



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)

2024年5月第5期 (总第10期)

2024年5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网安联发展工作委员会

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

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

吴晓文 安徽省计算机信息网络安全协会

刘长久 湖北省网络安全协会 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 常务副秘书长

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 会长
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 王彩玉 王明一 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。

目 录

境内前沿观察一：安全事件	1
1. 中国人民解放军信息支援部队成立	2
2. 2024年中非互联网发展与合作论坛发布关于中非人工智能合作 的主席声明	3
3. 2024年全国数据工作会议在京召开	4
境内前沿观察二：政策立法	6
（一） 部委层面动向	8
1. 九部门印发《加快数字人才培育支撑数字经济发展行动方案 （2024—2026年）》	8
2. 国家数据局发布《深化智慧城市发展 推进城市全域数字化转 型的指导意见（征求意见稿）》	9
3. 国家市场监管总局印发《市场监督管理行政执法电子数据取证 暂行规定》	10
4. 公安部发布《公共场所视频图像信息系统管理条例（征求意见 稿）》	11
5. 三部门印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》	12
6. 商务部印发《数字商务三年行动计划（2024—2026年）》 ..	12
7. 工信部发布 2024 年规章制定工作计划	13

8. 国家发展改革委办公厅、国家数据局综合司印发《数字经济2024年工作要点》	13
9. 全国网安标委印发《全国网络安全标准化技术委员会 2024 年度工作要点》	14
10. 全国网安标委发布七项国家标准征求意见稿	15
(二) 地方层面动向	15
1. 浙江省杭州市印发《杭州市智能网联车辆测试与应用促进条例》	15
2. 浙江省杭州市发布《杭州市数据流通交易促进条例（草案）》	16
3. 海南省印发《海南省公共互联网网络安全威胁监测与处置办法》	17
4. 北京市印发《北京市加快建设信息软件产业创新发展高地行动方案》	18
5. 江苏省印发《江苏省算力基础设施发展专项规划》	19
6. 福建省印发《福建省一体化大融合行政执法平台管理暂行办法》	20
境内前沿观察三：治理实践	22
(一) 公安机关治理实践	24
1. 公安机关打击整治网络谣言专项行动取得阶段性成效	24

2. 浙江杭州警方通报打击整治网络谣言、网络暴力专项行动推进情况.....	25
3. 上海警方通报打击整治网络谣言专项行动措施成效.....	25
4. 因未落实业主个人信息保护义务，甘肃 10 家物业公司被处罚	26
5. 陕西西安警方成功打击一起非法出售公民个人信息案件...	26
6. 北京警方成功侦破一起利用黑客手段“开盒”曝光个人信息的网络犯罪案件.....	27
7. 山西长治警方成功破获特大侵犯公民个人信息案.....	28
8. 江西上饶警方成功破获一起利用短视频平台引流推广色情 APP 的非法利用信息网络案件.....	29
9. 山东青岛警方破获一起特大非法利用信息网络案.....	29
（二）网信部门治理实践.....	30
1. 中央网信办部署开展“清朗·整治‘自媒体’无底线博流量”专项行动.....	30
2. 中央网信办部署开展“清朗·打击违法信息外链”专项行动	31
3. 国家互联网信息办公室发布生成式人工智能服务已备案信息	32
4. 国家互联网信息办公室发布第二批应用程序分发平台备案编号.....	32
5. 北京市网信办启动“清朗·E 企护航”专项整治行动.....	33
6. 江西南昌西湖区网信公安两部门联合依法约谈企业负责人	34

7. 江西南昌网信办依法对微信小程序“查成交价”运营主体作出行政处罚.....	35
(三) 通信管理部门治理实践.....	35
1. 广东、浙江、北京通信管理部门通报存在问题的 APP.....	35
2. 浙江省通信管理局部署防范治理电信网络诈骗工作.....	37
(四) 其他部门治理实践.....	38
1. 上海临港新片区数据跨境服务中心启用运营.....	38
2. 杭州互联网法院审理一起非法买卖、使用新生儿信息案件.....	39
3. 北京第四中级人民法院：词典 APP 附加功能违规收集个人信息构成侵权.....	40
4. 国家计算机病毒应急处理中心监测发现 10 款违规移动应用	41
境外前沿观察：月度速览十则	43
1. 联合国发布《全球数字契约：零案文》，为后续政府间磋商提供讨论基础.....	44
2. 美国总统拜登签署一揽子立法，《TikTok 剥离法》成为法律	44
3. 美国总统拜登签署《关于关键基础设施安全与韧性的国家安全备忘录》.....	45
4. 美国 FCC 发布《安全原则：系统性解决安全漏洞》.....	45
5. 德国联邦信息安全办公室发布指南《生成式人工智能模型：行业和政府部门的机遇和风险》.....	46

6. 英国《2022 年产品安全和电信基础设施法》及相关条例生效， 强化联网设备供应链安全管理	47
7. 英国政府发布《2024 年网络安全漏洞调查》	47
8. 美国市政监管机构遭遇美杜莎网络犯罪团伙勒索攻击	48
9. 美国司法部服务提供商数据泄露，导致 34 万多人数据被盗	48
10. 虚假 Facebook、MidJourney、OpenAI 页面向百万人推广恶意 软件	49
行业前沿观察一：2023《特殊人群（未成年人、老年人等）网络权益 保护专题报告》发布、工信部公示 2024 年度制造业新型技术改造城市试点 名单、工业互联网一体化进园区“百城千园行”活动开启	50
1. 聚焦特殊人群数字化应用！2023《特殊人群（未成年人、老年 人等）网络权益保护专题报告》发布	52
2. 工信部公示 2024 年度制造业新型技术改造城市试点名单 ...	61
3. 工信部：工业互联网一体化进园区“百城千园行”活动开启	62
行业前沿观察二：各地协会动态	66
1. 信创赋能（第三期）——“走进科大讯飞·探索中国智能先驱 者”顺利举办	67
2. 北京网络空间安全协会作为承办单位入列“国家专业技术人才 知识更新工程 2024 年高级研修项目计划”	68
3. “巴渝杯”大学生网络安全联赛——理论知识竞赛、CTF 夺旗竞 赛成功举办！	69

4. 大连市信息网络安全协会发布“大连市信息网络安全协会组建专家库”的通知背景与目的.....	70
5. 徐州网络公共安防技术协会召开无人机分会筹备会议.....	70
6. 东莞市信息技术联合会举行新一代信息技术新媒体运营中心授牌仪式.....	72

境内前沿观察一：安全事件

导读：4月，中国人民解放军信息支援部队成立。习近平主席在训词中强调信息支援部队是全新打造的战略性兵种，是统筹网络信息体系建设运用的关键支撑，在推动我军高质量发展和打赢现代战争中地位重要、责任重大。要有力支撑作战，坚持信息主导、联合制胜，畅通信息链路，融合信息资源，加强信息防护，深度融入全军联合作战体系，精准高效实施信息支援，服务保障各方向各领域军事斗争。

此外，2024年全国数据工作会议在京召开。会议总结2023年工作情况，安排部署2024年重点工作。会议指出，2024年将围绕健全数据基础制度、提升数据资源开发利用水平、以数字化赋能高质量发展、促进数据科技创新发展、优化数据基础设施布局、强化数据安全保障能力、提升数据领域国际合作水平、发挥试点试验引领作用八个方面开展工作。将大力发展数字经济，提升数字化公共服务水平。围绕技术发展加快产业布局，形成数据科技与数据产业相互融合、相互促进的良性发展态势；同时，始终紧绷数据安全这根弦，提升数据安全的技术保障水平。

关键词：中国人民解放军信息支援部队、全国数据工作会议、中非人工智能合作主席声明

1. 中国人民解放军信息支援部队成立

4月19日，中国人民解放军信息支援部队成立大会在北京八一大楼隆重举行。

中共中央总书记、国家主席、中央军委主席习近平向信息支援部队授予军旗并致训词。习近平指出，调整组建信息支援部队，是党中央和中央军委从强军事事业全局出发作出的重大决策，是构建新型军兵种结构布局、完善中国特色现代军事力量体系的战略举措，对加快国防和军队现代化、有效履行新时代人民军队使命任务具有重大而深远的意义。

习近平强调，信息支援部队是全新打造的战略性兵种，是统筹网络信息体系建设运用的关键支撑，在推动我军高质量发展和打赢现代战争中地位重要、责任重大。要坚决听党指挥，全面贯彻党对军队绝对领导的根本原则和制度，全面加强部队党的建设，坚定理想信念，严肃纪律规矩，弘扬优良作风，确保部队绝对忠诚、绝对纯洁、绝对可靠。要有力支撑作战，坚持信息主导、联合制胜，畅通信息链路，融合信息资源，加强信息防护，深度融入全军联合作战体系，精准高效实施信息支援，服务保障各方向各领域军事斗争。要加快创新发展，坚持作战需求根本牵引，加强体系统筹，推进共建共享，强化科技创新，建设符合现代战争要求、具有我军特色的网络信息体系，高质量推动体系作战能力加速提升。要夯实部队基础，落实全面从严治军要求，严格教育管理，保持正规秩序，激发动力活力，全

面锻造过硬基层，确保部队高度集中统一和安全稳定，奋力开创部队建设新局面，坚决完成党和人民赋予的各项任务。

根据中央军委决定，新组建的信息支援部队由中央军委直接领导指挥，同时撤销战略支援部队番号，相应调整军事航天部队、网络空间部队领导管理关系。（来源：央视新闻）

2. 2024 年中非互联网发展与合作论坛发布关于中非人工智能合作的主席声明

4月2日至3日，2024年中非互联网发展与合作论坛举行，就中非人工智能合作开展深入交流，并发布主席声明。

声明指出，人工智能是人类发展新领域。当前，全球人工智能技术快速发展，对经济社会发展和人类文明进步产生深远影响，给世界带来巨大机遇。

声明呼吁中非加强政策对话与沟通、推动技术研发与应用、促进产业合作与发展、开展人才交流与能力建设、筑牢网络和数据安全屏障。其中，中非应加强在联合国等多边框架下的协调与合作，增强发展中国家在人工智能全球发展与治理中的代表性和发言权，支持联合国发挥主渠道作用，成立人工智能国际治理机构。中非支持《全球人工智能治理倡议》，深化网络和数据安全领域的合作，共同推动网络安全技术和产品的研发与应用，打造可审核、可监督、可追溯、可信赖的人工智能技术。共同防范人工智

能技术滥用和网络攻击，保障人工智能研发和应用中的个人隐私与数据安全。（来源：中国网信网）

3. 2024 年全国数据工作会议在京召开

4 月 1 日，2024 年全国数据工作会议在北京召开。会议梳理总结前一阶段工作情况，安排部署 2024 年重点工作。

会议对 2023 年各项工作进行全面总结：一是党对数据工作的领导全面加强。认真贯彻新时代党的建设总要求，把党的全面领导贯穿数据工作全过程、各领域；二是数据工作体系初步成型。落实党和国家机构改革要求，高效推进机构筹建；三是数据要素市场化配置改革加快破局。以数据要素市场化配置改革为主线，加强基础制度建设，发挥数据要素乘数效应，扎实开展数据资源调查；四是统筹数字化发展力度稳步增强。开展数字中国、数字经济和数字社会发展情况评估；五是数据基础设施建设有力推进。持续实施“东数西算”工程，制定加快构建全国一体化算力网的实施意见，开展数据基础设施布局研究；六是数据领域开放合作进一步拓展。成功举办第三届“一带一路”国际合作高峰论坛数字经济高级别论坛，与 14 个国家共同发布《“一带一路”数字经济国际合作北京倡议》，积极推进数字经济多双边国际合作。

会议部署 2024 年工作重点：一要健全数据基础制度。建立健全数据产权制度，制定促进数据合规高效流通和交易的政策；二要提升数据资源开发利用水平。发挥公共数据资源开发利用的示范效应，持续探索企业数据、

个人数据开发利用新路径；三要以数字化赋能高质量发展。加快数字中国建设，大力发展数字经济，提升数字化公共服务水平；四要促进数据科技创新发展。围绕技术发展加快产业布局，形成数据科技与数据产业相互融合、相互促进的良性发展态势；五要优化数据基础设施布局。加快全国一体化算力网和数据流通基础设施建设，发挥好政府投资的放大效应；六要强化数据安全保障能力。始终紧绷数据安全这根弦，提升数据安全技术保障水平；七要提升数据领域国际合作水平。统筹做好数字经济领域国际合作，完善国际数字治理“中国方案”，持续优化数据跨境流动规则；八要发挥试点试验的引领作用。鼓励有条件的地方先行先试，支持更多地方因地制宜加快发展。（来源：国家数据局）

境内前沿观察二：政策立法

导读：4月，国家部委和地方立法的关注点较为多元，涉及数字人才培养、智慧城市建设、行政执法电子数据取证、行政执法平台管理、数字经济发展、公共场所视频图像信息系统管理、智能网联汽车管理等诸多方面。

具体来说，人力资源社会保障部等九部门联合印发《加快数字人才培养支撑数字经济发展行动方案（2024—2026年）》，提出用3年左右时间，扎实开展数字人才育、引、留、用等专项行动。行动方案要求持续发布数字职业，动态调整数字职称专业设置。支持各地根据行业发展需要增设人工智能、集成电路、大数据、工业互联网、数据安全等数字领域职称专业。

提升行政执法能力方面，国家市场监管总局印发《市场监督管理行政执法电子数据取证暂行规定》，聚焦行政执法过程中的电子数据取证环节，明确市场监督管理部门可以利用互联网信息系统或者设备收集、固定电子数据。对网络违法行为的技术监测记录资料，可以作为实施行政执法的电子数据证据。电子数据证据存储应当依据《保守国家秘密法》《数据安全法》等法律法规规定，实施安全与保密管理。此外，福建省人民政府印发《福建省一体化大融合行政执法平台管理暂行办法》，将打造省行政执法信息化综合应用平台，即“闽执法”平台。该平台将根据工作需求实现与国家部委行政执法系统、省级执法相关公共服务平台互联互通。该平台投入使用后，行政执法机关不再新建行政执法系统，已建行政执法系统不再单独申请政务云资源，对接平台应用需求的除外。

国家标准推进方面，全国网络安全标准化技术委员会印发 2024 年度工作要点，表示将尽快研制出台关键信息基础设施边界确定方法、安全能力指标体系、测评方法等急需标准，启动关键信息基础设施主动防御、监测预警等标准研制。加快研制软件物料清单数据格式、网络弹性评价准则等标准。

关键词：数字人才培育、电子数据取证、行政执法平台、关键信息基础设施国家标准

（一）部委层面动向

1. 九部门印发《加快数字人才培养支撑数字经济发展行动方案（2024—2026年）》

4月2日，人力资源社会保障部、中共中央组织部、中央网信办、国家发展改革委等九部门联合印发《加快数字人才培养支撑数字经济发展行动方案（2024—2026年）》，发挥数字人才支撑数字经济的基础性作用，加快推动形成新质生产力，为高质量发展赋能蓄力。

行动方案明确总体要求，提出要以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大精神，落实中央人才工作会议部署，坚持党管人才原则，坚持创新引领和服务发展，坚持需求导向和能力导向，紧贴数字产业化和产业数字化发展需要，用3年左右时间，扎实开展数字人才育、引、留、用等专项行动，提升数字人才自主创新能力，激发数字人才创新创业活力，增加数字人才有效供给，形成数字人才集聚效应，着力打造一支规模壮大、素质优良、结构优化、分布合理的高水平数字人才队伍，更好支撑数字经济高质量发展。

行动方案提出六项重点任务：1. 实施数字技术工程师培育项目；2. 推进数字技能提升行动；3. 开展数字人才国际交流活动；4. 开展数字人才创新创业行动；5. 开展数字人才赋能产业发展行动；6. 举办数字职业技术技能竞赛活动。其中，行动方案要求重点围绕大数据、人工智能、智能制造、集成电路、数据安全等数字领域新职业，以技术创新为核心，以数据赋能

为关键，制定颁布国家职业标准，开发培训教程，分职业、分专业、分等级开展规范化培训、社会化评价，取得专业技术等级证书的可衔接认定相应职称。在项目实施基础上，构建科学规范培训体系，开辟数字人才自主培养新赛道。

行动方案还围绕优化培养政策、健全评价体系、完善分配制度、提高投入水平、畅通流动渠道、强化激励引导提出六项政策保障措施。要求持续发布数字职业，动态调整数字职称专业设置。支持各地根据行业发展需要增设人工智能、集成电路、大数据、工业互联网、数据安全等数字领域职称专业。（来源：人力资源社会保障部）

2. 国家数据局发布《深化智慧城市发展 推进城市全域数字化转型的指导意见（征求意见稿）》

4月2日，国家数据局发布《深化智慧城市发展 推进城市全域数字化转型的指导意见（征求意见稿）》。

征求意见稿提出坚持系统推进、整体谋划；因地制宜、分级分类；以人为本、协同高效；场景牵引、数据驱动；改革创新、全域赋能；安全发展、可信可控六项基本原则；围绕全领域推进城市数字化转型、全方位增强城市数字化转型支撑、全过程优化城市数字化转型生态三方面提出十二项举措。

安全方面，征求意见稿要求提升城市安全韧性水平。加强城市物理空间安全管理和安全风险态势感知，强化应急广播等城市安全风险预警信息发布手段，围绕“高效处置一件事”，完善城市常态事件和应急事件分类

处置流程，打破城市管理条块分割和信息壁垒，构建全链条、全环节联动应急处置体系，实现弹性适应、快速恢复。加强城市数字空间安全管理，健全完善网络安全监测预警和应急处置机制，构建城市网络运行安全管理体系，提升通信网络韧性。加快推进城市数据安全体系建设，依法依规加强数据收集、存储、使用、加工、传输、提供、公开等全过程安全监管，落实数据分类分级保护制度，压实数据安全主体责任。推进建设有韧性的城市数据可信流通体系，健全数据要素流通领域数据安全实时监测预警、数据安全事件通报和应急处理机制。（来源：国家数据局）

3. 国家市场监督管理总局印发《市场监督管理行政执法电子数据取证暂行规定》

4月7日，国家市场监督管理总局印发《市场监督管理行政执法电子数据取证暂行规定》。

规定所称电子数据包括但不限于下列信息、电子文件：（1）文档、图片、音视频等电子文件及其属性信息；（2）网页、博客、论坛等网络平台发布的信息；（3）用户注册信息、身份认证信息、数字签名等用户身份信息；（4）交易记录、浏览记录、操作记录等用户行为信息；（5）源代码、工具软件、运行脚本等行为工具信息；（6）系统日志、应用程序日志、安全日志等系统运行信息；（7）在各类网络应用服务中存储的与案件相关的信息文件等。

规定要求，市场监督管理部门接收或依法调取的其他国家机关收集、提取的与案件相关的电子数据，经查证属实可以作为行政执法案件的证据

使用。市场监督管理部门可以利用互联网信息系统或者设备收集、固定电子数据。用来收集、固定电子数据的互联网信息系统或者设备应当符合相关规定，并记录使用的系统、设备、软件的名称和版本号。

规定明确，对公开发布的电子数据、境内远程计算机信息系统上的电子数据，可以通过网络在线提取。对网络违法行为的技术监测记录资料，可以作为实施行政执法的电子数据证据。在线收集、固定电子数据时，可以通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台获取。必要时可以提取有关电子签名认证证书、数字签名、注册信息等关联性信息。

规定要求，电子数据证据存储应当依据《保守国家秘密法》《数据安全法》等法律法规规定，实施安全与保密管理。电子数据证据存储可以采用介质存储、区块链、云存储等方式。为防止电子数据证据丢失，可以将其备份存储。（来源：中国政府网）

4. 公安部发布《公共场所视频图像信息系统管理条例（征求意见稿）》

4月8日，公安部发布《公共场所视频图像信息系统管理条例（征求意见稿）》，旨在规范公共场所视频图像信息系统的建设、使用及其监督管理，维护公共安全，保护个人信息安全。

征求意见稿共四十条，涉及监管责任、公共视频系统建设要求、设备安装要求、公共视频系统安全措施、个人图像信息使用、法律责任等内容。具体来说，隐私保护方面，征求意见稿规定，禁止在可能侵害个人隐私的

区域、部位安装图像采集设备，保护个人隐私权益；信息保存与使用方面，公共视频系统收集的信息应合理保存，并仅用于维护公共安全的目的，不得用于其他目的。（来源：公安部）

5. 三部门印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》

4 月 19 日，中央网信办、国家发展改革委、工信部联合印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》。

工作安排提出十个方面重点任务：一是增强 IPv6 网络性能和服务质量；二是提高应用设施 IPv6 部署水平；三是提高终端设备 IPv6 连通水平；四是强化先行先试和示范引领；五是推进 IPv6 单栈部署演进；六是深化行业融合应用；七是扩大 IPv6 内容源规模；八是推进创新生态和标准体系建设；九是强化网络安全保障；十是加大宣传推广力度。

网络安全保障方面，工作安排要求加快 IPv6 安全技术产品研发应用，推动 IPv6 网络安全技术产品、解决方案创新攻关和验证示范，培育打造一批具有创新性、实效性、普适性的 IPv6 安全产品和解决方案。加强 IPv6 网络安全防护和管理监督，指导督促重点行业加强 IPv6 过渡期网络安全保护，升级 IPv6 环境下网络安全防护措施。强化 IPv6 环境下网络安全技术手段建设，提高 IPv6 网络安全威胁监测处置能力。（来源：中国网信网）

6. 商务部印发《数字商务三年行动计划（2024—2026 年）》

4 月 26 日，商务部印发《数字商务三年行动计划（2024—2026 年）》，推动商务各领域数字化转型，赋能经济社会发展，服务构建新发展格局。

计划总体要求坚持创新驱动、数据赋能、融合发展与扩大开放，并提出数商强基、数商扩消、数商兴贸、数商兴产、数商开放五项专项行动。

其中，行动计划要求建立商务领域数据分类分级保护制度，形成重要数据目录，提升数据处理者安全意识和防护能力。提升符合条件的外资企业数据跨境流动便利度。支持北京、上海、天津等自由贸易试验区落实数据分类分级保护制度，制定重要数据目录等制度规范，探索建立合法安全便利的数据跨境流动机制。立足自身制度框架，对接国际高标准经贸规则，指导自由贸易试验区、自由贸易港等开展数字领域先行先试和压力测试，加快形成一批具有引领作用的制度型开放成果。（来源：中国政府网）

7. 工信部发布 2024 年规章制定工作计划

4月29日，工信部发布2024年规章制定工作计划。其中，年内提请部务会议审议的项目包括《通信短信息服务管理规定》等五项；抓紧研究论证起草的项目包括《电子认证服务管理办法（修订）》《规范互联网信息服务市场秩序若干规定（修订）》等九项。（来源：工信部）

8. 国家发展改革委办公厅、国家数据局综合司印发《数字经济 2024 年工作要点》

4月29日，国家发展改革委办公厅、国家数据局综合司印发《数字经济 2024 年工作要点》，对2024年数字经济重点工作作出部署。

工作要点提出9方面落实举措：一是适度超前布局数字基础设施；二是加快构建数据基础制度；三是深入推进产业数字化转型；四是加快推动

数字技术创新突破；五是不断提升公共服务水平；六是推动完善数字经济治理体系；七是全面筑牢数字安全屏障；八是主动拓展数字经济国际合作；九是加强跨部门协同联动。其中，筑牢数字安全屏障要求增强网络安全防护能力，健全数据安全治理体系，提高数字化治理能力，切实有效防范各类风险。（来源：国家数据局）

9. 全国网安标委印发《全国网络安全标准化技术委员会 2024 年度工作要点》

4 月 7 日，全国网安标委印发《全国网络安全标准化技术委员会 2024 年度工作要点》。

2024 年，全国网安标委将围绕加强网络安全战略规划与标准前瞻研究、加快推进重点领域网络安全国家标准制修订、拓展宣贯渠道、强化国际标准提案研究与人才储备、完善工作机制五方面展开工作。

具体来说，将尽快研制出台关键信息基础设施边界确定方法、安全能力指标体系、测评方法等急需标准，启动关键信息基础设施主动防御、监测预警等标准研制。加快研制软件物料清单数据格式、网络弹性评价准则等标准。加快研制数据安全保护要求、数据交易服务安全等标准，推动发布数据安全风险评估、数据安全评估机构能力要求等标准，开展数据分类分级、数据安全风险评估等标准全国贯标和试点示范工作。（来源：全国网络安全标准化技术委员会）

10. 全国网安标委发布七项国家标准征求意见稿

4月，全国网安标委共发布七项国家标准征求意见稿，分别是：1. 信息安全技术 基于个人请求的个人信息转移要求（征求意见稿）；2. 信息安全技术 生成式人工智能数据标注安全规范（征求意见稿）；3. 信息安全技术 生成式人工智能预训练和优化训练数据安全规范（征求意见稿）；4. 信息安全技术 数字水印技术实现指南（征求意见稿）；5. 网络安全技术 网络安全运维实施指南（征求意见稿）；6. 数据安全技术 政务数据处理安全要求（征求意见稿）；7. 网络安全技术 信息系统灾难恢复规范（征求意见稿）。

（来源：全国网络安全标准化技术委员会）

（二）地方层面动向

1. 浙江省杭州市印发《杭州市智能网联车辆测试与应用促进条例》

4月3日，杭州市人民代表大会常务委员会印发《杭州市智能网联车辆测试与应用促进条例》，自2024年5月1日起施行。

条例规定，开展智能网联汽车道路测试的，测试主体应当按照国家有关规定向市经济和信息化主管部门提交智能网联汽车安全性自我声明和相关证明材料。道路测试、创新应用期间智能网联车辆发生交通事故的，测试主体、应用主体应当立即暂停车辆运行，开启危险警示装置，立即报警并进行现场处置。智能网联车辆车载设备应当记录和存储事故或者故障前至少九十秒的车辆位置、运行状态、驾驶模式、车内外监控视频等数据，并保持数据的连续性和完整性。智能网联车辆测试主体、应用主体应当在事

故发生二十四小时内将前述数据提供给公安机关交通管理部门，并保存数据不少于一年。

条例要求，智能网联车辆测试主体、应用主体应当按照网络安全相关法律、法规和信息安全标准的强制性要求，建立网络安全管理制度，落实网络安全等级保护制度，采取技术措施和其他必要措施，提高网络安全保护水平，保障网络安全、稳定运行。智能网联车辆测试主体、应用主体应当建立全流程数据安全和个人信息保护制度，依法处理道路测试、创新应用活动中的全部信息，落实数据安全和个人信息保护责任，采取必要措施保障数据和个人信息安全。

针对智能网联车辆发生道路交通安全违法情形的处置方面，条例规定，配备驾驶人或者安全员的，公安机关交通管理部门可以依法对驾驶人或者安全员进行处理；不配备驾驶人、安全员的，公安机关交通管理部门可以依法对车辆所有人或者管理人进行处理。智能网联车辆发生交通事故的，应当根据事故各方的行为对事故发生所起的作用以及过错严重程度，确定各方的事故责任。（来源：杭州市经济和信息化局）

2. 浙江省杭州市发布《杭州市数据流通交易促进条例（草案）》

4月22日，杭州市数据资源管理局发布《杭州市数据流通交易促进条例（草案）》。草案共九章四十三条，涉及数据权益与主体、数据流通交易服务、数据授权运营、数据定价及分配、数据生态培育、数据产业引导等内容。

草案提出推动数据产权结构性分置。根据数据来源和数据生成特征，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的数据产权运行机制，促进数据要素流通交易。鼓励市场主体开发创造衍生数据，数据处理者对其享有使用权的数据，通过加工、聚合、分析等方式实现数据内容、结构显著改变或商业价值显著提升，形成衍生数据的，享有该衍生数据的数据资源持有权、数据加工使用权和数据产品经营权。市场主体在不违反法律法规、不侵犯其他主体合法权益的前提下收集的公开数据，享有该数据的数据资源持有权、数据加工使用权。

创新容错纠错方面，草案规定，市人民政府应当建立支持在数据流通交易领域就法律、行政法规未禁止事项先行先试的机制，鼓励探索和改革创新。改革创新出现失误、错误，但是符合国家确定的改革方向，决策程序符合法律法规规定，且勤勉尽责、未牟取私利，主动挽回损失、消除不良影响或者有效阻止危害结果发生的，对有关单位和个人不予、免予或从轻、减轻追究责任。（来源：杭州市数据资源管理局）

3. 海南省印发《海南省公共互联网网络安全威胁监测与处置办法》

3月25日，海南省通信管理局印发《海南省公共互联网网络安全威胁监测与处置办法》。

办法所称公共互联网网络安全威胁包括：（1）被用于实施网络攻击的恶意IP地址、恶意域名、恶意URL、恶意电子信息，包括木马和僵尸网络控制端、钓鱼网站、钓鱼电子邮件、短信/彩信、即时通信等；（2）被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序

等；（3）网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等；（4）网络服务和产品已被非法入侵、非法控制的网络安全事件，包括主机受控、数据泄露、网页篡改等；（5）其他威胁网络安全或存在安全隐患的情形。

办法规定，按照工业和信息化部网络安全管理局有关要求，海南省通信管理局组织开展海南省公共互联网网络安全威胁处置工作，及时处理部网安局或相关部门下发的处置任务，反馈处置结果。对涉及党政机关和关键信息基础设施的，海南省通信管理局通报其上级主管单位和网信部门；对认定为危害公共互联网网络安全和存在安全隐患的，通知海南省基础电信企业、增值电信企业、域名注册管理和服务机构等采取以下一项或多项处置措施：（1）对恶意 IP 地址（或宽带接入账号）、恶意域名、恶意 URL、恶意电子邮件账号或恶意手机号码等，采取停止服务或屏蔽等措施；（2）告知网络服务提供者，由其清除本单位网络、系统或网站中存在的可能传播扩散的恶意程序；（3）告知存在漏洞、后门或已经被非法入侵、控制、篡改的网络服务和产品的提供者，由其采取整改措施，消除安全隐患；（4）其他可以消除、制止或控制网络安全威胁的技术措施。（来源：海南省通信管理局）

4. 北京市印发《北京市加快建设信息软件产业创新发展高地行动方案》

4月19日，北京市经济和信息化局印发《北京市加快建设信息软件产业创新发展高地行动方案》。行动方案围绕全面拥抱大模型、筑牢关键技

术底座、抢抓新业态培育先机、探索数据驱动新机制、推动中国软件全球布局、深化区域间协同联动六方面提出十五项重点任务。

其中，任务六“攻关新型网络安全软件”要求支持建立大模型网络安全实验室，攻关人工智能全栈式网络软件及系统，积极应对大模型生产式病毒、勒索病毒等新威胁，提升实战攻防自动化水平和溯源能力。加强金融、电信、能源等关键信息基础设施攻防演练。搭建信创开源安全检测平台，对信创产品、开源代码开展安全风险检测。推动编制自动驾驶汽车、工业设备等新硬件终端装备的网络安全标准。

任务九“提升互联网平台治理能力”要求推动互联网平台稳健发展，促进科技向善，保护用户隐私，营造良好的创新环境。支持平台企业发挥技术优势，面向关键软件、新兴领域开展硬科技创新。优化管理部门协同机制，加强新技术、新业态的探索试用、中试验证与普及推广。探索搭建国产化的“监管沙盒”环境，建设数据流动监管沙盒。（来源：北京市经济和信息化局）

5. 江苏省印发《江苏省算力基础设施发展专项规划》

4月22日，江苏省通信管理局、省发展改革委、省工业和信息化厅、省数据局联合印发《江苏省算力基础设施发展专项规划》。作为全国首个省级算力基础设施发展专项规划，规划先行先试，明确四部分主要内容：

一是分析江苏算力基础设施发展基础和发展环境。规划指出，近年来江苏算力基础设施建设逐步推进，网络连接设施发展良好，江苏算力基础

设施具有开放和创新的先发先行优势。同时，指出江苏算力基础设施发展存在的短板弱项，分析当前及未来一段时期面临的新形势和挑战。

二是明确江苏算力基础设施发展总体思路。规划提出下一阶段江苏算力基础设施发展的总体思路，明确提出到 2030 年，“打造长三角算力供给服务新高地”“打造全国智能计算创新增长极”“打造国际数字经济发展新标杆”的发展定位，并在算力基础设施、网络基础设施、算力调度、绿色安全、应用赋能等方面提出具体目标。同时，从算力、运载力、存储力、应用赋能、绿色安全等 5 个方面设置 16 个量化指标。

三是细化江苏算力基础设施发展重点任务。规划围绕优化算力基础设施布局、打造多元算力供给体系、提升算力高效运载能力、强化存力高效灵活保障、深化算力赋能行业应用、促进算力绿色低碳发展、强化算力安全保障能力等七个方面，细化分解发展重点任务，并通过专栏形式提出 16 个重点工程。

四是提出江苏算力基础设施发展保障措施。规划强调在加强统筹组织、加大政策支持、推动技术创新、强化示范引领方面提出具体保障措施，推动规划落地落实。（来源：江苏省通信管理局）

6. 福建省印发《福建省一体化大融合行政执法平台管理暂行办法》

4 月 22 日，福建省人民政府印发《福建省一体化大融合行政执法平台管理暂行办法》，自 2024 年 6 月 1 日起实施。

办法指出，“省一体化大融合行政执法平台”（简称“闽执法”平台）是指省人民政府统筹规划建设的，具有执法办案、执法监督、信息公开、业务协同、数据汇聚等功能的行政执法信息化综合应用平台。

办法规定，“闽执法”平台投入使用后，行政执法机关不再新建行政执法系统，已建行政执法系统不再单独申请政务云资源，对接平台应用需求的除外。“闽执法”平台根据工作需求实现与国家部委行政执法系统、省级执法相关公共服务平台互联互通。各级行政执法机关应当梳理本系统执法事项、执法人员、裁量权基准等要素清单，提出本单位业务需求，配合做好平台规划、建设相关工作。

办法规定，省人民政府依法确定为平台提供技术服务的单位，应当根据职责或者协议承担平台具体建设、运行维护和日常管理等工作。技术服务单位和应用单位应当按照“谁管理、谁负责”“谁使用、谁负责”的原则，依法明确数据安全主体责任，加强数据安全保护。技术服务单位应当按照国家网络安全等级保护、数据安全、关键信息基础设施安全保护等法律、法规要求，落实本级平台网络安全主体责任，采取相关保护措施，加强数据安全、业务安全、接入安全保障，确保本级平台网络安全。（来源：福建省人民政府）

境内前沿观察三：治理实践

导读：4月，公安、网信、法院等部门网络与数据安全治理实践聚焦信息内容治理与个人信息保护两方面。

信息内容治理方面，公安部公布打击整治网络谣言专项行动工作成效。2023年12月至今，公安机关累计排查网络谣言线索8万余条，侦办网络谣言类案件1万余起。聚焦社交媒体、直播和短视频等重点平台开展执法检查，查处整治9800余家次，清理网络谣言信息73.5万余条，关停违法违规账号6.3万个；指导互联网平台企业严格落实网络安全管理主体责任，坚决查处不履行主体责任和义务的平台，行政处罚网站平台590余次。

中央网信办接连部署开展“清朗·整治‘自媒体’无底线博流量”专项行动、“清朗·打击违法信息外链”专项行动。其中，提出将重点整治滥发“新黄色新闻”行为。“新黄色新闻”是指运用煽情化表达手法，配以抓人眼球的标题和封面，制作发布要素不全、真假难辨、质量低下、公共价值缺失的信息内容。

个人信息保护方面，陕西西安、北京、山西长治等地警方破获多起个人信息相关刑事案件，违法犯罪行为包括“有偿查询、提供公民个人敏感信息”“境内外勾连、利用黑客手段“开盒”曝光个人信息”“在境外平台建立频道，以虚拟货币形式非法贩卖大量公民个人信息”等。杭州互联网法院审理一起非法买卖、使用新生儿信息的个人信息保护民事公益诉讼

案，涉案新生儿个人信息 3 万余条。北京四中院审理一起词典 APP 侵犯用户个人信息权益案件，从侵权角度规范 APP 个人信息处理活动。

此外，国家互联网信息办公室发布生成式人工智能服务已备案信息，截至 2024 年 3 月有 117 个已备案模型，包括文心一言（北京百度网讯科技有限公司）、云雀大模型（北京抖音信息服务有限公司）、紫东太初大模型开放平台（中国科学院自动化研究所）等。

关键词：网络谣言、清朗系列专项行动、个人信息保护、生成式人工智能服务备案

（一）公安机关治理实践

1. 公安机关打击整治网络谣言专项行动取得阶段性成效

4月12日，公安部公布打击整治网络谣言专项行动工作成效。2023年12月以来，公安部部署全国公安机关统一开展打击整治网络谣言专项行动。截至目前，公安机关累计排查网络谣言线索8万余条，侦办网络谣言类案件1万余起，抓获犯罪嫌疑人1500余名，行政处罚10700余人，开展公开辟谣等4200余次。

工作中，公安机关坚持“全链条、全平台、全领域”覆盖，持续加大打击整治力度，及时发现查处借热点事件进行造谣引流违法犯罪活动，坚决整治自媒体运营人员恶意摆拍、炮制谣言等违法违规行为，重拳打击编造虚假疫情、险情、灾情等违法犯罪活动。坚持打防管控一体推进，聚焦社交媒体、直播和短视频等重点平台开展执法检查，查处整治9800余家次，清理网络谣言信息73.5万余条，关停违法违规账号6.3万个；指导互联网平台企业严格落实网络安全管理主体责任，坚决查处不履行主体责任和义务的平台，行政处罚网站平台590余次。

同期公布浙江、江苏公安机关查处“寒假作业丢巴黎”摆拍引流案、山东公安机关查处造谣“喂住院婆婆吃泡面”案等10起打击整治网络谣言典型案例。（来源：公安部）

2. 浙江杭州警方通报打击整治网络谣言、网络暴力专项行动推进情况

4月10日，浙江省杭州市公安局召开新闻发布会，通报打击整治网络谣言、网络暴力专项行动推进情况。

通报指出，2023年12月和2024年1月，公安部先后启动“打击整治网络谣言”和“打击整治网络暴力”专项行动。自专项行动开展以来，杭州公安共侦破相关刑事案件3起，行政案件12起，采取刑事强制措施10人，行政拘留6人，行政罚款7人，教育训诫800余人，清理网络谣言信息11000余条，关停违法违规账号34000余个，整治互联网平台企业120余家次。

发布会同步发布五起典型案例，包括三起行政处罚案件以及两起刑事案件。（来源：公安部网安局）

3. 上海警方通报打击整治网络谣言专项行动措施成效

4月16日，上海市公安局召开新闻发布会，通报上海警方打击整治网络谣言专项行动措施成效和典型案例。

发布会指出，2023年12月，公安部部署打击整治网络谣言专项行动以来，上海警方面对网上恶意炒作、造谣生事等网络违法乱象开展全力集中整治，依法从严快处网络造谣违法人员、全链条打击网络谣言犯罪、持续开展网络谣言生态综合治理。截至目前，累计查处网络谣言384起，依法查处造谣传谣人员530余人，清理网上谣言信息53000余条，依法关停违法违规账号5000余个，坚决维护清朗有序的网络环境。（来源：上海网警）

4. 因未落实业主个人信息保护义务，甘肃 10 家物业公司被处罚

4月9日消息，甘肃天水武山县公安局近日按照上级统一部署要求，严肃整治物业公司信息泄漏乱象，开展公民个人信息保护专项检查行动。

经查，多家物业公司办公电脑随意存储大量小区业主家庭住址、身份证号码、联系方式等个人信息，并且存在内部管理制度及操作规程缺失、信息系统弱口令等严重问题，未落实个人信息分类管理及加密、去标识化制度，导致业主个人信息被泄漏的风险极大。其中，3家物业公司因未落实保护义务，致使业主信息被售楼中心、二手房交易中心非法获取，多名住户被骚扰电话困扰。

武山县公安机关依据《网络安全法》第四十四条、第六十四条之规定，对这3家物业公司处以罚款5000元的行政处罚并责令限期整改，同时对非法获取个人信息的售楼中心、二手房交易公司分别处以罚款1万元的行政处罚。

针对另外7家物业公司未落实个人信息保护义务的问题，公安机关依据《个人信息保护法》第五十一条、第六十六条之规定，处以警告的行政处罚并责令其限期整改。（来源：公安部网安局）

5. 陕西西安警方成功打击一起非法出售公民个人信息案件

4月1日消息，陕西省西安市未央警方近日成功打掉一个非法出售公民个人信息团伙，抓获犯罪嫌疑人124人，依法刑事拘留19人，冻结涉案银行卡账户13个。

2023年10月，有群众举报自己在网上咨询法律业务时，对方声称可通过其所在的西安某某法律咨询公司查询各种包括银行卡、手机号等在内的公民个人身份信息。经侦查，警方初步查明该公司老板为李某，其上线为刘某，下线为4部12组的运营管理体系。

该公司通过抖音、快手等网络社交平台发布广告引流，身披法律咨询业务外衣，以为客户提供诉讼代理为由，行“有偿查询、提供公民个人敏感信息”之实，所提供的查询内容包括身份证号查地址、身份证查手机等个人敏感信息，索要价格在600元至2000元不等，存在集团式非法买卖、获取公民个人信息的犯罪行为。2023年4月起，李某伙同万某等人，通过从其上线刘某处非法查询获取公民个人信息来“拓展业务”，公司通过查询买卖他人信息非法获利270余万。

目前，警方已对该法律咨询公司开展集中收网行动，共抓获犯罪嫌疑人124人，扣押电脑149台，查扣手机124部。目前，案件正在进一步侦办当中。（来源：公安部网安局）

6. 北京警方成功侦破一起利用黑客手段“开盒”曝光个人信息的网络犯罪案件

4月8日消息，北京警方近日成功侦破一起境内外勾连、利用黑客手段“开盒”曝光个人信息的网络犯罪案件。

据悉，北京市海淀分局接到某公司报警，称公司多名员工、艺人及粉丝的身份信息、通讯地址、家庭住址等个人信息被恶意曝光在网络上，导

致多名受害者遭受网络骚扰、威胁、辱骂，受害人不堪其扰，承受极大的心理负担，严重影响正常生活。

北京警方迅速行动，成功将两名利用黑客技术窃取信息并恶意公布的犯罪嫌疑人赵某、成某某抓捕归案，二人对相关犯罪事实供认不讳，称因与其他粉丝产生意见分歧，遂利用技术手段非法获取他人个人信息并在网络上公布、辱骂受害人。目前，二人已被北京市公安局海淀分局依法刑事拘留。（来源：公安部网安局）

7. 山西长治警方成功破获特大侵犯公民个人信息案

4月19日消息，山西长治屯留分局近日成功破获一起特大侵犯公民个人信息案，铲除一个在境外平台买卖公民信息的特大新型网络犯罪团伙。

2023年4月，山西长治屯留分局网安大队在工作中接到线索称，有人利用境外平台非法贩卖包含姓名、家庭住址、手机号等公民个人信息，涉及全市多个县区。经调查，民警发现多名犯罪嫌疑人在境外平台建立频道，以虚拟货币的形式非法贩卖大量公民个人信息，涉及人员多、地域广、涉案资金大、犯罪链条长，且犯罪手法新颖、犯罪手段隐蔽，社会危害极其严重。

警方立即抽调精干警力组成专案组展开侦查。经查，犯罪嫌疑人通过非法手段获取公民姓名、QQ号、手机号、抖音号、淘宝号等个人信息数据后，进行“清洗”加工，利用境外平台作为日常联系、传输数据的媒介，通过虚拟货币的形式进行交易，从中获取巨额利润。

专案组最终查清该犯罪团伙成员的真实身份和活动范围，辗转 5 省 9 市先后抓获 7 名犯罪嫌疑人，同时冻结涉案资金 3000 余万元，扣押涉案手机、电脑 30 余台。（来源：公安部网安局）

8. 江西上饶警方成功破获一起利用短视频平台引流推广色情 APP 的非法利用信息网络案件

4 月 25 日消息，江西上饶广丰警方近日成功破获一起利用短视频平台引流推广色情 APP 的非法利用信息网络案件，成功抓获 2 名嫌疑人，并扣押作案手机 200 余部。

2024 年 3 月，广丰区公安局网安大队发现互联网上相继发布一些利用某短视频直播平台为某境外色情 APP 进行引流的视频。经调查，发现嫌疑人张某、姜某购买大量二手手机用于注册某短视频平台账号，并发布含有“性暗示”类视频，诱导群众添加发布境外色情赌博 APP 下载链接的 QQ 或微信，以此为色情赌博类 APP “引流”。嫌疑人引导网民下载色情赌博类 APP 后，与该 APP 运营方结算从而获利。目前，案件正在进一步侦办中。（来源：公安部网安局）

9. 山东青岛警方破获一起特大非法利用信息网络案

4 月 26 日消息，山东青岛警方近日在“净网 2024”专项行动中破获一起特大非法利用信息网络案，抓获涉案人员 110 余名，捣毁吸粉引流工作室 10 余个，扣押作案设备 2400 余台，全方位打击为境外诈骗集团吸粉引流的“黑灰产”犯罪链条。

2022年10月，青岛网警在日常巡检中发现，青岛市黄岛区有人操作QQ账号为境外诈骗团伙提供吸粉引流服务，导致多人被骗。同时警方也接到多起报警电话，受害者被骗金额从2千到10万元不等。受害者添加陌生QQ好友后，会收到对方暧昧信息并被诱导下载交友软件。在使用交友软件与对方联系的过程中，受害者被要求参与刷单活动，起初有小额返利，但随着刷单量增加，对方逐渐以各种理由不再返利，受害者才意识到被骗。

经查，该团伙整个犯罪利益链条包括境外电信诈骗集团、引流工作室、软件程序开发人员等九个环节，分布全国多省多地，人员众多。每个环节均发挥着不可替代的作用，形成相对稳固的利益“关系网”，每日可对上万人实施诈骗犯罪。

截至今年3月，在公安部、省公安厅指挥协调下，青岛警方出动300余名警力奔赴全国各地，先后组织9次集中抓捕行动，成功抓获110余名涉案人员，扣押作案设备2400余台。目前，案件正处于公诉阶段。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办部署开展“清朗·整治‘自媒体’无底线博流量”专项行动

4月21日，中央网信办秘书局印发通知，决定开展为期两个月的“清朗·整治‘自媒体’无底线博流量”专项行动。

专项行动聚焦“自媒体”无底线造热点蹭热点，制造以假乱真、虚实混杂的“信息陷阱”等突出问题，重点整治五个方面：一是自导自演式造假；二是不择手段蹭炒社会热点；三是以偏概全设置话题；四是违背公序良俗制造人设；五是滥发“新黄色新闻”。其中，“新黄色新闻”是指运用煽情化表达手法，配以抓人眼球的标题和封面，制作发布要素不全、真假难辨、质量低下、公共价值缺失的信息内容。

专项行动提出加强重点平台和重点环节管理、加强“自媒体”账号全流程管理、加强信息来源标注展示、完善流量管理措施四项主要任务。其中，要求平台对开通营利权限的账号，应当以身份证件号码等进行真实身份信息认证。加强账号名称等账号信息动态核验，从严审核热点事件发生后新注册及名称变更的账号，发现假冒的一律关闭。严格执行“一人一号、一企两号”账号注册数量规定，对明确告知系小号、实际出镜人为同一人等的，应及时予以处置。（来源：中国网信网）

2. 中央网信办部署开展“清朗·打击违法信息外链”专项行动

4月28日，中央网信办印发通知，在全国范围内部署开展为期2个月的“清朗·打击违法信息外链”专项行动。

本次专项行动聚焦违法信息外链问题易发多发的8个重点环节开展整治，分别是账号，评论，群圈，直播、短视频，生活服务，浏览器、搜索引擎，电商以及涉未成年人版块环节。其中，直播、短视频环节将加强对AI技术和虚假身份背景的监管，防止发布伪成功学、伪国学、“养生课程”、

理财技巧等信息，诱导网民添加好友、加入群组进而实施诈骗。（来源：中国网信网）

3. 国家互联网信息办公室发布生成式人工智能服务已备案信息

4月2日，国家互联网信息办公室发布生成式人工智能服务已备案信息，落实《生成式人工智能服务管理暂行办法》中的备案要求。

国家网信办指出，提供具有舆论属性或社会动员能力的生成式人工智能服务的机构或个人，需通过属地网信部门履行备案程序，属地网信部门应及时将已备案信息对外公开发布。这些信息将在国家网信办官网定期汇总更新，不再另行公告。

此次公布的是截至2024年3月的备案信息，涉及117个已备案模型，具体包括文心一言（北京百度网讯科技有限公司）、云雀大模型（北京抖音信息服务有限公司）、紫东太初大模型开放平台（中国科学院自动化研究所）等。

国家网信办强调，已上线的生成式人工智能应用或功能，应在显著位置或产品详情页面公示所使用的已备案生成式人工智能服务情况，包括模型名称及备案号。（来源：中国网信网）

4. 国家互联网信息办公室发布第二批应用程序分发平台备案编号

4月8日，国家互联网信息办公室发布第二批共二十三家应用程序分发平台名称及备案编号，落实《移动互联网应用程序信息服务管理规定》中的备案管理要求。

第二批备案清单包含中关村在线手机应用、豌豆荚、应用汇、荣耀应用市场、魅族应用商店、小天才电话手表应用商店、PC 下载网、下载之家、抖音开放平台等。

根据《移动互联网应用程序信息服务管理规定》有关规定，备案仅是对应用程序分发平台提供分发服务行为的确认，不代表对该平台服务能力和其在架应用程序的认可，任何平台和个人不得用于任何商业目的，不得违规从事其他业务。（来源：中国网信网）

5. 北京市网信办启动“清朗·E企护航”专项整治行动

4月2日，北京市网信办宣布自即日起，启动为期9个月的“清朗·E企护航”专项整治行动，落实中央网信办“清朗·优化营商环境—整治涉企侵权信息乱象”专项行动部署要求。

此次专项整治行动重点聚焦侵犯企业和企业家合法权益的网络信息内容乱象，集中整治抹黑诋毁企业形象声誉、炮制传播虚假不实信息、敲诈勒索谋取非法利益、扰乱企业生产经营秩序、恶意炒作涉企公开信息，及水军账号控评造谣、唱衰经济破坏营商环境等七方面突出问题。属地各网站平台应当严格履行主体责任，健全管理制度，加强热搜榜单、用户账号及MCN机构等重点环节管理，依法依规开展服务，切实维护健康有序的网络传播秩序。

专项整治行动期间，北京市网信办将加大巡查检查力度，充分发挥统筹协调作用，联合有关部门、各区网信办对落实整治要求不力的网站平台

和问题严重、影响恶劣的网络账号，依法依规予以严肃查处，并及时公开曝光典型案例，震慑打击违法违规行为。

4月30日，北京市网信办公布专项行动成效。截至公布之日，共受理举报5700余起，指导属地网站平台清理违法违规信息3万余条、依法依规处置违规账号1000余个，依法约谈处罚网站、“自媒体”账号5家。（来源：网信北京）

6. 江西南昌西湖区网信公安两部门联合依法约谈企业负责人

4月11日，在江西省南昌市网信办的指导下，西湖区网信办联合西湖区公安分局网安大队依法约谈辖区内南昌卓蓝科技有限公司负责人胡某。

经查，南昌卓蓝科技有限公司运营的APP存在“未明示收集使用个人信息的目的、方式和范围”等问题，相关行为涉嫌违反《网络安全法》《App违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法律法规。

经过约谈，该企业负责人充分认识到问题的严重性，表示将按照监管部门要求，在规定期限内完成整改，并将进一步加强互联网法律法规的学习，完善公司内部的网络安全制度，杜绝此类问题的再次发生。（来源：网信南昌）

7. 江西南昌网信办依法对微信小程序“查成交价”运营主体作出行政处罚

4月22日消息，江西省南昌市互联网信息办公室近日在日常巡查监测中发现属地某公司运营的微信小程序“查成交价”（主要用于查询南昌市内新房和二手房成交价）涉嫌存在履行个人信息保护义务和数据安全保护义务不到位等问题。

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，查明微信小程序“查成交价”：（1）未公开收集使用个人信息规则、未明示收集使用个人信息的目的、方式和范围；（2）未采取加密、去标识化等措施确保个人信息处理活动符合法律、行政法规的规定；（3）存在可导致150余万条个人信息泄露的漏洞。上述行为违反《网络安全法》《数据安全法》《个人信息保护法》的相关规定。

4月22日，南昌市网信办依据《网络安全法》《数据安全法》《个人信息保护法》的有关规定，对微信小程序“查成交价”的运营公司予以警告处罚并责令限期改正，并责令微信小程序“查成交价”暂停服务。（来源：网信南昌）

（三）通信管理部门治理实践

1. 广东、浙江、北京通信管理部门通报存在问题的APP

（1）广东

4月30日，广东省通信管理局公开通报7款未按要求完成整改APP。通报指出，广东省通信管理局持续开展APP隐私合规和数据安全专项整治行动，发出《违法违规APP处置通知》责令APP运营者限期整改，并通知相关应用商店协助督促APP运营者整改。截至目前，尚有7款APP未完成整改。被通报的APP应在5月10日前完成整改及反馈工作。APP所涉问题包括违规收集个人信息，APP强制、频繁、过度索取权限，APP频繁自启动和关联启动，超范围收集个人信息等。

同日，广东省通信管理局还通报下架1款侵害用户权益的APP。通报指出，截至通报规定时限，经核查复检，尚有1款APP“太享福利社”未按要求完成整改反馈。该APP存在问题为频繁自启动和关联启动。为严肃处理上述APP的违规行为，广东省通信管理局决定对上述APP予以下架。相关应用商店应立即组织对名单中的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。广东省通信管理局将对通报APP持续跟踪，视情况进一步采取断开网络、行政处罚、纳入电信业务经营不良名单等后续处理措施。

(2) 浙江

4月30日，浙江省通信管理局通报2024年第3批15款侵害用户权益的APP。浙江省通信管理局近期组织第三方检测机构对群众关注的网上购物、运动健身、实用工具等类型APP进行检查，并书面要求违规APP开发运营者限期整改。截至目前，尚有15款APP未按要求完成整改，现予以通报。请上述APP开发运营者在5月13日前完成整改落实工作，整改落实不到位的，将视情采取下架、关停、行政处罚等措施。

APP 所涉问题包括违规收集个人信息, APP 强制、频繁、过度索取权限, APP 频繁自启动和关联启动等。

(3) 北京

4 月 30 日,北京市通信管理局通报 2024 年第四期问题 APP。通报指出,北京市通信管理局近期通过抽测发现本市部分 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 6 款 APP 未整改或整改不到位,现予以公开通报。

此外,3 月 29 日,北京市通信管理局通报本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“展讯通”“小艺宝”等 11 款 APP 未整改或整改不到位,现予以全网下架处置。(来源:广东信息通信业、浙江省通信管理局、北京市通信管理局)

2. 浙江省通信管理局部署防范治理电信网络诈骗工作

4 月 16 日,浙江省通信管理局组织召开防范治理电信网络诈骗工作会议,总结当前形势,通报问题不足,部署 2024 年度重点工作。

会议部署 6 个方面 20 条工作举措:(1)健全责任体系:严格落实《反电信网络诈骗法》各项要求,加强内部机制和安全生产制度建设,健全考核督导机制,建强反诈专职队伍,加大追查问责力度;(2)深化断卡行动:开展断卡效果评估与审核报备工作,加强新入网异常开卡风险监测,做好事前审核阻断、事中动态监管和事后拓展排查;(3)严控电信业务涉诈风险:充分发挥风险评估机制“体检”作用,全面梳理新增和重点存量业务

的涉诈风险隐患，根据风险等级采取相应的应对措施；（4）提升技术反制能力：坚持预警为先，不断创新技术手段，构筑行业“全链式”技术防线。组织开展技术创新，攻关技术难点，提升技术反制能力；（5）强化综合防范措施：深化信用惩戒，完善问题通报和公开曝光机制。加大反诈宣传工作力度，创新各类宣传方式，提升广大用户的识诈防骗意识；（6）做好重点专项工作：增强行业法治观念、提升合规能力，推进涉卡涉用户数据涉诈风险治理，进一步建立健全涉卡涉用户数据安全长效管理机制。（来源：浙江省通信管理局）

（四）其他部门治理实践

1. 上海临港新片区数据跨境服务中心启用运营

4月7日，上海临港新片区数据跨境流动创新服务沙龙暨数据跨境服务中心启用仪式顺利举行。

服务中心将致力于为数据处理者提供全方位、全流程数据跨境服务，包括材料受理、业务咨询等环节，在自贸区一线打造数据跨境流动的“绿色通道”。

临港新片区数据跨境公共服务管理平台同步上线试运行。据介绍，该平台与服务中心紧密协作，主要为在临港新片区率先推进数据跨境模式创新，从“正面案例”出发服务企业安全合规开展相关业务提供一站式服务。数据处理者可以根据平台上的相关指引申请数据跨境场景化创新试点业务，

实现材料在线提交、项目在线申报、结果在线查询等便捷功能。（来源：上海临港）

2. 杭州互联网法院审理一起非法买卖、使用新生儿信息案件

4月16日，杭州互联网法院公开开庭审理公益诉讼起诉人杭州市萧山区人民检察院诉李某、某摄影公司、某创意公司个人信息保护民事公益诉讼案，当庭判令三被告在国家级媒体上公开赔礼道歉并支付公益损害赔偿金29万余元。上述公益损害赔偿金用于个人信息保护或者妇女儿童权益保护等公益事项。

公益诉讼起诉人发现，2020年下半年至2022年2月期间，李某通过非法渠道陆续购入多地新生儿个人信息3万余条，包括新生儿出生日期、性别、父母姓名及联系方式等。某摄影公司、某创意公司为拓展婴童摄影业务，先后向李某购买交易并使用上述信息，李某从中非法获利29万余元。

公益诉讼起诉人认为，三名被告未经个人同意，非法买卖、使用公民个人信息，严重扰乱公民生活安宁，侵害公共信息安全，损害社会公共利益，依法应当承担赔偿损失、赔礼道歉、消除影响的民事侵权责任。另被告李某的上述行为已被依法追究刑事责任。

法院经审理认为，涉案的新生儿个人信息包含出生日期、性别、父母姓名及联系方式等，足以识别到特定的新生儿及其父母，属于《民法典》所保护的公民个人信息。三名被告以牟利为目的，在未取得个人同意的情况下，非法买卖、使用特定人群的相关个人信息，不仅有损相关主体的公

民个人信息权益，扰乱新生儿及其父母的生活安宁，还侵害了公共信息安全领域的社会公共利益，故三名被告应当承担相应的民事责任。

庭审过程中，三名被告明确表示已认识到自身错误，向社会公众致歉，并自愿承担相应的民事责任。（来源：杭州互联网法院）

3. 北京第四中级人民法院：词典 APP 附加功能违规收集个人信息构成侵权

4月25日消息，北京市第四中级人民法院近日审理一起词典 APP 侵犯用户个人信息权益的案件。

本案中，原告张某下载了一款词典 APP。下载后发现注册该 APP 时无需用户点击同意，系统会自动勾选“已阅读并同意服务条款和隐私政策”的选项，且《隐私政策》中显示“一旦注册完成，APP 将会自动收集用户的设备信息、地理位置、用户行为等信息。若用户取消勾选，就无法完成注册，也无法使用该词典 APP。”张某只能按照要求，填写手机号并同意《隐私政策》完成注册。使用一段时间后，张某想停用涉案 APP，但因 APP 一直收集自己的个人信息，张某便想撤回允许该 APP 处理其信息的同意，但发现 APP 并未提供撤回同意的途径。张某遂将 APP 运营主体某科技公司告上法庭，要求法院判令科技公司停止收集并删除已经收集的张某个人信息，向其赔礼道歉并赔偿公证费、律师费、精神损失费共计 10 万元。

法院认为，涉案 APP 的名称、官方描述、应用市场的描述等均指向流行语词典功能，因此涉案 APP 的属性应为实用工具类 APP，基本业务是词汇查询。根据《常见类型移动互联网应用程序必要个人信息范围规定》的规

定，“实用工具”类 APP 其基本功能服务包括词典翻译等，无须手机号等个人信息，即可使用基本功能服务，因此该词典 APP 要求先收集个人信息才提供服务的行为违反上述规定。此外，涉案 APP 的《隐私政策》被默认勾选“同意”，并未让张某主动自愿作出同意的选择，不符合《个人信息保护法》第十四条“自愿”“明确”的要求。同时，APP 未提供便捷的撤回同意方式，侵犯用户个人信息权益。

案件经过一审、二审，涉案词典 APP 的运营公司被判删除收集的张某个人信息，并向张某赔礼道歉、赔偿其合理开支 3080 元。（来源：北京市第四中级人民法院）

4. 国家计算机病毒应急处理中心监测发现 10 款违规移动应用

4 月 28 日，国家计算机病毒应急处理中心通报 10 款违规移动应用，具体存在的隐私不合规行为包括：

(1) 在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则，或以默认选择同意隐私政策等非明示方式征求用户同意；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：个人信息处理者的名称或者姓名和联系方式；个人信息处理目的、处理方式，处理个人信息的种类、保存期限。涉嫌隐私不合规。涉及 9 款 App。

(2) 未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）

受理并处理；个人信息处理者未建立便捷的个人行使权利的申请受理和处理机制。涉嫌隐私不合规。涉及 5 款 App。

(3) 个人信息处理者未提供便捷的撤回同意的方式；个人撤回同意，影响撤回前基于个人同意已进行的个人信息处理活动的效力。涉嫌隐私不合规。涉及 4 款 App。

(4) 个人信息处理者处理不满十四周岁未成年人个人信息的，未制定专门的个人信息处理规则。涉嫌隐私不合规。涉及 1 款 App。（来源：国家计算机病毒应急处理中心）

境外前沿观察：月度速览十则

导读：4月，联合国发布《全球数字契约：零案文》，为实现包容、安全可靠的数字未来提出行动目标。美国总统拜登签署一揽子立法，《TikTok剥离法》正式成为法律，若字节跳动未能在规定时限内将TikTok美国业务出售或以其他方式剥离，以保证TikTok不受包括中国在内的外国对手的控制，将面临美国的全国禁令。

美国总统拜登签署《关于关键基础设施安全与韧性的国家安全备忘录》，细化和明确联邦政府在关键基础设施安全、弹性和风险管理方面的角色和责任。英国《2022年产品安全和电信基础设施法》和《2023年产品安全和电信基础设施（联网设备安全要求）条例》生效，强化联网设备供应链安全管理。

此外，美国一市政监管机构遭遇美杜莎网络犯罪团伙勒索攻击，勒索赎金10万美元，否则将披露218GB数据。美国司法部一服务提供商发生数据泄露事件，源于司法部的诉讼案件相关数据被盗。

关键词：TikTok剥离法、关键基础设施安全与韧性、联网设备安全、网络攻击

1. 联合国发布《全球数字契约：零案文》，为后续政府间磋商提供讨论基础

4月2日，联合国发布《全球数字契约：零案文》，旨在为所有人实现包容、安全、可靠的数字未来。文件提出5项行动目标：（1）缩小数字鸿沟，加速实现可持续发展目标；（2）扩大融入数字经济的机会；（3）培育包容、开放、安全的数字空间；（4）推进公平的国际数据治理；（5）以人为本，强化人工智能等新兴技术治理。同时，各项行动目标下也提出具体支持契约实施的制度安排和举措，为后续政府间磋商提供讨论基础。联合国承诺每两年召开《全球数字契约》高级别审议会议，审查《全球数字契约》内容，评估目标进展，明确全球数字合作的新机遇、新挑战。（来源：联合国）

2. 美国总统拜登签署一揽子立法，《TikTok 剥离法》成为法律

4月14日，美国总统拜登签署一揽子立法《2024财年（截至9月30日）紧急补充拨款法》，包含经过修订的《保护美国人免受外国对手控制的应用程序法》（简称《TikTok 剥离法》）。

与2024年3月众议院通过版本相比，正式通过的《TikTok 剥离法》主要变化在于控制权剥离时限的修改。该法对TikTok母公司字节跳动的剥离控制权时限从原先的180日延长至270日，并授权美国总统可将该时限再延长90日。若字节跳动未能在规定时限内将TikTok美国业务出售或以其

他方式剥离，以保证 TikTok 不受包括中国在内的外国对手的控制，将面临美国的全国禁令。（来源：美国国会）

3. 美国总统拜登签署《关于关键基础设施安全与韧性的国家安全备忘录》

4月30日，美国总统拜登签署《关于关键基础设施安全与韧性的国家安全备忘录》，旨在细化和明确联邦政府在关键基础设施安全、弹性和风险管理方面的角色和责任，为关键基础设施的安全与韧性建立最低要求和问责制。

备忘录规定由国土安全部领导联邦政府的关键基础设施安全保卫工作，要求国土安全部部长落实以下措施：（1）国家层面协调与评估。与关键基础设施部门风险管理机构合作，确保其履行职责，根据战略指导和国家计划来落实国家优先事项，并不断加强关键基础设施安全和韧性的统一方法；（2）风险识别与评估。识别并评估行业和跨行业风险，分析关键基础设施资产和系统之间的依赖关系，考虑物理威胁、网络威胁以及漏洞相关的潜在威胁之间的联系，支持关键基础设施风险管理和优先排序；（3）推荐保护美国关键基础设施的措施。（来源：美国白宫）

4. 美国 FCC 发布《安全原则：系统性解决安全漏洞》

4月17日，美国联邦贸易委员会（FCC）发布《安全原则：系统性解决安全漏洞》，旨在有效应对复杂系统中的安全漏洞风险。文件要求网络安

全和基础设施安全局敦促制造商提升产品安全性，消除影响客户安全的产品缺陷或安全漏洞。文件对 3 类常见安全漏洞提出解决建议：（1）针对跨站脚本（XSS）漏洞建议采用模板渲染系统提供安全机制；（2）针对 SQL 注入漏洞建议采用查询构建器提供安全机制，区分攻击者控制的数据和查询结构；（3）针对缓冲区溢出和使用后释放漏洞建议采用内存安全编程语言进行开发，对代码进行静态和动态分析以检测潜在漏洞，使用内存调试工具跟踪内存分配和使用情况等。（来源：美国联邦贸易委员会）

5. 德国联邦信息安全办公室发布指南《生成式人工智能模型：行业和政府部门的机遇和风险》

4 月 10 日，德国联邦信息安全办公室发布指南《生成式人工智能模型：行业和政府部门的机遇和风险》，旨在提高企业和政府部门使用大语言模型（LLM）的安全意识。指南指出，LLM 生成结果存在错误、偏见、质量不高、时效性弱、缺乏可解释性、生成的代码缺乏安全性等风险。对此，指南提出相关对策：（1）加强数据管理；（2）确保数据完整性；（3）提升数据质量；（4）保护敏感训练数据；（5）强化模型安全。（来源：德国联邦信息安全办公室）

6. 英国《2022年产品安全和电信基础设施法》及相关条例生效，强化联网设备供应链安全管理

4月29日，英国《2022年产品安全和电信基础设施法》和《2023年产品安全和电信基础设施（联网设备安全要求）条例》生效，旨在确保联网设备满足最低安全标准。该法和条例的适用范围涵盖联网设备制造商、进口商和分销商等供应链环节上的各方，明确联网设备安全要求，包括：（1）每个产品应当配备唯一密码或允许用户设置密码，防范未经授权的入侵；（2）制造商应当就如何报告产品安全漏洞提供明确说明，及时发现并修复潜在安全漏洞；（3）制造商应当向使用者提供产品安全更新的详细信息，确保产品在使用周期内保持最新安全状态。产品安全和标准办公室（OPSS）负责相关执法活动，采取必要措施监管制造商、进口商和分销商的合规情况并处罚违规行为。（来源：英国政府）

7. 英国政府发布《2024年网络安全漏洞调查》

4月10日，英国政府发布《2024年网络安全漏洞调查》。调查显示，在英国2000家企业和1004家慈善机构中，一半企业（50%）和三分之一的慈善机构（32%）在过去1年内经历过漏洞攻击。中型企业（70%）、大型企业（74%）和年收入50万英镑以上的慈善机构（66%）相比于小微企业更易遭受漏洞攻击。

常见攻击类型包括网络钓鱼攻击、在线欺诈攻击、病毒或其他恶意软件攻击。调查建议企业和慈善机构采取以下防范措施：（1）优化事件响应，

及时通知高级管理层并向相关监管机构报告；（2）完善外部报告机制，建立多渠道报告体系。除向监管机构报告外，还应建立向其他利益攸关方报告的机制，例如保险公司、客户、网络安全机构等；（3）采取安全防范措施，部署安全防护技术，加强员工安全意识培训，定期更新网络安全政策。

（来源：英国政府）

8. 美国市政监管机构遭遇美杜莎网络犯罪团伙勒索攻击

4月3日消息，美国得克萨斯州塔兰特县的地方财产税评估部门发表声明，确认遭到美杜莎网络犯罪团伙攻击，导致部分个人数据泄露。美杜莎网络犯罪团伙称，若塔兰特县不支付10万美元赎金，将在6日内泄露近218GB数据，包括各种财务文件、商业和住宅房产数据库、业主信息、房产记录、法庭文件、董事会成员信息、税务信息、员工记录等。塔兰特县正在与网络安全专家合作，恢复受影响系统。美杜莎勒索软件组织在2023年首次出现，其受害者包括一家为50万人提供饮用水的意大利公司、明尼苏达州最大的学区之一、法国小镇萨特鲁维尔、汤加国有电信公司等。（来源：Recorded Future News）

9. 美国司法部服务提供商数据泄露，导致34万多人数据被盗

4月9日消息，美国司法部服务提供商Greylock McKinnon Associates（GMA）咨询公司近日发生数据泄露事件，导致341650人的个人数据被盗，包括姓名、出生日期、地址、医疗保险健康保险索赔号码、社会安全号码

等。GMA 是一家提供诉讼支持服务并协助司法部门处理法律案件的咨询公司，本次被盗数据源于司法部的诉讼案件相关数据。事件发生后，GMA 已从其系统中删除司法部数据，并向受影响的个人提供 24 个月的免费身份盗窃保护和信用监控服务。（来源：SC Media）

10. 虚假 Facebook、MidJourney、OpenAI 页面向百万人推广恶意软件

4 月 9 日消息，有黑客正在利用 Facebook 广告和被劫持的页面推广虚假人工智能服务。黑客假装提供 MidJourney、OpenAI 的 SORA 和 ChatGPT-5、DALL-E 等人工智能服务，传播恶意软件以窃取用户密码。其中，一个冒充 Midjourney 的恶意 Facebook 页面吸引 120 万粉丝，并在最终被删除之前保持活跃近一年。信息窃取恶意软件从受害者浏览器中窃取数据，包括存储的登录凭据、cookie、加密货币钱包信息、信用卡信息等。这些数据可能被在暗网出售，或用以破坏目标的在线账户、实施诈骗等活动。（来源：E 安全）

行业前沿观察一：2023《特殊人群（未成年人、老年人等）网络权益保护专题报告》发布、工信部公示2024年度制造业新型技术改造城市试点名单、工业互联网一体化进园区“百城千园行”活动开启

导读：作为2023“安满周”的重磅内容，第三届网络志愿服务大会暨《2023网民网络安全感满意度调查“特殊人群（未成年人、老年人等）网络权益保护”专题报告》发布会于4月16日下午在北京香山圆满举行。

日前，财政部、工信部发布《关于开展制造业新型技术改造城市试点工作的通知》（以下简称《通知》）。《通知》提到，发挥中央财政资金引导作用，大力推进“智改数转网联”新技改，打造一批重大示范项目，促进企业设备更新、工艺升级、数字赋能、管理创新，推动传统产业转型升级，提高制造业高端化、智能化、绿色化发展水平，为巩固和增强经济回升向好态势，加快培育新质生产力、推进新型工业化提供有力支撑。

工信部发布《关于组织开展 2024 年工业互联网一体化进园区“百城千园行”活动的通知》（以下简称《通知》）。工信部指出，其目的是为贯彻落实党中央、国务院决策部署，深入实施工业互联网创新发展战略，推动工业互联网高质量发展和规模化应用，发挥工业园区产业集聚优势，推动工业互联网向地市县域落地普及，促进广大企业特别是中小企业加快数字化转型，促进经济高质量发展。

关键词：安满周、2023 年全国网民网络安全感满意度调查统计总报告、工信部、网络安全、工业互联网、网络强国

1. 聚焦特殊人群数字化应用！2023《特殊人群（未成年人、老年人等）网络权益保护专题报告》发布

4月15日-19日，以习近平总书记关于“网络安全为人民、网络安全靠人民”的重要讲话精神为指引，以“你我携手——构筑数字时代网络安全新防线”为主题的2023网民网络安全感满意度调查报告发布周（简称“安满周”）在全国线上线下成功举办。其中，4月16日至18日以北京为主会场圆满举办了“北京香山会议”系列活动。

作为2023“安满周”的重磅内容，第三届网络志愿服务大会暨《2023网民网络安全感满意度调查“特殊人群（未成年人、老年人等）网络权益保护”专题报告》发布会于4月16日下午在北京香山圆满举行。大会上，上海交通大学信息内容分析技术国家工程研究中心高级研究员沈金宗作为发布人，面向全社会发布报告内容。

2024《政府工作报告》中明确提出，2024年要“大力发展数字教育”、要“加强城乡社区养老服务网络建设”、要“提高网络、数据等安全保障能力”、要“完善网络综合治理，培育积极健康、向上向善的网络文化”等，对以未成年人为主要的学生群体、老年人等特殊人群的数字化应用及权益保护相关工作进行了部署。2023网民网络安全感满意度调查“特殊人群（未成年人、老年人等）网络权益保护”专题，就有关青少年权益保护、上网管理、网络环境风险与防范，以及老年人的网络素养教育和数字鸿沟等一系列问题展开调查，旨在全面了解社会公众对特殊人群网络权益保护

的观点，探讨推进未成年人和老年人以及残障人士网络权益保护工作的策略和建议。

《2023 网民网络安全感满意度调查“特殊人群（未成年人、老年人等）网络权益保护”专题报告》基于 2023 调查活动采集回收到的问卷样本，由调查活动组委会联合上海交通大学信息内容分析技术国家工程研究中心通过进行数据梳理、研究、分析而撰写形成，主要包含“未成年人网络使用的基本情况与公众态度”“未成年人网络权益保护措施及满意程度”“未成年人网络权益保护主体和责任认知”“老年人、残障人士网络权益保护情况”四大方面。并提出特殊人群网络权益保护的相关建议。

报告主要研究结果如下：

调查显示，未成年人对娱乐类网络应用的使用率明显下降，网络沉迷、不良信息等网络问题仍最受关注，对未成年人的网络使用还需加强引导和监管。此外，“饭圈”文化整治行动效果显著，后续要注重成果巩固，推动整治工作纵深发展。

（一）未成年人的娱乐类网络应用使用度呈下降趋势，网络保护举措效果显著

针对未成年人使用网络应用服务的调研显示，网络视频、网络游戏是未成年人最常用的两种服务，使用比例分别为 41.7%、45.04%，较 2022 年相比，使用频率有一定幅度的下降，其中网络视频的使用频率下降最明显，同比下降 16.67%。

总体而言，未成年人对各类网络应用的使用程度呈下降趋势，说明我国未成年人的网络沉迷问题在有关政府部门、网络平台、家长、学校等主体的多方共治下已得到明显改善。

（二）公众对未成年人上网问题仍然态度消极，加强防沉迷管理的需求保持不变

对比 2022 年数据，公众在对待未成年人上网问题上，整体仍体现为消极态度大于积极态度。虽然公众的正负面态度都有下降，但其中“需要对未成年人上网进行严格管理”占比与 2022 年十分接近，下降程度较低，显示出公众对推进青少年防沉迷管理的需求仍然强烈。

（三）未成年人上网问题复杂多样，网络沉迷和不良信息泛滥是重灾区

在对未成年人上网容易引发的问题的调研中，最受网民关注的是网络沉迷问题，占比达 66.12%，这侧面反映出未成年人在上网过程中多存在自控力不足的问题。其次，个人隐私泄露和接触色情赌博等不良信息也是受访网民关注的重点，分别占比 45.77%和 54.22%，说明个人信息泄漏以及不良信息泛滥的问题亟待解决。

（四）“饭圈”活动多乱象，良性引导需重视

在有关受访网民曾参与过的“饭圈”活动调查中，投票打榜和集资应援的占比分别为 38.85%和 35.78%，位居前两位。另外，转发控评和网上口水战也占不小的比例，为 28.63%和 20.4%。不难看出，“饭圈”活动多涉

及资本集中和舆论控制，带有恶性竞争性质，未成年人尚未形成完整的三观，极易受到“饭圈”活动的不良影响。

此外，调查数据说明，参与“饭圈”活动的群体大多希望通过这些行为，来获取认同感、归属感和爱等情绪价值。

（五）“饭圈”问题整治效果显著，维持良好风气需多方巩固

统计数据显示，2023年受访网民对“饭圈”文化的正面看法已成为主流。有10.15%的受访网民认为“饭圈”文化是资本操纵的结果，较2022年同比下降23.59%。而认为粉丝因喜爱共同事物自发聚集，共同探讨发展“饭圈”文化的受访网民比例达38.1%，较2022年大幅增长，成为了占比最多的一项看法。

在整治“饭圈”文化以及网络综艺方面，33.78%的受访网民认为卓有成效，这表明相关部门的整治行动在一定程度上取得了显著成果，得到了社会认可。但相应数据也说明，整治行动在广度和深度上还有所欠缺，相关部门应继续加强对“饭圈”文化和相关网络综艺的监管和整治力度，注重舆论导向和教育宣传，进一步巩固和拓展成果。同时，需要加强与互联网平台的合作，共同落实责任，建立长效机制，持续推动整治工作向纵深发展。

在未成年人网络权益保护上，仍有相当部分公众未感到满意，后续应加大力度，推动保护工作纵深发展。值得关注的是，网民对未成年人保护软件的效果满意度和使用率较去年皆有一定涨幅。

（一）未成年人上网管理受重视，陪伴类措施有所欠缺

数据显示，大多数中国家长都较为重视未成年人上网问题，并在引导和管理方面采取了积极措施。数据表明，大部分家长能够对未成年人上网问题积极采取行动，但“时间限制”、“上网前提”等硬性限制措施是家长解决问题的主要方式，而陪伴上网等有助于营造良好家庭氛围的温和方式则采取较少。

（二）青少年保护模式有效性不足，功能设计和内容质量亟待改进

从对青少年保护模式的了解和使用情况来看，76.09%的受访网民知道和了解青少年保护模式，表示使用过的占比约五成。

对于现行青少年保护模式的作用效果，近半数受访网民认为效果一般或不够明显，这类模式在应用的有效性上还有待提高。青少年保护模式被认为失效主要有两个方面的原因，分别是功能设计缺陷和内容质量欠佳。

（三）游戏防沉迷措施效果显著，未成年人过度游戏问题得到改善

在本次有关各大游戏公司推出的“网络宵禁”、未成年人实名认证和限时令等措施的满意度调查中，超过五成的受访网民为支持态度，认为相关措施改善未成年人沉迷游戏的作用明显。

（四）未成年人网络权益保护情况整体向好，保护工作任重道远

调研数据显示，44.48%的受访网民对未成年人网络权益保护工作表示满意，感到不满意的受访网民占比最少，为14.16%，说明未成年人网络权益保护情况呈现出整体向好的趋势，未成年人网络保护的重要性日渐凸显。不过，有41.37%的受访网民对当前未成年人网络权益保护状况持“一般”

态度，后续的保护工作还有待加强，在巩固现阶段成果的同时努力向纵深推进。

未成年人网络权益保护引起多方重视，家庭、学校和互联网平台等主体构成多方治理格局，共同推进了未成年人健康上网的引导工作。同时，未成年人网络素养教育课程工作初见成效，学校、社区应继续贯彻落实《未成年人网络保护条例》，多维度全方位培养未成年人网络素养。

（一）恶搞孩子类视频泛滥网络，未成年人网络权益认识需提高

针对“在抖音、快手等短视频平台上是否看过恶搞孩子类的视频”的调研显示，一半以上的受访网民表示看过类似视频。不难看出，恶搞孩子类的视频在互联网上的传播度并不小，甚至已经逐渐成为了平台账号博眼球博关注的一种手段。而将恶搞孩子类视频随意发到互联网上，其实是对未成年人网络权益认识的缺失。

（二）非实质性伤害也是伤害，网络绝非法外之地

调查数据显示，近六成的受访网民认为裸聊、隔空猥亵等行为已经严重侵犯被害人的身心健康和人格尊严。另有超过四成的网民表示隔空猥亵一旦发生就构成了性侵。

在预防网络侵害方面，受访网民的主要诉求是加强对青少年防侵害教育，占比超六成。另外约四成的网民对监护人、平台软件提出了要求，希望家长能够及时监管，相关 APP 落实保护未成年人措施。

（三）家庭、学校和未成年人“内外”合力，形成倡导健康上网的良性互动

有关引导未成年人健康上网的责任主体认知调查发现,与2022年相比,家庭(67.06%)和学校(58.53%)仍在引导未成年人健康上网行为上扮演重要角色。另外,认为未成年人的自我监督也是重要因素的受访网民占比47.09%,超过了去年的“互联网平台”选项,位列第三。

值得注意的是,公众逐渐认识到了未成年人自我约束的必要性,“内部”自省与家庭、学校和互联网平台等“外部”条件相结合,以形成良性相互作用。

(四) 网络素养知识普及任重道远,未成年人网络素养教育课程工作需要再接再厉

六成以上的受访网民认为网络素养涉及对隐私安全和道德规范进行意识和能力的培养,体现了人们对于公民素质和安全素养层面的重视。20.21%的受访网民认为网络素养包括基本认知和使用技能的掌握。剩下13.67%的受访网民选择了对网络信息的评估和利用能力的培养,偏向信息素养层面。

实际上,网络素养涵盖了对网络基础知识、安全意识、信息评估能力以及社交行为规范的全面培养,未来的网络素养教育中需要综合考虑这些方面,以促进全民网络素养水平的提升。

网络应用适老化改造和残疾人士辅助功能支持效果现状良好,老年人、残障人士等特殊群体的网络权益得到初步保障。跨越数字鸿沟障碍措施正在进行时,“面向老人”的专属渠道、工具和服务备受公众期待。未来,全体社会应当致力于提供包容性的数字化服务和平台,致力于消除不公平和不平等现象,确保他们能够平等、便利、安全地使用互联网。

（一）互联网操作复杂成最大痛点，网络应用适老化改造效果差强人意

调查显示，63.43%的受访网民认为技术操作过于复杂是老人使用互联网感到困难的原因。另有58.30%的受访网民表示安全和隐私，以及受骗问题也是造成老人使用互联网困难的原因。

近四成受访网民对网络应用适老化改造效果的感到满意，说明目前网络应用适老化改造已取得初步效果并得到了网民的初步认可。不过，还有近一半的受访网民表示适老化改造效果一般，改造工作仍有欠缺，后续还需进一步推进落实。

（二）跨越数字鸿沟需多措并举，“面向老人”式服务备受期待

通过对“老年人最需要什么服务或措施来跨越数字鸿沟障碍”的调查，公众普遍认为专门“面向老人”的服务效果更佳。其中希望实施单独面向老人的服务、工具和渠道的受访网民占比较大，均为五成左右。这表明社会各界对老年人群体的特殊需求和使用习惯有一定程度的认知，并希望能够保障他们在数字化社会中的便利性和舒适度。此外，立法消除数字歧视也被部分受访网民所认可，占比34.16%。

（三）公众呼吁网络应用无障碍改造，助力特殊人群融入互联网社会

调研显示，48.32%的受访网民对当前网络应用有关残障人士辅助功能支持效果表示满意，但也存在5.22%的网民对此表示不满意。残障人士的网络需求和权益逐渐被全体社会所重视，现阶段的相关辅助功能一定程度上

对残障群体起到了保护作用，但仍需进一步提升，打造一个残障人士等特殊群体能够共建共享共治的数字社会。

（一）保障未成年人用网安全需全社会助力，共同维护清朗空间

本次调查发现，近半数受访网民不了解或未尝试过青少年保护模式，对于现行青少年保护模式的作用效果，也有近半数受访网民认为效果一般或不够明显。这表明在维护未成年人网络权益保护方面，凝聚社会各界力量任重而道远。

（二）老年人如何跨越数字鸿沟受瞩目，打通用网“最后一公里”

政府部门、社会组织等应定期进行调查，了解老年人对数字化服务的需求和反馈，以及他们面临的障碍和困难。这样可以更好地了解老年人的实际需求，为制定针对性的服务和措施提供数据支持。

（三）残障人士等特殊群体用网需全社会凝聚共识，消除应用歧视

政府层面应制定包容性政策，规定数字服务必须符合无障碍标准，确保残障人士可以平等地获得和使用网络。企业层面需加强对残障人士数字化需求的研究和创新，针对残障人士的应用难点、痛点开发辅助工具和应用程序。在社会层面，各界应该加强对残障人士数字化需求的宣传和教育，促进公众对残障人士用网的重视程度。依托全社会合力，为残障人士创造更加包容和友好的用网环境。（来源：网安联）

2. 工信部公示 2024 年度制造业新型技术改造城市试点名单

近日,工信部公示 2024 年度制造业新型技术改造城市试点拟入选名单,共计 20 个,公示期为 2024 年 4 月 29 日—2024 年 5 月 9 日。

据了解,日前,财政部、工信部发布《关于开展制造业新型技术改造城市试点工作的通知》(以下简称《通知》)。《通知》提到,发挥中央财政资金引导作用,大力推进“智改数转网联”新技改,打造一批重大示范项目,促进企业设备更新、工艺升级、数字赋能、管理创新,推动传统产业转型升级,提高制造业高端化、智能化、绿色化发展水平,为巩固和增强经济回升向好态势,加快培育新质生产力、推进新型工业化提供有力支撑。

《通知》明确,支持城市采用“点线面”结合的方式组织示范项目。“点”上开展数字化智能化改造示范、“线”上开展产业链供应链数字化协同改造示范、“面”上开展产业集群及科技产业园区数字化绿色化改造示范,加快数智技术、绿色技术以及创新产品推广应用。

“申报城市应在制造业中选择 3 个左右主导行业作为技术改造重点,实施期内累计开展数字化技术改造的规上企业占比应达到 80%以上。选取的行业应符合国家区域战略发展规划和产业导向,体现本地区产业基础和特色优势,具有产值规模较大、产业集聚度较高等特征。”《通知》要求,申报城市应在确定的技术改造重点行业中,选择链主企业、龙头企业和处于产业链关键环节的企业,选择技术水平高、具有示范带动作用的标志性重大项目作为支持对象,提出重点项目清单。每个行业至少包含一家链主

企业或龙头企业，每个城市至少包含一个投资规模超 5 亿元的标志性重大项目。

与此同时，《通知》提到，中央财政对入选城市给予定额奖励。按照每个入选城市不超过 3 亿元下达奖补资金，试点实施期第一年拨付 50% 奖补资金，实施期满考核评价通过后拨付其余 50% 奖补资金。（来源：工联网）

3. 工信部：工业互联网一体化进园区“百城千园行”活动开启

日前，工信部发布《关于组织开展 2024 年工业互联网一体化进园区“百城千园行”活动的通知》（以下简称《通知》）。

工信部指出，其目的是为贯彻落实党中央、国务院决策部署，深入实施工业互联网创新发展战略，推动工业互联网高质量发展和规模化应用，发挥工业园区产业集聚优势，推动工业互联网向地市县域落地普及，促进广大企业特别是中小企业加快数字化转型，促进经济高质量发展。

本次“百城千园行”活动主题为“工赋园区 数智未来”。活动包括政策进园区、设施进园区、技术进园区、标准进园区、应用进园区、企业进园区、服务进园区，包括但不限于高新技术产业开发区、经济开发区等各级行政园区，以及先进制造业集群、中小企业特色产业集群等重点产业发展载体。

（一）政策进园区。各地工业和信息化主管部门、通信管理局组织相关产业组织、研究机构、行业专家等对国家和本地工业互联网相关政策开

展宣贯工作，推广普及政策体系，对标识“贯通”行动计划、5G 工厂建设指南、“5G+工业互联网”融合应用先导区、设备更新和技术改造等相关文件进行解读。引导园区企业了解财政资金、产业基金等对工业互联网的支持政策。

（二）设施进园区。推动企业利用 5G、时间敏感网络、工业光网、IPv6 等新型网络技术进行园区网络优化升级，鼓励园区企业开展工业 5G 专网试点建设；鼓励行业龙头企业建设标识解析二级节点，引导园区企业普遍接入标识解析体系；鼓励园区结合产业特点和实际需求，推动园区工业设备和业务系统上云上平台；深入实施工业互联网安全分类分级管理，引导园区企业接入国家安全态势感知平台。

（三）技术进园区。引导园区企业加快人工智能、大数据、区块链、数字孪生、边缘计算等新一代信息通信技术与工业互联网的融合应用，加快开展工业级 5G 芯片/模组/网关、工业光网、云化 PLC、安全设备等技术产品创新应用，发布服务园区的技术清单和产品清单，鼓励园区、企业开展重点行业设备更新和技术改造。

（四）标准进园区。开展工业互联网相关标准体系宣贯，引导园区企业实施工业互联网相关标准，加快工业互联网体系架构、数据互通、行业应用等国家标准、行业标准、团体标准在园区落地普及。鼓励企事业单位、研究机构、产业协会等参与标准研制工作，推动发布园区标准清单。

（五）应用进园区。推动园区企业编制、实施工业互联网与细分行业融合应用指南，为中小企业提供可复制、可推广、轻量化、低成本的解决

方案。鼓励链主企业打造工业互联网典型集成创新应用标杆，带动中小企业链式数字化转型。引导园区推广平台化设计、智能化生产、个性化定制、网络化协同、服务化延伸、数字化管理、绿色化生产、精细化投融、可视化治理等工业互联网新模式新业态，培育一批典型应用场景和样板标杆。

（六）企业进园区。引导工业企业、信息通信企业等入驻园区，实现园区产业链精准招商。鼓励规划咨询、设施建设、系统集成、应用服务等各类解决方案供应商企业进园区，为园区大中小企业提供一体化解决方案。坚持场景牵引，需求导向，鼓励搭建园区工业互联网供需资源池，发布供需目录清单。

（七）服务进园区。组织银行、保险、基金等金融机构深入园区，优化金融资源配置，为企业提供个性化、精准化的金融产品和服务。鼓励高校、事业单位、行业协会深化产教融合、科教融汇，开展培训讲座、实践实训、能力评价、技能交流等，联合打造园区人才服务体系。推动园区组织工业互联网专家开展诊断评估，帮助园区企业明确改造路径，制定针对性解决方案，打造一批园区示范应用标杆，推动园区数字化、网络化、智能化、绿色化发展。

《通知》指出，2024年5月底前，各地工业和信息化主管部门、通信管理局系统梳理本地区园区名录，对有发展基础和条件、数字化转型需求明显的园区，制定活动实施方案，报工业和信息化部（信息通信管理局）。2024年10月底前，各地工业和信息化主管部门、通信管理局组织开展本地进园区活动，推动园区企业提升利用工业互联网加快数字化转型的意识、

能力和成效。2024年11月底前，组织开展成效评估，并形成活动总结报工业和信息化部（信息通信管理局）。（来源：工联网）

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，搭建合作交流平台，助推网络安全发展。广州网络空间安全协会、科大讯飞股份有限公司承办的信创赋能（第三期）——“走进科大讯飞·探索中国智能先驱者”活动顺利举行；北京网络空间安全协会作为承办单位入列“国家专业技术人员知识更新工程 2024 年高级研修项目计划”；“巴渝杯”大学生网络安全联赛——理论知识竞赛、CTF 夺旗竞赛成功举办；大连市信息网络安全协会发布“大连市信息网络安全协会组建专家库”的通知背景与目的；徐州网络公共安防技术协会召开无人机分会筹备会议；东莞市信息技术联合会举行新一代信息技术新媒体运营中心授牌仪式等。

关键词：信创、大学生网络安全、信息安全、网络安全、工业互联网、网络强国

1. 信创赋能（第三期）——“走进科大讯飞·探索中国智能先驱者”顺利举办

4月29日，由广东省网络空间安全协会、广东省数字安全协会、广东省科协信创联合体联合主办，广州网络空间安全协会、科大讯飞股份有限公司承办的信创赋能（第三期）——“走进科大讯飞·探索中国智能先驱者”活动顺利举行，来自深圳金蝶、中理科技、广州亚信技术、广州联通、广州东华职业学院、杭州安恒信息技术等30多家企业和学校的代表参加了本次活动，活动由广东省网络空间安全协会会员服务中心副主任兼业务服务部部长蔡舒婷主持。

科大讯飞组织了专员为前来观摩的代表进行了细致的讲解，在科大讯飞人工智能展厅，各单位代表们被科大讯飞体现科技元素的环境所吸引，参观了展厅各展示区，近距离体验AI在智慧司法、智慧医疗、智慧教育、智慧汽车等方面的前沿产品，感受讯飞科技将AI赋能于各行各业的优秀应用。

本次活动为深入贯彻党的二十大和中央经济工作会议精神，推进信创行业的资源整合和信息共享，学习和借鉴优秀企业的典型先进经验和做法，加强协会会员之间的学习交流和互动合作有一定促进作用。广东省网络空间安全协会还将持续举办相关合作交流活动，全方位搭建行业交流和合作的平台。（来源：网安联）

2. 北京网络空间安全协会作为承办单位入列“国家专业技术人才知识更新工程 2024 年高级研修项目计划”

2024 年 3 月 22 日，人力资源社会保障部办公厅印发了《关于专业技术人才知识更新工程 2024 年高级研修项目计划的通知》，并下发给各省、自治区、直辖市及新疆生产建设兵团人力资源社会保障厅（局），以及中共海南省委人才发展局，国务院有关部委、直属机构人事部门，有关行业协会、企业、事业单位落实执行。

北京市今年有七个选题入列。北京网络空间安全协会作为《信息技术应用创新及安全能力提升》选题承办单位入列，在北京市人力资源和社会保障局统一领导下组织实施高级研修项目具体工作。

高级研修项目是培养高层次急需紧缺人才的重要抓手，对于支撑引领经济社会高质量发展、推动形成新质生产力具有重要意义。参与高级研修项目学员审核合格后将颁发《国家专业技术人才知识更新工程培训证书》，培训学时也记入专业技术人员继续教育学时（继续教育学时也是申报北京新增“网络空间安全专业职称评审”的申报条件）。高级研修项目学员可凭姓名和身份证号在国家专业技术人才知识更新工程公共服务平台（<http://zsgx.mohrss.gov.cn>）查询和打印本人证书。

《信息技术应用创新及安全能力提升》高级研修项目将免费为各省（自治区、直辖市）、新疆生产建设兵团，党政、金融、电信、交通、电力、石油、航空航天、医疗、教育等 2+8 行业单位及企业机构的信息化数字化负责人、高级技术人员、高级管理人员提供研修课程，学员人数控制在 70

到 100 人。研修项目将围绕共同发展新质生产力下信息技术应用创新及安全能力提升，邀请工程院士、行业专家、领域学者和企业实战专家，以专题报告、专题研讨、现场教学等方式进行研修授课，以培养一批创新性、应用型和技术型的信创人才。（来源：北京网络空间安全协会）

3. “巴渝杯”大学生网络安全联赛——理论知识竞赛、CTF 夺旗竞赛成功举办！

4 月 24 日，2024 “巴渝杯”大学生网络安全联赛-理论知识竞赛、CTF 夺旗竞赛在重庆科技大学拉开序幕，来自重庆各大高校 82 支队伍，240 多人参加了本次比赛。重庆信息安全产业技术创新联盟秘书长马传龙主持了开幕式并宣布比赛开始，重庆科技大学智能技术与工程学院副院长雷亮进行致辞。

2024 “巴渝杯”大学生网络安全联赛采取积分制，将逐一进行理论知识竞赛、CTF 夺旗竞赛、网络安全作品赛和 AWD 网络安全攻防对抗竞赛比赛，本次比赛以理论知识竞赛、CTF 夺旗竞赛模式进行，经过 4 小时的持续鏖战，按照积分排名，最终有 47 支队伍获得证书。

在比赛的同时，2024 网络安全人才培养研讨会暨校企合作交流会也在同步进行，会议邀请了各高校、企业代表，大家各抒己见，分享了网络安全专业建设与人才培养经验，并针对网络安全人才培养的实际问题、行业热点、痛点问题进行有针对性、全面深入的交流和研讨，校企双方就师资

共建、产教融合、实习就业等方面达成初步合作意向。（来源：重庆信息安全产业技术创新联盟）

4. 大连市信息网络安全协会发布“大连市信息网络安全协会组建专家库”的通知背景与目的

为深入贯彻落实习近平总书记关于网络安全和信息化工作的重要指示，为进一步提升大连网络和数据安全管理水平，充分发挥行业专家在技术决策、咨询服务等方面作用。

大连市信息网络安全协会经过深入研究和广泛调研，决定组建网络安全专家库。这一举措旨在汇聚网络安全领域的精英人才，构建一支具备高度专业素养和实战能力的专家团队，为大连市网络安全事业提供强大的智力支持和技术保障。（来源：大连市信息网络安全协会）

5. 徐州网络公共安防技术协会召开无人机分会筹备会议

5月11日下午，徐州网络公共安防技术协会在秉信人力资源集团会议室召开了无人机分会筹备会议，来自全市20多家机关、企事业单位30位嘉宾参加了会议。协会卜庆亚理事长、孙吉祥副理事长、马继刚秘书长及秘书处工作人员参加会议。

潘万功总经理首先致欢迎辞，并介绍了集团概况。秉信人力资源集团2018年植根业界，至2023年春季迈出了战略性的一步，涉足无人机领域，专攻无人机应用培训与技能认证服务。培训项目精准定位多元群体：在职员工渴求技能升级、城镇失业人员寻求再就业途径、灵活就业者探索新机遇、特殊群体成员及退役军人转型发展，至今已卓有成效地培育近500名学员，其中高达80%的学员成功取得无人机操作资质，为无人机技术的普及与深化应用奠定了坚实的基石。

卜庆亚理事长汇报协会前期无人机分会筹备工作和思路、打算。他强调，成立无人机分会旨在响应行业监管要求，汇聚无人机领域内的杰出企业，构建一个互学互鉴、资源共享、协同发展的高端平台。在协会的引领下，携手直面并解决无人机产业发展中的安防挑战与难题，积极代言企业权益，减少运营成本，提升运作效率，同时强化行业自律性，守护行业形象，共筑无人机产业稳健且蓬勃发展的基石。

会议核心议题聚焦于无人机分会的命名、组织结构确立以及全市范围无人机应用技能竞赛的精细筹划，各方展开了深入而富有成效的讨论，力求每一项决策都能精准助推行业前行。

会议中，关于分会名称的讨论尤为热烈。与会代表们一致认为，分会应超越“无人机”这一传统定义，拥抱“低空经济”带来的广泛机遇。

在讨论环节，企业家们纷纷强调了建立互信、开放沟通的重要性，倡导构建一个团结协作、高效有序的团队氛围，以共同的社会责任感和使命感推动行业发展。（来源：徐州网络公共安防技术协会）

6. 东莞市信息技术联合会举行新一代信息技术新媒体运营中心授牌仪式

为进一步加强协会能力建设，提升服务水平，充分发挥视频号等推广渠道的作用，做好会员单位的宣传推广服务工作，展示会员风采，提高会员单位知名度和影响力，4月29日东莞市信息技术联合会新一代信息技术新媒体运营中心授牌（下称新媒体运营中心）在广东栖贤谷传媒有限公司正式揭牌成立！

新媒体运营中心主任、联合会秘书长温婷婷（下称温秘）宣读关于设立新一代信息技术多媒体运营中心的复函。新媒体运营中心执行主任卢少红（下称卢总）致欢迎辞并向嘉宾介绍新媒体运营中心的主要业务及未来发展。卢主任表示希望能够在联合会指导下加快推进东莞市信息技术行业发展，促进信息技术宣传再上新台阶。

揭牌以后，由新媒体运营中心项目策划温捷介绍目前的基本情况，从活动策划、短视频运营、品牌孵化、信息流代运营等四个方面阐述了整套运营中心的方案。

会后，各行业专家就此次授牌仪式表示受益匪浅，并结合自身工作，畅谈自身体会，交流收获心得。

新媒体运营中心致力为东莞市各企业线上发展需求，以新媒体平台为载体，通过图文、视频、直播等多种形式，全方位展示运营中心的最新动

态、技术进展、行业应用等多方面内容，同时，新媒体运营中心致力于打造一个互动交流平台，让广大受众能够更好的了解、学习、推动产业创新与发展。（来源：东莞市信息技术联合会）

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

网络安全漏洞 数据安全 网络安全审查
网络信息内容生态治理 关键信息基础设施保护 网络安全等级保护
网络安全人才培养 数据跨境流动 新技术新应用
网络安全法
网络安全行政执法
网络安全行刑衔接
物联网安全 个人信息保护 供应链安全
密码法治

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

.....

