，已及时回应网民诉求。（来源：网信湖南）

7. 因存在个人信息泄露风险，湖南怀化网信办集中约谈15家单位

12月13日消息，湖南省怀化市网信办近日通过技术手段发现，怀化**网络信息有限公司、怀化市**中学、怀**集团等15家单位的系统平台存在较高网络安全隐患，有泄露个人信息（含人脸生物特征）风险。针对上述情况，怀化市网信办集中约谈该15家单位。

会上，怀化市网信办组织学习《网络安全法》《数据安全法》《个人信息保护法》等法律法规，要求各单位要树牢网络安全、数据安全、个人信息保护意识，遵守相关法律法规，保障公民权益。会议要求，各单位要提高政治站位，切实增强做好网络安全、数据安全、个人信息保护工作的使命感和责任感，按照“问题导向”原则，认真抓好网络安全风险隐患限期整改，确保个人信息安全。（来源：网信湖南）

8. 因未履行数据安全保护义务，重庆市网信办对属地公司作出行政处罚

12月23日消息，重庆市网信办近日根据上级部门移交线索，依法对属地存在网络数据安全违法行为的公司作出行政处罚。

经查，重庆某网络科技有限公司未履行网络安全、数据安全保护义务，存在未建立完善相关制度规范，未明确相应管理机构，未采取相应的技术措施和其他必要措施保障数据安全，存在网络数据泄露风险，同时存在未经授权的访问和未按法规要求留存相关网络日志等违法情形，违反《网络安全法》和《数据安全法》。重庆市网信办依据《数据安全法》，对该公司作出责令改正，给予警告，并处五万元罚款的行政处罚，对直接主管人员和其他责任人员分别处以一万元罚款处罚。（来源：网信重庆）

9. 因系统页面被篡改为博彩页面，江西南昌网信办对属地某软件销售公司作出行政处罚

1月3日消息，江西省南昌市网信办近日接上级网信部门通报，南昌市某软件销售公司所属CRM系统疑似遭黑客组织攻击并植入木马病毒，系统首页被篡改为博彩页面。

经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：该企业履行网络安全保护义务不到位，未按照法律要求开展网络安全等级保护测评，未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，导致所属CRM系统首页显示为博彩网站，

提供大量违法违规内容及服务，造成危害网络安全的后果。相关行为违反《网络安全法》第二十一条的规定。

2024年12月31日，南昌市网信办依据《网络安全法》第五十九条的规定，对该企业作出罚款1万元、对直接负责的主管人员作出罚款5千元的行政处罚。（来源：网信南昌）

（三）通信管理部门治理实践

1. 工信部、多地通信管理局通报侵害用户权益行为 APP

（1）工信部

12月27日，工信部信息通信管理局通报2024年第10批（总第45批）侵害用户权益行为的APP（SDK）。通报指出，工信部近日组织第三方检测机构进行抽查，共发现22款APP及SDK存在侵害用户权益行为，涉及超范围收集个人信息、违规收集个人信息、信息窗口“摇一摇”乱跳转等问题，予以通报。上述APP及SDK应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）上海

12月23日，上海市通信管理局通报2024年第三批侵害用户权益行为的APP。上海市通信管理局近日组织第三方检测机构对本市移动互联网应用程序进行抽查，共发现29款APP及小程序存在侵害用户权益行为，予以通报。上述APP及小程序应按有关规定在12月31日前落实整改工作。整改落实不到位的，上海市通信管理局将依法依规组织开展处置工作。

(3) 浙江

12月23日，浙江省通信管理局通报2024年第12批侵害用户权益行为的APP。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即时通信、婚恋相亲、网络游戏等类型APP进行检查，并书面要求违规APP开发运营者限期整改。截止通报，尚有6款APP未按要求完成整改，予以通报。请上述APP开发运营者在2025年1月1日前完成整改落实工作，整改落实不到位的，浙江省通信管理局将视情采取下架、关停、行政处罚等措施。

(4) 江苏

12月24日，江苏省通信管理局通报2024年第5批侵害用户权益行为的APP。江苏省通信管理局近日组织第三方检测机构对群众关注的省内生活服务、休闲娱乐、实用工具等类型的APP进行检查，并通报相关违规APP主办者限期整改。截止通报，尚有27款APP未完成整改，予以通报。上述APP开发运营者在12月30日前完成整改，整改落实不到位的，江苏省通信管理局将视情采取下架、关停、行政处罚等措施。

(5) 广东

12月27日，广东省通信管理局公开通报4款未按要求完成整改APP，以及下架2款侵害用户权益APP。通报指出，因存在违规收集个人信息、超范围收集个人信息问题，怡亚通、索菲亚智能、花礼网鲜花、帮啦跑腿四款APP运营者被责令限期整改，但是截至目前尚未整改。上述四款APP应在2025年1月6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。通报还指出，扒圈、魔方直播助手两款APP存在违规收集个人信息、超范围收集个人信息、APP强制、频繁、

过度索取权限问题，经通报要求整改后，在规定时限内未按要求整改，因而被强制下架。

(6) 北京

12月30日，北京市通信管理局通报2024年第十二期问题APP。北京市通信管理局近日通过抽测发现北京市部分APP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”等侵害用户权益和安全隐患类问题。截至目前，尚有1款APP未整改或整改不到位，予以公开通报。2024年11月29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APP并要求整改。截至目前，仍有5款APP未整改或整改不到位，予以全网下架处置。（来源：工信部，北京市、上海市、浙江省、江苏省、广东省通信管理局）

2. 湖北省通信管理局组织开展工业领域网络和数据安全风险监测处置专项行动工作

11月29日，湖北省通信管理局印发通知，组织开展工业领域网络和数据安全风险监测处置专项行动工作，聚焦于湖北省工业领域，旨在整合各方资源，及时发现、有效处置工业领域网络和数据安全风险隐患，增强企业风险防范意识，提升企业风险应对能力，推动企业落实网络和数据安全主体责任，建立完善管理制度和防护措施，检验磨合网络和数据安全风险监测处置机制，锻炼相关单位风险监测处置能力，提升行业风险监测处置水平。

通知指出，本次专项行动的监测对象为湖北省内工业企业、工业互联网平台企业、工业互联网标识解析企业、车联网平台企业。通知强调，本次专项行动的重点任务：一是强化风险监测，二是深入分析研判，三是及时报送风险，四是加强通报处置。（来源：湖北省通信管理局）

3. 上海市通信管理局组织开展 2024 年度云服务安全专项治理工作

12月2日消息，上海市通信管理局近日成立专项工作组，对上海电信、上海移动、上海联通、上海有孚网络股份有限公司、行吟信息科技有限公司（上海）有限公司、上海携程商务有限公司开展云服务安全专项治理现场检查。

检查组依据此次专项行动治理方案细则，通过听取汇报、查阅台账、交流提问等方式，重点检查企业网络运行及云服务安全制度建设落实、风险隐患清单管理、平台监控及系统冗余保护能力建设、运行事故应急演练等方面工作情况，并对企业现场提交材料中发现的问题反馈改进要求。（来源：上海通信圈）

4. 浙江省通信管理局组织开展 2024 年“数安铸盾”数据安全应急演练

12月23日消息，浙江省通信管理局近日加强顶层谋划，系统提升数据安全水平，结合行业特色、数据特征等，组织浙江电信、浙江移动、浙江联通、华数集团、阿里云等5家基础电信企业及重点互联网企业，针对不同数据安全典型事件场景开展2024年“数安铸盾”应急演练。

此次演练采用场景模拟方式开展，分为事件研判分析、事件上报、事件预警通报、事件响应处置、处置确认、事件总结六个环节，各企业参与人员涉及 BOSS 运维团队、云网运维团队、安全团队、客户服务团队和业务团队。演练紧贴电信和互联网领域业务场景数据保护需求，设置各类实战应急场景。（来源：浙江省通信管理局）

5. 青海、贵州、宁夏通信管理局组织开展 2024 年基础电信企业网络与信息安全责任考核年终检查

（1）宁夏

12 月 3 日至 5 日，宁夏回族自治区通信管理局对区内 3 家基础电信企业开展网络与信息安全责任考核年终检查。检查组严格对照考核要点和评分标准，通过查阅资料、人员访谈、技术检测等方式，对各基础电信企业省公司网络安全防护、互联网信安系统运行、数据安全治理、防范治理电信网络诈骗、电信业务实名制基础管理、新技术新业务安全评估工作及地市公司数据安全保护措施、数据合作方管理等情况进行检查，并就中期检查问题整改情况进行“回头看”，各企业已按要求对中期检查发现的问题进行整改，网络和数据安全工作整体水平较上年提升明显。

（2）青海

12 月 9 日至 11 日，青海省通信管理局组织对省内 3 家基础电信企业省公司及市州分公司开展网络与信息安全责任考核年终检查。检查组严格对照考核要点和评分标准，通过听取汇报、查阅资料、访谈交流、技术检测等方式，对基础电信企业落实网络安全防护管理、数据安全治理、新技术

新业务安全评估、电信业务实名登记管理、防范治理电信网络诈骗、关键信息基础设施安全保护等工作情况进行检查，现场反馈检查发现的各类问题，要求各企业严格落实法律法规和制度规范，举一反三深入排查整治各类风险隐患，对标对表健全完善问题整改闭环管理机制。

(3) 贵州

12月10日至11日，贵州省通信管理局对省内各基础电信运营企业进行2024年网络与信息安全年终检查。本次检查着重对中期检查及落实《反电信网络诈骗法》专项检查中发现问题整改情况进行“回头看”，同时对全年网安其他工作进行检查。检查组通过查阅资料、实地查看、交流座谈等多种方式，对各企业的网络安全、数据安全、防范治理电信网络诈骗、涉卡涉用户信息安全及平安建设等方面工作进行全面认真核查。本次检查坚持问题导向和结果导向，对发现问题提出整改意见和建议。（来源：工信部）

(四) 其他部门治理实践

1. 最高检、公安部联合挂牌督办第四批特大跨境电信网络诈骗犯罪案件

12月1日消息，最高人民检察院、公安部近日决定继续联合挂牌督办第四批8起特大跨境电信网络诈骗犯罪案件，坚持深挖组织者、领导者及幕后“金主”，依法从重从快严厉打击跨境电信网络诈骗及境内关联违法犯罪活动，坚决维护社会稳定和人民群众切身利益。

此次联合挂牌督办的第四批 8 起特大跨境电信网络诈骗案件分别是：

(1) 江苏无锡“博翔园区”电信网络诈骗案；(2) 江苏盐城“巅峰科技”电信网络诈骗案；(3) 浙江嵊州“豪志园区”电信网络诈骗案；(4) 福建泉州“5·27”电信网络诈骗案；(5) 福建龙岩、重庆“盛源集团”电信网络诈骗案；(6) 重庆九龙坡“11·15”电信网络诈骗案；(7) 四川泸州“3·21”系列电信网络诈骗案；(8) 云南怒江“8·09”电信网络诈骗案。（来源：公安部）

2. 因违反数据安全管理制度等问题，江苏灌南农村商业银行股份有限公司被处罚

12月27日，中国人民银行连云港市分行披露一则行政处罚决定信息公示表。罚单显示，江苏灌南农村商业银行股份有限公司存在违反账户管理规定，违反数据安全管理制度，违反信用信息采集、提供、查询及相关管理规定，未按规定履行客户身份识别义务等七项违法违规行为。

基于此，江苏灌南农村商业银行股份有限公司被处警告，并处罚款 97.5 万元；时任公司信贷管理部总经理李某因对“违反信用信息采集、提供、查询及相关管理规定”的违规行为负有责任，被处罚款人民币 4.1 万元；时任公司运营管理部总经理杨某玉因对“未按规定履行客户身份识别义务、未按规定报送大额交易或者可疑交易报告”的违规行为负有责任，被处罚款人民币 4.5 万元。（来源：中国人民银行江苏省分行）

境外前沿观察：月度速览十则

导读：12月，联合国通过首个全球打击网络犯罪公约，规定刑事罪名，包括非法访问、非法拦截等和明确法人责任和自然人责任。欧盟《网络弹性法》正式生效，这是欧盟首部对包含数字元素产品的强制性网络安全立法文件，该法全面规定数字产品的网络安全要求、制造商和相关市场主体的责任义务，同时强化监管执行机制，覆盖数字产品从设计到淘汰的完整生命周期。美国总统拜登签署《2025财年国防授权法》，该法的两大要点是设立“首席数字工程招募与管理官”和提升人工智能系统的人机交互能力。韩国国会全体会议通过《旨在构建人工智能发展与信赖基础的人工智能基本法案》，主要内容包括建立韩国人工智能政策组织体系、推动韩国人工智能技术与产业发展、确保人工智能安全可靠等。

欧盟网络安全局发布首份欧盟网络安全状况报告《2024年欧盟网络安全状况报告》。报告指出，随着地缘政治和经济紧张局势加剧，网络战不断升级，间谍、破坏和虚假宣传活动成为各国操纵事件和获得战略优势的关键工具。美国管理和预算办公室发布《2024影响评估报告》，重点评估拜登政府期间，美国政府在网络安全、技术现代化、数字服务交付和人工智能方面取得的进展。美国网络安全公司Fortinet发布《2025年网络威胁趋势预测报告》，回顾2024年网络威胁，主要包括高级持续性网络犯罪数量激增、攻击者大肆收揽新颖TTP工具等；并预测2025年及未来网络威胁

趋势，主要包括攻击链专业化趋势显现、环境成网络攻击“重灾区”、暗网上自动化黑客工具增多等。

此外，美国财政部确认其多个工作站遭遇网络攻击，攻击源被归咎于高级持续性威胁行为者。攻击者利用盗取的密钥突破云服务安全，远程访问财政部多个用户工作站和非保密文件。苹果公司同意支付 9500 万美元以解决一项长达 5 年的隐私集体诉讼，该案件涉及苹果公司十多年来未经用户同意通过苹果手机和其他设备上的 Siri 虚拟语音助手非法录制用户私人 and 机密对话。爱尔兰数据保护委员会宣布其对 Meta 处以 2.51 亿欧元罚款，原因是 Meta 于 2018 年 9 月报告一起数据泄露事件后，DPC 经调查发现该公司密码存储做法违反欧盟《通用数据保护条例》。

关键词：网络安全、人工智能、网络犯罪、黑客攻击、数据泄露

1. 欧盟《网络弹性法》正式生效

12月10日，欧盟《网络弹性法》正式生效，这是欧盟首部对包含数字元素产品的强制性网络安全立法文件，标志着欧盟在增强网络安全保护和抵御网络威胁方面迈出重要步伐。该法共计8章71条，全面规定数字产品网络安全要求、制造商和相关市场主体责任义务，同时强化监管执行机制，覆盖数字产品从设计到淘汰的完整生命周期。

该法主要包括以下内容：（1）适用范围和网络安全基本要求。该法适用于具有数字元素的产品（简称“数字产品”），且其预期用途或合理可预见的使用范围涉及与设备或网络的直接或间接连接；（2）制造商、进口商和经销商责任。该法对各类运营者的网络安全责任进行规定。其中，运营者是指制造商、授权代表、进口商、经销商以及根据该法在数字产品的制造或者投放市场方面负有相关义务的其他自然人或法人；（3）自由和开源软件相关规定。该法明确，仅供非商业用途的开源软件和独立于数字产品的第三方云服务不在直接适用范围内，这为技术创新和开发提供一定的灵活性；（4）市场监管与处罚措施。该法要求欧盟成员国指定一个或多个市场监管机构，以确保该法有效实施。对于违反网络安全基本要求的，该法规定最高1500万欧元或公司上一财年全球年营业额的2.5%的罚款。（来源：欧盟委员会）

2. 韩国国会全体会议通过《旨在构建人工智能发展与信赖基础的人工智能基本法案》

12月26日，韩国国会全体会议正式通过《旨在构建人工智能发展与信赖基础的人工智能基本法案》。法案共5章43条，包括人工智能健康发展框架与信任基础建立、发展人工智能技术和培育产业、人工智能伦理与可信度等内容。

法案主要内容包括：（1）建立韩国人工智能政策组织体系。规定韩国应制定人工智能基本计划、设立国家人工智能委员会、建立人工智能政策中心、建立人工智能安全研究所以建立韩国人工智能政策组织体系来推动人工智能技术和产业的发展；（2）推动韩国人工智能技术与人工智能产业发展政策。规定鼓励人工智能企业、培养人工智能专业人才的相关政策，旨在通过对企业的支持和对人才的培育政策发展人工智能技术，振兴人工智能产业；（3）确保人工智能安全可靠。规定人工智能伦理原则、设立人工智能伦理委员会、人工智能安全性和可靠性检验与认证、人工智能透明度义务、安全性义务、高影响人工智能运营者义务等，以实现人工智能发展与安全可靠之间的平衡。（来源：数字治理全球洞察）

3. 联合国通过首个全球打击网络犯罪公约

12月27日，联合国官网发布由193个成员国通过的《联合国打击网络犯罪以及为打击利用信息通信技术系统实施的某些犯罪并共享严重犯罪电子证据而加强国际合作公约》。公约是继《联合国反腐败公约》20多年来

联合国以犯罪为主题的第一部国际法律文书，也是历史上首部具备普遍法律约束力的打击网络犯罪全球性国际公约。

公约共计九章六十八条，第二章规定了刑事定罪，包括非法访问、非法拦截、干扰信息通信技术系统、滥用设备、与信息通信技术系统有关的伪造、与信息通信技术系统有关的盗窃或欺诈、涉及网上儿童性虐待或儿童性剥削材料的犯罪、为对儿童实施性犯罪而进行教唆或诱骗、未经同意传播私密图像、对犯罪所得的洗钱行为等。公约明确法人责任和自然人责任，在不违反缔约国法律原则的情况下，法人责任可包括刑事责任、民事责任或行政责任。法人责任不得影响实施此类犯罪的自然人的刑事责任。

下一步，公约将于 2025 年在越南河内举行的正式仪式上开放签署，随后在纽约联合国总部开放公约供各国签署至 2026 年 12 月 31 日。公约将在第 40 个签署国批准 90 天后正式生效。（来源：联合国大会）

4. 美国总统签署《2025 财年国防授权法》

12 月 23 日，美国总统拜登签署《2025 财年国防授权法》。该法是美国国会每年通过的国防政策支柱性文件，将为国防部的运作项目提供计划并授权资金。

该法提及人工智能与军事科技方面，主要内容包括：拟投资 1438 亿美元用于研发、测试和评估投资高超音速、人工智能、机器人系统、移动微型核反应堆及高能激光技术，另有 17.5 亿美元用于科学与技术计划。该法

要求国防部启动多项试点项目和计划，以推动人工智能在国防领域的采纳和应用，既包括技术创新的探索，也涵盖对国家安全风险的预警机制。

该法的一大要点是设立“首席数字工程招募与管理官”，该官员负责明确国防部人工智能相关人员的职责分工；该法还要求国防部在该法生效后 180 天内开发针对部门成员的人工智能教育课程。该法的另一重点是提升人工智能系统的人机交互能力。通过引入认知工程技术，改善人工智能系统的可用性和数据解读效率，从而减少技术复杂性对战斗决策的干扰。最后，该法强调与盟友的多边合作。该法规定在 90 天内国防部需组建一个多边人工智能工作组，以协调盟国间的人工智能项目。（来源：新华网、复旦发展研究院）

5. 欧盟网络安全局发布《2024 年欧盟网络安全状况报告》

12 月 3 日，欧盟网络安全局(ENISA)发布首份欧盟网络安全状况《2024 年欧盟网络安全状况报告》。报告指出，2023 年 7 月至 2024 年 6 月期间欧盟面临的网络威胁级别为“相当高”。该报告旨在为欧盟层面的政策制定者提供欧盟、国家和社会层面网络安全状况和能力的概述，并提出政策建议，解决已发现的缺陷并提高整个欧盟的网络安全水平。报告指出，随着地缘政治和经济紧张局势加剧，网络战不断升级，间谍、破坏和虚假宣传活动成为各国操纵事件和获得战略优势的关键工具。

报告的重要发现包括：一是 DDoS 和勒索软件为最大威胁。DDoS 攻击和勒索软件攻击是最常见的攻击形式。报告指出勒索软件的主要攻击趋势包

括：（1）从加密到数据泄露的转变；（2）中小企业成为网络犯罪分子更具吸引力的目标；（3）双重勒索成为知名勒索软件团体的常态攻击形式；二是公共管理部门是受攻击最多的行业，报告期内共发生 1870 起网络事件，占总数的 19%；交通运输和金融业位居第二和第三，分别发生 1110 起和 890 起事件；三是网络间谍、虚假信息和雇佣黑客活动不断增加。根据 ENISA 对网络安全事件和网络威胁的分析，针对欧盟成员国和欧盟基本实体的网络间谍活动仍在持续，这些攻击主要来自与俄罗斯有联系的团体。（来源：欧盟委员会、安全内参）

6. 美国政府首席信息官办公室发布《2024 影响评估报告》

12 月 17 日消息，美国管理和预算办公室近日发布《2024 影响评估报告》，重点评估拜登政府期间，美国政府在网络安全、技术现代化、数字服务交付和人工智能方面取得的进展。

报告主要内容包括：（1）网络安全方面。自 2020 年 Solar Winds 网络攻击事件以来，美国总统发布 E014028 行政命令，要求联邦机构加强网络安全并采纳现代安全实践，如零信任。关键举措包括加强软件安全、多因素认证和加密、增强调查能力、持续监控、风险指导等；（2）技术和数据现代化方面。关键举措包括推进技术和数据现代化、推动零信任数据安全、开放数据；（3）人工智能方面。关键举措包括强调人工智能的重要性和组织政策框架、加大人工智能投资、成立首席人工智能官理事会、制定人工智能用例清单等。（来源：美国白宫）

7. 美国 Fortinet 公司发布《2025 年网络威胁趋势预测报告》

12 月 12 日消息，美国网络安全公司 Fortinet 近日发布《2025 年网络威胁趋势预测报告》，回顾 2024 年网络威胁，预测 2025 年及未来网络威胁趋势。

报告回顾 2024 年网络威胁，指出经典网络攻击手段持续升级，全球安全体系面临前所未有的考验。具体包括：（1）高级持续性网络犯罪数量激增；（2）攻击者大肆收揽新颖 TTP 工具；（3）人工智能成为网络犯罪分子的“得力助手”；（4）勒索软件攻击再升级，关键行业受损严重；（5）重大事件成网络犯罪“可乘之机”。

报告预测 2025 年网络威胁将更加复杂多变，主要包括：（1）攻击链专业化趋势显现，网络犯罪即服务市场崛起；（2）云环境成网络攻击“重灾区”；（3）暗网上自动化黑客工具增多，攻击门槛降低；（4）网络攻击与真实世界威胁“联手”等。

面对未来网络安全威胁，报告认为应当采取以下措施：（1）深化技术研发与创新，构建智能防御体系；（2）全面提升员工安全意识与技能；（3）建立健全应急响应与恢复机制；（4）深化国际合作，共同应对网络威胁。

（来源：网络安全和信息化）

8. 美国财政部工作站遭遇网络攻击

12 月 30 日，美国财政部确认其多个工作站遭遇网络攻击，攻击源被归咎于高级持续性威胁行为者。入侵行为通过第三方软件供应商 BeyondTrust

实施，该公司提供身份和访问管理服务；攻击者利用盗取的密钥突破云服务安全，远程访问了财政部多个用户工作站和非保密文件。财政部在接到 BeyondTrust 警告后立即采取行动，与网络安全和基础设施安全局、联邦调查局及其他执法部门合作进行调查。BeyondTrust 相关服务已下线，财政部表示没有证据显示攻击者仍能访问系统。根据《联邦信息安全和现代化法》，这些黑客攻击被归类为“重大事件”。（来源：网空闲话）

9. 苹果同意支付 9500 万美元和解苹果公司 Siri 窃听诉讼

12 月 31 日，Fumiko Lopez 等原告向美国加州北部地区法院奥克兰分院提交编号 4:19-cv-04577-JSW 案件的和解协议，意味着苹果公司同意支付 9500 万美元（约合人民币 6.95 亿），以解决一项长达 5 年的隐私集体诉讼。该案件涉及苹果公司十多年来未经用户同意，通过苹果手机和其他设备上的 Siri 虚拟语音助手非法录制用户私人和机密对话。

原告主张，即使没有试图通过触发词“嘿，Siri”来激活虚拟语音助手，也会发生录音且该对话随即被分享给广告商，试图将其产品推销给更多可能对其产品和服务感兴趣的消费者，这违背了苹果公司长期以来保护客户隐私的承诺。苹果公司虽与原告方达成和解，但并未承认提供服务时有任何不当行为。

下一步，和解协议仍需得到美国地区法官杰弗里·怀特的批准。该案的律师提议于 2025 年 2 月 14 日在奥克兰举行法庭听证会，以审查和解协议条款。如果和解协议获得批准，自 2014 年 9 月 17 日至 2024 年 12 月 31

日期间激活 Siri 的拥有苹果手机和其他苹果设备(最多限于五台苹果设备)的数千万消费者可以提出索赔，每位消费者每台配备 Siri 的设备最多可获得 20 美元的赔偿。（来源：classaction）

10. 因数据泄露影响约 2900 万 Facebook 账户，爱尔兰对 Meta 处以 2.51 亿欧元罚款

12 月 17 日，爱尔兰数据保护委员会（DPC）宣布对 Meta 处以 2.51 亿欧元罚款，原因是 Meta 于 2018 年 9 月报告一起数据泄露事件后，DPC 经调查发现该公司密码存储做法违反欧盟《通用数据保护条例》。

Meta 这起数据泄露事件影响全球约 2900 万 Facebook 账户，其中约 300 万账户位于欧盟经济区，受影响的个人数据类别包括用户的全名、电子邮件地址、电话号码、位置、工作地点、出生日期、宗教、性别、时间轴上的帖子、用户所属的群组以及儿童个人数据等。DPC 指出，这起泄露是由于未经授权的第三方在 Facebook 平台上利用用户令牌（user token）造成的，Meta 及其美国母公司在发现泄露不久后便修复了该问题。（来源：爱尔兰数据保护委员会）

行业前沿观察一：倾听 324 万份网民意见心声—— 2024 “安满周” 盛大举办；国家网信办就《网络信息 内容多渠道分发服务机构相关业务活动管理规定（草 案稿）》公开征求意见；《互联网平台企业涉税信息 报送规定》向社会公开征求意见

导读：12月21日上午，2024网民网络安全感满意度调查报告发布周（简称2024“安满周”）全国线上线下同步开幕，连续7天向全社会发布系列重磅网络安全感满意度调查报告和各类数据成果。

为规范MCN机构互联网信息内容相关业务活动，保障公民、法人和其他组织的合法权益，营造清朗网络空间，根据《中华人民共和国网络安全法》《未成年人网络保护条例》等法律法规，国家互联网信息办公室起草了《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》，向社会公开征求了意见。

为促进平台经济健康有序发展，国家税务总局会同国家市场监督管理总局研究起草了《互联网平台企业涉税信息报送规定（征求意见稿）》，向社会公开征求意见。

关键词：安满周、网络安全、未成年人网络保护条例、互联网

1. 倾听 324 万份网民意见心声——2024 “安满周” 盛大举办！发布《2024 年全国网民网络安全感满意度调查统计总报告》等数据成果

2024 年 12 月 21 日上午，2024 网民网络安全感满意度调查报告发布周（简称 2024 “安满周”）全国线上线下同步开幕，连续 7 天向全社会发布系列重磅网络安全感满意度调查报告和各类数据成果。作为本届“安满周”的重头戏，《2024 年全国网民网络安全感满意度调查统计总报告》（以下简称《总报告》）发布会于 12 月 22 日上午在北京成功举行，由调查活动组委会主任、公安部第一、三研究所原所长严明发布报告，公布 2024 年度网民网络安全感满意度指数以及相关主要调查发现。

在深入学习贯彻习近平总书记关于网络强国的重要思想和党的二十届三中全会精神热潮中，在全国各级党政有关部门的支持和指导下，2024 网民网络安全感满意度调查活动于 2024 年 7 月 17-26 日开展了样本采集工作，面向广大网民征求意见，最终共收获全国 34 个省（直辖市、自治区、特别行政区）超 324 万份问卷样本（主问卷+专题问卷）。

经过对这些调查数据进行整理、统计、分析后，编写形成了 2024 年度的全国总报告、专题报告、区域报告、分析报告等 170 多份调查报告和各类数据成果。

为进一步倾听、传达 324 万份网民意见心声，向国家有关部门开展网络空间安全治理提供详实的网情民意，活动组委会联合中国互联网协会、12321 网络不良与垃圾信息举报受理中心、中国教育技术协会网络安全专业

委员会、公安部第三研究所法律研究中心、密码科技国家工程研究中心、复旦大学、上海交通大学、浙江大学、西安电子科技大学、海南大学、广州大学、郑州大学、北京联合大学、粤港澳网络空间治理创新研究院、广州市大湾区现代产业发展研究院、乌镇数字文明研究院、互联网实验室、广州华南检验检测中心、国源天顺、长扬科技等专业权威机构及部分网安联成员单位等学术合作单位，集中一周时间，密集发布 2024 年调查活动各类成果报告、以及相关领域工作报告。

全国总报告发布，网民网络安全感满意度指数连续 6 年上升

《总报告》由活动承办单位广东新兴国家网络安全和信息化发展研究院基于 2024 调查活动总数据的分析研究编制形成。据《总报告》显示，2024 年网民网络安全感满意度指数为 75.179（2023 年版指数口径），迈上 75 分台阶，为较好偏好的水平。和 2023 年比较上升了 2.665，指数上升幅度明显。数据显示 2024 年度网民网络安全感满意度指数值跨上新的台阶，反映了 2024 年我国网络空间安全治理取得明显进展，网民的满意度评价有较大幅度的上升。

针对与群众人身财产安全紧密相关的网络诈骗问题，《总报告》数据显示，2024 年网络诈骗形势依然严峻，但公众防范与应对能力增强。参与调查的公众网民的网络诈骗遇见率前三位分别是“电话欠费、积分兑换、中奖诈骗”（遇见率 42.77%）、“贷款金融诈骗”（遇见率 38.83%）、“疫情诈骗圈套”（遇见率 27.23%）。网络诈骗活跃度仍处在较高的位置。

同时，公众对官方反诈服务渠道和平台的认知度在过去一年中实现了显著提升，最为显著的是对“国家反诈中心”APP的认知度，知晓选择率为68.10%，较2023年有大幅度上涨。其余渠道的知晓率也有所上升，“都不知道”的选择率下降了2.69个百分点。

网络社会迅猛发展，给中国社会带来巨变，也带来冲击。2024调查活动新增“网络社会发展的变化和冲击”热点专题，着重调查了当前网络社会的发展成就、变化感受、冲击挑战、存在问题、未来期望等问题。报告数据显示，中国互联网发展30年来，网民印象最深的前三个我国网络社会发展新成就分别是：网络强国战略提出（选择率57.03%）、网络空间治理取得成就（选择率54.23%）和网络基础设施建设水平提升（选择率53.63%），均超过50%的关注度。

经过对调查数据统计、汇总和分析，《总报告》中得出以下10大主要发现：一是网络安全治理成效显著，安全感满意度明显提升；二是网络法治建设效果显著，网络安全生态不断优化；三是网络犯罪打击初见曙光，公众防范能力稳步提升；四是网络诚信建设稳步前行，全面深化治理任重道远；五是个人信息保护仍需努力，数据安全提升有待深化；六是网购环境治理效果明显，维权意识与要求渐提高；七是网络权益保护效果凸显，数字鸿沟消除仍需加强；八是平台监管效果显著提升，企业自律仍需持续关注；九是数字政务治理好评上涨，网上服务覆盖仍需提高；十是网络强国战略成效显著，网民期望更多的获得感。

2024 网民网络安全感满意度调查报告发布周（安满周）由网民网络安全感满意度调查活动组委会指导，全国 135 家网络社会组织及相关机构（网安联）发起，全国 228 家网安联志愿服务机构及相关志愿服务团队联合发起，北京网络空间安全协会主办，广东新兴国家网络安全和信息化发展研究院、北京关键信息基础设施安全保护中心承办，于 2024 年 12 月 21-27 日以北京为主会场，上海、广州、杭州、郑州设置分会场，线上线下同步举办，连续 7 天向全社会发布系列重磅网络安全感满意度调查报告和各类数据成果。

有关党政主管部门领导、中国工程院院士、科研院所专家学者、网安联“网安之友”、网安专业技术人员、头部企业精英、社会组织代表、志愿服务团队代表、网民代表等 500 多位嘉宾出席大会，参与报告发布、报告解读、主题演讲和讨论等活动内容，共同呈现 2024 网民反映的网络安全问题，探讨新时代网络空间安全治理和监管，促进发展网络安全新质生产力，助力提升网民群众获得感、幸福感、安全感和满意度，服务国家网络安全和信息化工作高质量发展。

2. 国家网信办就《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》公开征求意见

国家互联网信息办公室关于《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》公开征求意见的通知。

为规范 MCN 机构互联网信息内容相关业务活动，保障公民、法人和其他组织的合法权益，营造清朗网络空间，根据《中华人民共和国网络安全法》《未成年人网络保护条例》等法律法规，国家互联网信息办公室起草了《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》，现向社会公开征求意见。

公众可将反馈意见通过电子邮件方式发送至：mcnjg@cac.gov.cn

意见反馈截止时间为 2025 年 2 月 9 日。

附件：网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）

国家互联网信息办公室

2025 年 1 月 10 日

网络信息内容多渠道分发服务机构

相关业务活动管理规定

（草案稿）

第一条 为规范网络信息内容多渠道分发服务机构互联网信息内容相关业务活动，保障公民、法人和其他组织的合法权益，营造良好网络生态，根据《中华人民共和国网络安全法》《未成年人网络保护条例》等法律法规，制定本规定。

第二条 在中华人民共和国境内运营的网络信息内容多渠道分发服务机构开展互联网信息内容相关业务活动，适用本规定。

本规定所称网络信息内容多渠道分发服务机构（MCN 机构）是指在网络信息内容服务平台入驻，为网络信息内容生产者提供策划、制作、营销、经纪等相关服务的机构。

第三条 网络信息内容多渠道分发服务机构开展互联网信息内容相关业务活动，应当遵守法律法规规定，坚持正确政治方向、舆论导向、价值取向，弘扬社会主义核心价值观，遵循公序良俗，遵守商业道德，维护良好网络生态。

第四条 网络信息内容服务平台应当要求在本平台开展互联网信息内容相关业务活动的网络信息内容多渠道分发服务机构办理入驻手续，重点审核以下事项：

（一）是否依法办理经营主体登记；

（二）是否设立内容管理负责人，有与业务范围和服务规模相适应的内容审核人员；

（三）是否有健全的内容安全、人员管理培训等制度。

第五条 网络信息内容服务平台应当在网络信息内容多渠道分发服务机构在本平台入驻之日起 10 个工作日内，向平台所在地省级网信部门办理备案登记手续。

备案登记信息发生变更的，网络信息内容服务平台应当自变更之日起 10 个工作日内，向平台所在地省级网信部门办理变更手续。

网络信息内容多渠道分发服务机构从事表演、节目等活动的，应当依法依规取得相关从业资格或服务资质。

第六条 网络信息内容服务平台应当加强本平台入驻网络信息内容多渠道分发服务机构的日常管理，定期组织机构学习法律法规和网络信息内容管理方面规章制度，及时通报有关部门工作要求。

网络信息内容服务平台应当制定并公开网络信息内容多渠道分发服务机构管理规则，以显著方式提醒告知机构需遵循的义务，同时网络信息内容生产者应当协助、配合机构履行本规定的相关义务。上述平台规则应当向网信部门报告。

第七条 网络信息内容服务平台应当根据网络信息内容多渠道分发服务机构合规情况、旗下账号数量及其粉丝总数量等指标维度，建立分级管理制度，并采取相应管理措施防范信息内容风险。

第八条 网络信息内容服务平台应当要求网络信息内容多渠道分发服务机构注册后台管理账号，并绑定旗下网络账号。在网络账号注册、拟变更账号信息等环节，要求网络信息内容生产者申报所属机构情况。

对于网络信息内容多渠道分发服务机构与网络账号之间的账号绑定、解绑等操作，网络信息内容服务平台应当强化审核、规范流程。

第九条 网络信息内容服务平台应当以显著方式，在网络账号信息页面展示该账号所属网络信息内容多渠道分发服务机构名称。

第十条 网络信息内容多渠道分发服务机构应在其签约的网络账号发布信息前，履行信息发布审核义务，进行合规审核，并留存审核记录备查。

网络信息内容生产者对其发布的信息内容负主体责任，对所属机构审核结果存在异议的，可以向网络信息内容服务平台提出申诉。

第十一条 网络信息内容多渠道分发服务机构不得违规操纵旗下网络账号，不得以任何形式允许第三方违规使用其后台管理账号或旗下网络账号。

第十二条 网络信息内容多渠道分发服务机构不得直接或组织、教唆、委托、协助签约的网络账号实施下列行为：

（一）以议题设置、合成伪造、臆测编造、拼凑剪接等方式，制造发布网络谣言；

（二）煽动网民情绪，故意引发群体对立，制造负面话题撕裂共识，扰乱网络秩序；

（三）集纳负面信息，翻炒旧闻旧事，蹭炒社会热点事件，误导公众；

（四）以附加标签、发布无关内容等方式，恶意蹭炒社会热点事件；

（五）渲染炒作突发案事件，消费灾难事故，违规展示违法犯罪行为细节；

（六）利用“网红儿童”牟利，包装、炒作未成年人，影响未成年人身心健康；

（七）宣扬不良价值观，传播不良生活方式，鼓吹低级趣味；

（八）编造虚假或引人误解的背景、情节、人设，进行恶意营销；

(九) 虚构关注度、浏览量、点击量、评价评分、投票量、消费金额等数据，通过人工方式或技术手段实施流量造假，批量发布同质化内容等网络水军行为；

(十) 组织对个人集中发布含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等网络暴力信息；

(十一) 违规开展互联网新闻信息服务；

(十二) 其他违反法律法规规定的行为。

第十三条 网络信息内容服务平台应当建立专门针对网络信息内容多渠道分发服务机构的举报通道，及时处理公众投诉举报。

网络信息内容服务平台应当将核查属实的投诉举报情况与网络信息内容多渠道分发服务机构进行关联记录，作为评价机构合规情况的依据。

第十四条 网络信息内容服务平台对于违反法律法规规定、平台规则和入驻协议的网络信息内容多渠道分发服务机构，依法依规采取警示提醒、限期改正、暂停营利权限、限制提供服务、入驻清退、纳入本平台黑名单等措施，并向网信部门报告。

网络信息内容服务平台发现网络账号存在违法违规行为的，应当依法依规处置网络账号所属机构。

第十五条 网信部门根据需要对网络信息内容服务平台、网络信息内容多渠道分发服务机构执行本规定情况开展监督检查。

网络信息内容服务平台、网络信息内容多渠道分发服务机构对网信部门依法实施的监督检查应当予以配合，提供必要数据、技术支持。

第十六条 对严重违法法律法规及本规定的网络信息内容多渠道分发服务机构，由网信部门依法依规纳入互联网黑名单，实现联动处置，网络信息内容服务平台在一定期限内不再为其办理入驻手续。

不履行本规定义务或履责不力的网络信息内容服务平台，由网信部门依据职责予以警告、通报批评、责令限期改正，整改期间可视情暂停平台网络信息内容多渠道分发服务机构入驻。

第十七条 网络信息内容多渠道分发服务机构违反本规定，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由网信等有关部门依据各自职责依照有关法律法规予以处理。

第十八条 本规定自 年 月 日起施行。

3. 《互联网平台企业涉税信息报送规定》向社会公开征求意见

为促进平台经济健康有序发展，国家税务总局会同国家市场监督管理总局研究起草了《互联网平台企业涉税信息报送规定（征求意见稿）》，近日向社会公开征求意见。

此规定根据《中华人民共和国电子商务法》《中华人民共和国税收征收管理法》等法律规定起草，旨在通过健全常态化涉税信息报送制度，有效维护法治公平税收秩序，对绝大部分行业及相关人群不会产生实质影响，合规经营企业更无需担忧。

近年来，我国平台经济迅速发展壮大，在扩内需、稳就业、惠民生等方面发挥重要作用。互联网平台企业汇聚着平台内经营者和从业人员的身份信息和收入信息。按照《中华人民共和国电子商务法》第二十八条规定，互联网平台企业应当依照税收征收管理法律、行政法规的规定，向税务部门报送涉税信息。

规定与电子商务法有效衔接，进一步规范互联网平台企业向税务机关报送平台内的经营者和从业人员涉税信息，并对涉税信息谁来报、报什么、怎么报等事项作出明确规定。规定特别强调，从事配送、运输、家政等便民劳务活动的从业人员收入信息可不报送。

根据规定，互联网平台企业应当在季度终了的次月纳税申报期内，向主管税务机关报送平台内的经营者和从业人员上季度汇总的相关收入信息，对于规定施行前的存量收入信息则无需报送。税务部门将对获取的涉税信息依法保密，按照有关规定建立涉税信息数据安全管理制度，确保数据安全。

同时，规定还明确了减轻平台企业信息报送负担、保障信息安全和质量以及法律责任等方面内容，对工信、人社和市场监管等部门与税务部门共享的涉税信息，互联网平台可不重复报送。税务机关将为互联网平台企业报送涉税信息提供安全可靠的渠道和便捷高效的服务。

对良好税收秩序的有效维护，就是对守法经营者最好的保护。国家税务总局征管和科技发展司负责人介绍，2022年以来，税务部门已在天津、江西、湖北、湖南、广东等5省市试点开展网络销售、网络直播等互联网

平台企业按季报送涉税信息，参与试点的平台及平台内商户和从业人员普遍感受到“三不变、一变化”。

“三不变”是指互联网平台企业只需依法履行报送涉税信息的程序性义务，其自身经营情况和税收负担不会因此发生变化；平台内合规经营的广大经营者和从业人员，税收负担不会因此发生变化；绝大部分小微企业和商户税负不会发生变化，因为商户月销售额不超过10万元可享受增值税免税优惠政策，综合所得年收入不超过12万元的平台内从业人员，在享受各项扣除后，也基本无需缴纳个人所得税或仅需缴纳少量税款。

“一变化”是指少部分存在虚假申报、偷逃税等行为的经营者，特别是不合规经营的高收入者，其违法行为将因此得到有效遏制，税负会回归正常水平。

规定的征求意见时间为2024年12月20日至2025年1月19日，公众可以通过登录国家税务总局网站、邮寄信函等方式提出意见建议。（来源：新华网）

行业前沿观察二：各地协会动态

导读：各地协会活动精彩纷呈，召开发布会、交流会等活动。广东省网络空间安全协会举行信创赋能（第五期）——“信创适配技术交流与推广：共筑数字经济安全基石”活动；北京网络空间安全协会召开人工智能专委会（筹）专家咨询会议；甘肃省商用密码行业协会捐款4万余元驰援西藏抗震救灾；重庆信息安全产业技术创新联盟成功举办2025年网络安全技术沙龙暨联盟两长工作会议；可信联盟基础平台专业委员会召开换届工作会议；海南省网络安全和信息化协会与海口市广告协会联合举办网络安全与法律培训活动等。

关键词：大讲堂、信创大赛、技能竞赛、网络安全、信息安全

1. 广东省网络安全协会举行信创赋能（第五期）——“信创适配技术交流与推广：共筑数字经济安全基石”活动

为积极响应国家创新驱动发展部署，促进信创产品与应用场景的深度融合与适配，提升行业智能化与国产化水平，2025年1月9日下午，由广东省网络安全协会、广州网络安全协会联合主办的信创赋能（第五期）——“信创适配技术交流与推广：共筑数字经济安全基石”活动在协会报告厅举行，华南信创适配认证中心副主任吴一丰、成珍苑，广东省网络安全协会秘书长周贵招、副秘书长兼职称办主任蔡舒婷以及会员单位代表等人员参加活动。

此次活动搭建了双方常态化沟通交流平台，使参与者对信创领域的产品革新、技术创新、标准升级、市场需求和应用场景有了更为透彻地理解，为推动信创产业不断向前发展，助力广东高质量发展贡献力量。

2. 北京网络安全协会召开人工智能专委会（筹）专家咨询会议

2025年1月8日下午15时，北京网络安全协会隆重召开人工智能专业委员会（筹）专家咨询会议。协会理事长黄丽玲、人工智能专委会筹备组负责人方楠等协会领导出席会议，邀请了国家信息中心国信研究院人工智能安全中心秘书长杨绍亮，中央广播电视总台技术局技术规划研究部主任、教授级高工辛威，中国移动研究院原院长、教授级高工刘涛，贵州

大数据安全工程研究中心主任杜跃进，中国指挥与控制学会网络安全专委会副主任刘毅，武警特警学院原副院长、教育长朱文军，北京邮电大学互联网治理与法律研究中心研究员许运红，国投智能股份公司党委书记申强，国投智能股份公司人工智能安全首席专家金辉，北京天融信网络安全技术有限公司高级副总裁、高级工程师景鸿理，启明星辰信息安全技术公司高级工程师杨天识，科大讯飞公共安全业务部行业总监束和平，一点资讯党委书记王营涛，北京天空卫士网络安全技术有限公司研发副总裁柳赛普等专家参与讨论。

此次会议旨在进一步优化专委会的工作机制，广泛倾听来自各方的宝贵意见，凝聚行业内的智慧与力量，共同推动人工智能安全领域的创新与发展。

3. 甘肃省商用密码行业协会捐款 4 万余元驰援西藏抗震救灾

1月7日9时5分，西藏日喀则市定日县发生6.8级地震，造成重大人员伤亡。为贯彻落实党中央、国务院对定日县抗震救灾工作指示精神，甘肃省商用密码行业协会于1月7日晚紧急开设捐赠专用通道，向广大会员发起抗震救灾爱心捐赠活动，截止1月10日，会员单位及个人会员累计捐款44100元。目前，协会已将善款拨付至西藏日喀则市慈善总会，用于地震灾区的民众救助和灾后重建。

山河无恙，众志成城。后续，甘肃省商用密码行业协会将持续关注抗震救灾形势，积极履行社会责任，多措并举捐献爱心，与灾区人民共渡难关。

4. 重庆信息安全产业技术创新联盟成功举办 2025 年网络安全技术沙龙暨联盟两长工作会议

1 月 8 日，由重庆信息安全产业技术创新联盟、重庆计算机安全学会主办，重庆信安网络安全等级测评有限公司、绿盟科技集团股份有限公司、重庆奇安信科技有限公司、重庆市合川区网络安全学会协办的 2025 年网络安全技术沙龙暨联盟两长工作会议圆满举行。

此次活动汇聚了众多网络安全领域的专家、企业代表，共同探讨数字安全面临的前所未有的挑战、AI 应用于网络安全的前景、如何通过 AI 赋能安全运营等方面的问题。

5. 可信联盟基础平台专业委员会召开换届工作会议

2025 年 1 月 8 日，中关村可信计算产业联盟（以下简称：可信联盟）基础平台专业委员会换届暨第三届第一次会议在北京召开。换届会议由可信联盟副秘书长周文颖主持，可信联盟党支部书记、秘书长刘达、副秘书长王年出席会议。参会单位有，北京可信华泰信息技术有限公司、华为技术有限公司、北京工业大学可信计算北京市重点实验室、北京旋极安辰计算科技有限公司、海光信息技术股份有限公司、天津国芯科技股份有限公

司、北京启明星辰信息安全技术有限公司、江苏云涌电子科技股份有限公司、威尔创新（天津）科技发展有限公司、北京兴汉网际股份有限公司、管芯微技术（上海）有限公司、北京同创安全可信科技有限公司、飞腾信息技术有限公司、湖南麒麟信安科技股份有限公司。

会议依据可信联盟章程及专业委员会管理办法，经投票选举产生了新一届领导班子，北京可信华泰信息技术有限公司荣任主任单位，华为技术有限公司和北京工业大学可信计算北京市重点实验室当选为副主任单位。北京可信华泰信息技术有限公司首席技术官田健生博士发表当选感言，表示要团结成员单位共同努力，为推动可信计算产业发展贡献力量。各成员单位纷纷发言，在简单介绍本单位优势资源的同时，对专委会工作提出建议。

6. 海南省网络安全和信息化协会与海口市广告协会联合举办网络安全与法律培训活动

1月8日下午15时，由海口市广告协会与海南省网络安全和信息化协会联合举办2025海南户外广告网络安全与法律培训活动，在正邦网络空间安全共同体成功举行。

通过本次网络安全与法律培训活动，参会的相关企业代表们收获颇丰，对网络安全与法律意识有一定提升，为行业的健康发展注入新的活力与动力。

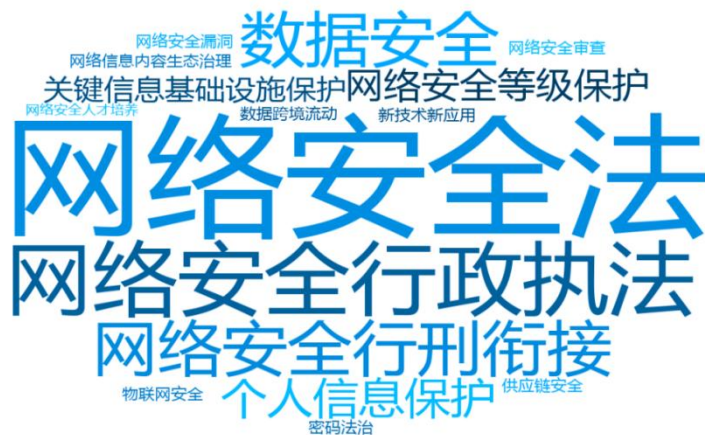
公安部第三研究所网络安全法律研究中心

2016年2月，公安部第三研究所正式成立“网络安全法律研究中心”。中心成立以来，聚焦前瞻性研究，切实践行理论与实践与立法实践深度结合，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用发展及安全风险，并持续推动科研成果应用于网络安全相关立法活动，在国内网络安全法律方面的影响力逐步提升。同时投身警务实践活动和公安一线服务，为公安部门提供立法动态研判和决策研究支撑。

基础性

专业性

针对性



推动立法、服务实务、智库支撑



联系方式

电子邮箱: cslaw@gass.ac.cn

咨询电话: 王老师 18817309169

网络与数据安全法律合规咨询服务

提供《网络安全法》《数据安全法》《密码法》《个人信息保护法》及配套制度为核心的数据安全保护合规体系建设，包括但不限于帮助企业落实网络安全等级保护、关键信息基础设施安全保护、网络安全审查、数据出境安全风险评估、数据交易安全保障、安全事件应急处置等要求。开展个人信息、重要数据、核心数据等数据安全合规自查、合规差距性分析，发现、识别、分析、研判、控制数据收集、存储、使用、加工、传输、提供、公开等全生命周期的法律风险，提供法律意见和整改建议。

数据安全合规体系构建



为企业提供网络安全漏洞发现与披露、漏洞扫描与渗透测试等安全测试、“白帽子”与众测等业务场景下的合规体系构建，帮助企业厘清行为边界，避免经营风险。

安全测试法律合规体系构建



开展情况调研，评估拟出境活动风险，发现安全风险并提供整改建议，根据客户整改落实情况，出具数据出境安全风险评估报告。

数据出境安全风险评估咨询服务



帮助企业构建事先防范网络安全、数据安全行政与刑事风险框架，指导企业如何正确配合监督检查、理解执法要求等。

网络安全、数据安全执法调查与刑事风险的防范与处置意见



针对《个人信息保护法》第五十五条规定的个人信息处理情形，帮助企业开展个人信息保护影响评估，履行个人信息保护义务。

个人信息保护影响评估/合规审计咨询服务



结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

网络安全、数据安全法律法规专业培训



数据出境安全风险评估咨询服务

近年来，我国在国家数据安全和个人信息保护的顶层设计布局下，加快数据出境相关立法，数据出境规则体系不断完善，数据出境安全评估成为数据出境的重要路径。2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》，落实《网络安全法》《数据安全法》《个人信息保护法》上位法要求，明确数据出境安全评估相关规定。在此形势下，企业普遍面临出境数据识别难、出境风险评估难、申报材料填报难等难题。为帮助企业解决以上难题，及时履行数据出境安全评估申报义务，公安部第三研究所网络安全法律研究中心特推出**数据出境安全风险评估咨询服务**。

数据出境活动

1

境内运营中收集和产生的数据传输、存储至境外



2

数据存储在国内，境外的机构、组织或者个人可以访问或者调用



数据出境安全风险评估咨询服务流程

1 - 3 周

周期视情况而定

01 情况调研

02 风险评估

03 指导落实
整改

04 出具风险
评估报告



3 - 5 周



1 - 2 周

- 开展合规差距分析
- 识别安全风险并划定风险等级
- 针对安全风险提供整改建议

- 结合客户落实整改情况，出具《数据出境风险评估报告》

合规咨询服务项目

中心已为互联网、银行、服装、签证、传统制造业等分属不同行业类别的企业提供APP合规咨询、个人信息保护（隐私政策）评估、个人信息保护合规整改、数据出境安全风险自评等方面的合规咨询服务，合规咨询服务能力得到客户一致认可。

典型项目

- 某互联网公司APP合规咨询
- 某银行个人信息保护（隐私政策）评估
- 某跨国服装零售企业个人信息保护合规整改
- 某签证跨国集团数据出境安全风险评估咨询
- 某传统制造业跨国集团数据出境安全风险评估咨询

.....

