网安联
Wang An Lian

网络与数据安全治理前沿洞察

Frontiers of Regulatory Oversight in CyberSecurity and Data Governance

2023年10月 第3期(总 第3期)

2023年10月20日

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

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）

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：立法动向.....1

（一） 国家层面动向.....2

1. 十四届全国人大常委会公布立法规划：包括网络犯罪防治法等2

2. 《治安管理处罚法（修订草案）》公布：违规出售或提供个人信息或被行政拘留.....2

3. 国务院常务会议审议通过《未成年人网络保护条例（草案）》3

4. 国务院办公厅印发《提升行政执法质量三年行动计划（2023—2025 年）》.....3

5. 国务院办公厅印发《关于依托全国一体化政务服务平台建立政务服务效能提升常态化工作机制的意见》.....4

（二） 部委层面动向.....5

1. 两高一部印发《关于依法惩治网络暴力违法犯罪的指导意见》5

2. 国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》.....6

3. 国家密码管理局印发《商用密码检测机构管理办法》《商用密码应用安全性评估管理办法》.....7

4. 五部门印发《元宇宙产业创新发展三年行动计划（2023－2025 年）》.....8

5. 工信部发布《工业和信息化部元宇宙标准化工作组筹建方案（征求意见稿）》.....9

6. 国家金融监管总局等五部门印发《关于规范货币经纪公司数据服务有关事项的通知》 9
7. 全国信安标委发布四项网络安全国家标准 10
（三） 地方层面动向 11
1. 武汉市人民政府办公厅印发《武汉建设国家人工智能创新应用先导区实施方案（2023-2025 年）》 11
2. 贵州省大数据发展管理局发布《贵州省数据要素登记管理办法（试行）》（征求意见稿） 12
3. 贵州省工业和信息化厅印发《贵州省工业领域数字化转型实施方案（2023-2025 年）》 13
4. 长沙市数据资源管理局印发《长沙市数据官制度建设实施意见》 13
5. 北京经开区印发《北京经济技术开发区首席数据官制度工作方案》 14
6. 四川省印发《四川省元宇宙产业发展行动计划（2023—2025 年）》 14
7. 福建省印发《福建省加快推进数据要素市场化改革实施方案的通知》 15
境内前沿观察二：治理实践 17
（一） 公安机关治理实践 19
1. 上海公安机关：累计对 2800 余家单位开展执法检查 19

2. 江苏公安“净网 2023”专项行动取得显著成效 20
3. 北京警方通报打击整治网络乱象专项行动成果 21
4. 河南公安深入推进“净网 2023”专项行动 22
5. 江苏公安机关公布多起不履行数据安全保护义务行政执法案例 23
6. 因存在数据泄露隐患，北京网安适用《数据安全法》处罚两家违法单位 25
7. 因导致用户设备被漏洞利用攻击，一网络产品提供者被处罚 26
8. 江西南昌网安部门走访全市 MCN 机构 27
9. 因导致信息系统被入侵，天津警方对一单位进行处罚 27
10. 公安机关依法严厉打击缅北涉我国电信网络诈骗犯罪取得重大战果 28
11. 最高检、公安部启动第三批 5 起特大跨境电信网络诈骗犯罪案件联合挂牌督办 29
12. 山东烟台网安部门打掉一黑客犯罪团伙，涉案资金 30 亿 ... 30
13. 广东网警打掉 22 个“网络水军”团伙， 涉案金额 5.3 亿元 31
14. 江苏警方公布打击网络违法犯罪 6 起典型案例 32
15. 张家界警方全链条团灭 1600 余台非法侵入计算机系统终端案 32
16. 四川攀枝花警方打掉一犯罪团伙，超 1400 万部“老年机”被木马控制自动扣费 33
17. 重庆北碚警方破获多起帮助信息网络犯罪活动案 35
18. 浙江温州警方打掉一犯罪团伙，专门针对企业投放木马程序 37

（二） 网信部门治理实践 38
1. 国家网信办公布第二批深度合成服务算法备案清单 38
2. 国家互联网信息办公室公布第一批应用程序分发平台备案编号 39
3. 中央网信办部署开展“清朗·生活服务类平台信息内容整治”专项行动 39
4. “清朗·杭州亚运会和亚残运会网络环境整治”专项行动查处一批违法违规网络账号 40
5. 国家互联网信息办公室对知网依法作出网络安全审查相关行政处罚 41
6. 网信部门依法查处腾讯 QQ 危害未成年人身心健康违法案件 . 41
7. 海南省网信办通报 23 款移动应用程序违法违规收集使用个人信息情况 42
8. 因网站被植入非法网站暗链，重庆市巴南区网信办对一企业处以警告 43
9. 因设置迷惑性按钮诱导消费者“入会”，“胡子大厨”被严肃约谈 43
10. 公民个人信息泄露遭境外披露兜售，上海一政务信息系统技术服务公司被行政处罚 44
11. 上海网信办联合多部门发布《上海市互联网证券信息服务企业合规指引》 45

12. 上海市网信办、市市场监管局对部分房产中介、汽车 4S 店开展个人信息保护工作联合检查 46
13. 上海市网信办对属地 46 款 App 收集使用个人信息情况开展专项检查 47
（三） 通信管理部门治理实践 48
1. 工信部及多省通信管理局通报或下架侵害用户权益 APP/SDK 48
2. 江苏省信息通信行业“铸网 2023”专项行动：累计发现网络安全风险 1000 余个 50
（四） 其他部门治理实践 51
1. 因重要信息系统突发事件未报告，北京中关村银行被罚 20 万元 51
2. 深圳市人民检察院联合多部门发布《深圳市企业数据合规指引》 51
境外前沿观察：月度速览十则 53
1. 澳大利亚计划建立六大网络盾牌，确保国家网络安全 54
2. “英美数据桥”正式确定，于 10 月 12 日生效 54
3. 欧盟《数据治理法》全面施行 55
4. 迪拜《数据保护条例（修正案）》正式施行，新增人工智能相关规定 55
5. 欧盟委员会发布《关于<协调联盟应对重大跨境关键基础设施中断的蓝图>的理事会建议提案》 56

6. 英国 ICO 发布《北爱尔兰警察局数据保护审计报告》执行摘要56

7. 德国因数据盗窃、网络间谍破坏活动造成的损失将达到 2060 亿欧元 57

8. 英国 2023 年关键信息基础设施网络攻击数量创历史新高 57

9. 斯里兰卡国家政务云被攻击，四个月数据被删除 58

10. 因非法追踪用户位置数据，谷歌支付 9300 万美元和解 59

行业前沿观察一：2023 网络诚信建设专题样本采集工作启动 60

1. 2023 网络诚信建设专题样本采集工作启动仪式在京举行 61

2. “网络诚信建设”专题支撑《中国网络诚信发展报告 2024》 62

3. “网络诚信建设”专题促进志愿团队转型升级…… 63

4.网络诚信领域向上向善形势巩固，2024 调查结果值得期待… 64

行业前沿观察二：专业技术评价迫在眉睫..... 66

1.广东：先行先试，开全国网安人才专业技术评价之先河.....67

2.四川：全国首批建成网信职称评价体系.....67

3.江苏：2021 年 9 月网络安全行业拥有独立的评价体系和标准…69

4.山东：首次设立网络安全工程职称，填补网信职称评价空白…70

境内前沿观察一：立法动向

导读：9 月，十四届全国人大常委会公布立法规划，网络安全法（修改）、网络犯罪防治法均提上日程。国务院办公厅印发《提升行政执法质量三年行动计划（2023—2025 年）》，强调行政执法质量直接关系法治政府建设成效，提出全面提升行政执法人员能力素质、全面推进严格规范公正文明执法等 6 项重点任务，涉及落实行政裁量权基准、引导受处罚企业合规、行政执法标准化制度化培训等方面。国家密码管理局印发《商用密码检测机构管理办法》《商用密码应用安全性评估管理办法》，加强商用密码检测机构管理，规范商用密码应用安全性评估工作。

工信部等 5 部门联合印发《元宇宙产业创新发展三年行动计划（2023—2025 年）》、工信部发布《工业和信息化部元宇宙标准化工作组筹建方案（征求意见稿）》，推动元宇宙创新发展，加快元宇宙标准化工作。

长沙市数据资源管理局、北京经开区相继发布《长沙市数据官制度建设实施意见》《北京经济技术开发区首席数据官制度工作方案》，加快数据官制度在本地的落实。

关键词：网络犯罪防治法、提升行政执法质量、网络暴力、数据跨境流动、商用密码管理、数据官制度、元宇宙

（一）国家层面动向

1. 十四届全国人大常委会公布立法规划：包括网络犯罪防治法等

9 月 7 日，十四届全国人大常委会公布立法规划，包含三类项目共 130 件法律草案。

第一类项目是条件比较成熟，任期内拟提请审议的法律草案，共计 79 件，包括网络安全法（修改）、治安管理处罚法（修改）等。同时，贯彻落实党中央决策部署，对维护国家安全，推进科技创新和人工智能健康发展，完善涉外法律体系等，要求制定、修改、废止、解释相关法律，或者需要由全国人大及其常委会作出相关决定的，适时安排审议。

第二类项目是需要抓紧工作、条件成熟时提请审议的法律草案，共计 51 件，包括电信法、数字经济促进法、网络犯罪防治法、人民警察法等。

第三类项目是立法条件尚不完全具备、需要继续研究论证的立法项目，包含数据权属和网络治理等方面，经研究论证，条件成熟时，可以安排审议。（来源：中国人大网）

2. 《治安管理处罚法（修订草案）》公布：违规出售或提供个人信息或被行政拘留

9 月 1 日，中国人大网公布《中华人民共和国治安管理处罚法（修订草案）》，向社会公众征求意见。

在侵犯人身权利、财产权利的行为和处罚方面，修订草案规定，违反规定向他人出售或者提供个人信息的，处十日以上十五日以下拘留；情节较轻的，处五日以上十日以下拘留。

在执法监督方面，修订草案增加对个人信息的保护，要求公安机关及其人民警察不得将在办理治安案件过程中获得的个人信息，依法提取、采集的相关人体生物识别信息、样本用于与治安管理、打击犯罪无关的用途，或者出售、提供给他人。人民警察办理治安案件违反上述规定的，依法给予处分，构成犯罪的依法追究刑事责任。（来源：中国人大网）

3. 国务院常务会议审议通过《未成年人网络保护条例（草案）》

9 月 20 日，国务院总理李强主持召开国务院常务会议，审议通过《未成年人网络保护条例（草案）》。会议指出，未成年人是国家的未来、民族的希望。要筑牢未成年人网络保护的法治支撑，推动各有关方面严格落实未成年人网络保护责任，引导支持相关企业积极落实条例、做到合规经营，促进未成年人健康成长。（来源：司法部）

4. 国务院办公厅印发《提升行政执法质量三年行动计划（2023—2025 年）》

8 月 9 日，国务院办公厅印发《提升行政执法质量三年行动计划（2023—2025 年）》，指出行政执法是行政机关履行政府职能、管理经济社会事务的重要方式，行政执法质量直接关系法治政府建设成效。

行动计划围绕全面提升行政执法人员能力素质、全面推进严格规范公正文明执法、健全完善行政执法工作体系、加快构建行政执法协调监督工作体系、健全行政执法和行政执法监督科技保障体系、不断强化行政执法保障能力6项重点任务，提出17项具体工作举措。

行动计划要求，聚焦人民群众反映强烈的运动式执法、“一刀切”执法、简单粗暴执法、野蛮执法、过度执法、机械执法、逐利执法等不作为乱作为问题，开展专项整治和监督行动。全面落实行政裁量权基准制度，加强行政裁量权基准的动态管理和备案审查。综合运用多种方式督促引导受处罚企业加强合规管理、及时整改违法问题，防止以罚代管。探索建立涉企行政执法案件经济影响评估制度，依法降低行政执法对企业的负面影响。建立健全行政执法标准化制度化培训机制，开展分类分级分层培训，在完成政治理论教育和党性教育学时的基础上，确保行政执法人员每人每年接受不少于60学时的公共法律知识、业务知识和行政执法技能培训，原则上于2024年6月前完成对本地区、本部门行政执法队伍的全员轮训。（来源：中国政府网）

5. 国务院办公厅印发《关于依托全国一体化政务服务平台建立政务服务效能提升常态化工作机制的意见》

8月18日，国务院办公厅印发《国务院办公厅关于依托全国一体化政务服务平台建立政务服务效能提升常态化工作机制的意见》。

意见要求强化新技术应用赋能机制。依托全国一体化政务服务平台，探索利用大数据、人工智能、区块链等新技术，分析预判企业和群众办事需求，通过智能问答、智能预审、智能导办等方式，建设企业服务空间和个人服务空间，提供智能化、个性化、精准化服务，推动惠企利民政策和服务“免申即享、直达直享、快享快办”。

意见要求优化政务数据有序共享机制，更好发挥公共通道作用。加快推动制定政务数据共享条例，明确数据提供、使用部门的权责义务，规范政务数据采集、共享、使用等流程。依托全国一体化政务服务平台数据共享枢纽，推动政务数据跨地区、跨部门、跨层级、跨系统、跨业务共享利用。强化政务数据目录编制，做好动态更新、同源发布。（来源：中国政府网）

（二）部委层面动向

1. 两高一部印发《关于依法惩治网络暴力违法犯罪的指导意见》

9 月 20 日，两高一部印发《关于依法惩治网络暴力违法犯罪的指导意见》。

指导意见指出，要充分认识网络暴力的社会危害，依法维护公民权益和网络秩序。人民法院、人民检察院、公安机关要充分认识网络暴力的社会危害，坚持严惩立场，依法能动履职，为受害人提供有效法律救济，维护公民合法权益，维护公众安全感，维护网络秩序。

指导意见明确，要准确适用法律，依法严惩网络暴力违法犯罪。依法惩治网络诽谤、网络侮辱、侵犯公民个人信息等七类网络暴力违法行为，依法支持民事维权，准确把握违法犯罪行为的认定标准。

指导意见强调，要畅通诉讼程序，及时提供有效法律救济。落实公安机关协助取证的法律规定，准确把握侮辱罪、诽谤罪的公诉条件，依法适用侮辱、诽谤刑事案件的公诉程序，加强立案监督工作，依法适用人格权侵害禁令制度，依法提起公益诉讼。（来源：最高人民法院）

2. 国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》

9 月 28 日，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》，涉及十一项内容。

征求意见稿明确不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形，包括：（1）国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据的；（2）不是在境内收集产生的个人信息向境外提供的；（3）为订立、履行个人作为一方当事人的合同所必需，如跨境购物、跨境汇款、机票酒店预订、签证办理等，必须向境外提供个人信息的；（4）按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理，必须向境外提供内部员工个人信息的；（5）紧急情况下为保护自然人的生命健康和财产安全等，必须向境外提供个人信息的。

征求意见稿还指出，未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。自由贸易试验区可自行制定本自贸区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，报经省级网络安全和信息化委员会批准后，报国家网信部门备案。负面清单外数据出境，可以不申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。（来源：中国网信网）

3. 国家密码管理局印发《商用密码检测机构管理办法》《商用密码应用安全性评估管理办法》

9 月 26 日，国家密码管理局印发《商用密码检测机构管理办法》《商用密码应用安全性评估管理办法》，均自 2023 年 11 月 1 日起施行。

《商用密码检测机构管理办法》共 29 条，涉及总体要求、资质认定条件和程序、从业规范、监督检查及法律责任等内容。办法明确国家密码管理局负责全国商用密码检测机构的资质认定和监督管理。县级以上地方各级密码管理部门负责本行政区域内商用密码检测机构的监督管理。商用密码检测机构应当在资质认定业务范围内从事商用密码检测活动。国家密码管理局制定并公布商用密码检测机构资质认定基本规范和商用密码检测机构资质认定业务范围。

《商用密码应用安全性评估管理办法》共 21 条，涉及总体要求、程序及内容要求、实施规范、监督检查及法律责任等内容。从事商用密码应用

安全性评估活动，向社会出具具有证明作用的商用密码应用安全性评估数据、结果的机构，应当经国家密码管理局认定，依法取得商用密码检测机构资质。（来源：国家密码管理局）

4. 五部门印发《元宇宙产业创新发展三年行动计划（2023－2025年）》

8月29日，工信部办公厅、教育部办公厅、文化和旅游部办公厅、国务院国资委办公厅、国家广播电视总局办公厅联合印发《元宇宙产业创新发展三年行动计划（2023－2025年）》。

行动计划强调完善元宇宙协同治理机制。持续完善元宇宙政策法规，加强元宇宙风险跟踪研判，打造部门协同、社会参与的治理体系。明晰元宇宙监管主体职能，完善内容审查、风险处置、违规处理等规则流程。开展元宇宙伦理研究，将主流价值和伦理要求贯穿技术研发应用全过程。加强元宇宙行业自律，提升企业合规能力和社会责任意识，压实主体责任。加强社会监督，防范概念过度炒作，保障产业公平健康发展。

行动计划要求强化安全保障能力建设。加强元宇宙安全技术研究，常态化开展安全风险评估，建立安全风险事件处置机制。指导元宇宙企业加强信息安全管理，建立健全违法信息监测、识别和处置机制，遏制虚假有害信息传播，切实防范网络诈骗等违法活动。建立元宇宙数据治理框架，加强数据安全和出境管理，规范对用户信息的收集、存储、使用等行为，提升数据安全治理能力和个人信息的保护水平。（来源：工信部）

5. 工信部发布《工业和信息化部元宇宙标准化工作组筹建方案（征求意见稿）》

9 月 18 日，工信部发布《工业和信息化部元宇宙标准化工作组筹建方案（征求意见稿）》，提出组建工信部元宇宙标准化工作组的具体方案，加强我国元宇宙标准化工作。

征求意见稿指出，元宇宙安全风险突显，亟需通过标准引导向善发展。元宇宙涉及到用户生理、行为、资产等个人敏感信息采集分析，存在多种数字身份、内容呈现方式和价值交换途径。传销诈骗、网络暴力、算法捆绑、数据滥用等乱象频发，伦理、数据安全、信息安全等风险突出，亟需通过标准化支撑监管，明确安全红线要求，积极引导元宇宙向善发展。

征求意见稿强调，强化前沿技术融合，推动行业标准预研。面向隐私保护、内容监管、数据安全等元宇宙领域中新技术、新产品、新业态、新模式，加快开展关键技术和产业发展研究，加强与脑机接口、生成式人工智能、量子信息等领域技术融合创新。（来源：工信部）

6. 国家金融监管总局等五部门印发《关于规范货币经纪公司数据服务有关事项的通知》

8 月 25 日，国家金融监督管理总局、中国人民银行、中国证券监督管理委员会、国家互联网信息办公室、国家外汇管理局联合印发《关于规范货币经纪公司数据服务有关事项的通知》。

通知指出，货币经纪公司应当将数据治理纳入公司治理范畴，建立与业务发展目标相适应的数据安全治理体系，健全数据安全管理制度，加强经纪人员执业规范性管理，构建覆盖数据全生命周期和应用场景的安全保护机制，开展数据安全风险监测评估，保障数据服务安全稳健开展。

通知强调，货币经纪公司应严格落实信息科技监管要求，加强信息科技风险管理体系建设，提升信息科技外包风险管控能力，严格控制生产系统访问权限，加强数据安全保护，确保网络和数据安全。（来源：国家金融监督管理总局）

7. 全国信安标委发布四项网络安全国家标准

9 月 15 日，全国信安标委发布四项网络安全国家标准，分别是：

（1）GB/T 32914-2023《信息安全技术 网络安全服务能力要求》

（2）GB/T 32916-2023《信息安全技术 信息安全控制评估指南》

（3）GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》

（4）GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》

（来源：全国信安标委）

（三）地方层面动向

1. 武汉市人民政府办公厅印发《武汉建设国家人工智能创新应用先导区实施方案（2023-2025 年）》

8 月 30 日，武汉市人民政府办公厅印发《武汉建设国家人工智能创新应用先导区实施方案（2023-2025 年）》。

方案提出六项主要任务，分别是实施人工智能技术突破计划、人工智能要素伙伴计划、人工智能产业提能计划、人工智能场景应用计划、人工智能集聚发展计划、人工智能生态营造计划。

方案要求加强大模型要素支撑。推动头部企业联合多模态人工智能产业联盟组建创新联合体，创建人工智能方向制造业创新中心，开展大模型创新算法开发与开源开放。培育高质量数据要素市场。培育数源商、数据开发商、数据服务商、平台服务商等多元主体，做大做强武汉数据集团。优先推进企业登记监管、卫健、教育、交通运输、气象等高价值行业数据资源安全合规开放，推进多模态公共数据集建设，在全市建设 5 个以上公共数据集。利用隐私计算、数据安全流通等技术，推进行业数据与企业数据融通使用，发展数据清洗、信息抽取、标注、分类、注释等服务。（来源：武汉市人民政府）

2. 贵州省大数据发展管理局发布《贵州省数据要素登记管理办法（试行）》（征求意见稿）

8月31日，贵州省大数据发展管理局发布《贵州省数据要素登记管理办法（试行）》（征求意见稿），从登记机构、登记主体、登记内容、登记程序、登记类型、安全管理等方面规范数据要素登记。

登记机构方面，征求意见稿指出，贵州省数据流通交易服务中心是贵州省数据要素登记工作的登记机构，进行统一的数据要素登记服务，建立权益保护和流转机制，运用云计算、区块链等新兴技术，建设安全可信的数据要素登记OID服务平台，支撑数据要素登记申请、合规审核、在线公示、颁发凭证、存证溯源等全流程登记工作，保障数据生产、流通、使用过程中各参与方享有的合法权益。

登记程序方面，征求意见稿强调，数据要素登记按照申请、受理、审查、在线公示、异议处理和发证等程序组织实施。登记主体、登记机构应通过数据要素登记OID服务平台申请登记，开展登记审查工作。

安全管理方面，征求意见稿强调登记机构应当建立重大安全风险监测、风险警示、风险处置等风险控制制度以及突发事件应急处置预案，按要求保管登记相关资料。建立保护数据传输、存储和使用安全的基础设施，加强防攻击、防泄漏、防窃取的监测、预警、控制和应急处置能力建设。（来源：贵州省大数据发展管理局）

3. 贵州省工业和信息化厅印发《贵州省工业领域数字化转型实施方案（2023-2025 年）》

9 月 1 日，贵州省工业和信息化厅印发《贵州省工业领域数字化转型实施方案（2023-2025 年）》，聚焦八大工程，提出四项保障措施，推动工业领域数字化转型。

实施方案强调要实施工信安全保障工程。引导企业加强数据规划管理和开发利用，推进工业数据分类分级。对照国家有关标准，面向重点企业开展数据安全评估和应急演练工作，落实企业主体责任，提升数据安全风险防护能力。构建工业信息安全态势感知网络，加强各级工信主管部门监测保障和应急处置能力。（来源：贵州省工业和信息化厅）

4. 长沙市数据资源管理局印发《长沙市数据官制度建设实施意见》

9 月 14 日消息，长沙市数据资源管理局近日印发《长沙市数据官制度建设实施意见》。

实施意见强调，要建立覆盖市区两级和相关单位的数字化人员队伍体系。市级层面，首席数据官由分管数据管理工作的副市长担任，首席数据执行官由数据资源管理部门主要负责人担任。区县（市）、园区以及市直相关单位参照市级建立数据官组织体系，分别设首席数据官、首席数据执行官、业务工作人员、技术工作人员各 1 名，按照职责设定开展相关工作。

实施意见指出，数据官主要承担七方面职责：统筹整体规划、推进数据汇聚、深化数据应用、实施源头治理、发展数字产业、提升数字素养、确保数据安全。（来源：长沙市数据资源管理局）

5. 北京经开区印发《北京经济技术开发区首席数据官制度工作方案》

9 月 15 日，北京经济技术开发区印发《北京经济技术开发区首席数据官制度工作方案》。

工作方案指出，经开区采用“首席数据官+数据专员+部门联系人”的“三级工作制”，建立起上下贯通的数据治理组织体系，由各部门主要负责同志担任“首席数据官”，各部门信息化分管领导担任“数据专员”，同时设立一名部门联系人。

工作方案强调，首席数据官需要对所在部门数据肩负 7 个方面的具体职责，包括部门总体统筹、项目闭环管理、数据目录梳理、开展数据治理、共享使用审批、场景开放创新、保障数据安全。（来源：北京亦庄）

6. 四川省印发《四川省元宇宙产业发展行动计划（2023—2025 年）》

9 月 15 日，四川省经济和信息化厅、省委宣传部等 16 部门联合印发《四川省元宇宙产业发展行动计划（2023—2025 年）》，聚焦五大方面十八条主要任务，加快形成新质生产力，建设“中国元宇宙谷”。

行动计划指出，要加强数字治理能力建设。探索数据主权认证管理，强化数据主权安全保障。密切跟踪元宇宙发展中出现的价值伦理、虚拟空间管控等新问题，不断完善元宇宙环境下网络空间相关法规制度，提升合规性审查服务能力。加强区块链风险管理制度建设，探索创新监管模式，抓好合规引导，营造元宇宙信任发展生态。加强社会监督，防范概念过度炒作，推动元宇宙产业健康有序发展。

行动计划强调，要强化数字安全能力建设。加强密码、零信任等元宇宙安全技术研究，开展常态化安全风险评估，建立安全风险事件处置机制。指导元宇宙企业加强信息安全管理，建立健全违法信息监测、识别和处置机制。落实依法治网，切实防范网络诈骗等违法活动。加强元宇宙信息传播监管，个人隐私保护等，规范对用户信息的收集、存储、使用等行为，提升数字安全防护能力和个人信息保护水平。（来源：四川省经济和信息化厅）

7. 福建省印发《福建省加快推进数据要素市场化改革实施方案的通知》

9 月 19 日，福建省数字福建建设领导小组办公室印发《福建省加快推进数据要素市场化改革实施方案的通知》。

通知明确，要健全数据安全管理机制，推行国家数据流通和交易负面清单，建立健全数据流通监管制度，实施数据流通全流程合规监管。构建

个人隐私数据和企业非公开数据安全保障制度体系，规范个人数据和企业非公开数据安全、合法、合规使用。

通知要求，要维护数据要素市场秩序。严厉打击黑市交易，取缔数据流通非法产业。强化反垄断和反不正当竞争，加强重点领域执法司法，依法依规查处垄断协议、滥用市场支配地位和违法实施经营者集中行为，营造公平竞争、规范有序的市场环境。

通知强调，要鼓励社会参与协同治理。鼓励企业、科研机构和行业协会等社会力量积极参与数据要素市场建设，开展数据流通相关安全技术研发和服务。（来源：福建省发展和改革委员会）

境内前沿观察二：治理实践

导读：9 月，上海、江苏、北京等地公安机关公布 2023 年执法工作情况。上海公安机关累计对 2800 余家单位开展执法检查，下发限期整改通知书 960 余份，并与 300 余家重点单位建立网络安全信息通报预警机制。江苏公安机关行政处罚违法违规互联网运营单位 368 家次，整改网络安全高危隐患 2783 个，并主动向 118 家行业单位发出黑客攻击预警。北京公安机关开展安全监督检查 1100 余家次，安全评估 1000 余家次，对发现的隐患漏洞及时督促整改。

行政执法个案方面，多地公安机关、网信部门公布依据《数据安全法》进行行政处罚的案件，执法对象涉及医学检验机构、科技公司、不动产登记中心等主体，处罚结果为警告、警告并处罚款。这表明《数据安全法》正在逐步成为各部门行政执法实践中的重要依据，预计未来数据安全行政执法案件数量将进一步增多。依据《网络安全法》进行行政处罚的案件方面，地方公安机关公布多起“一案双查”案件，如四川警方对某型网络设备WEB管理页面被攻击篡改案件开展“一案双查”，查明该型网络设备产品服务商存在未及时将设备漏洞和补救措施告知用户等多项违法行为，四川警方依据《网络安全法》第二十二条、第六十条进行行政处罚。又如天津警方对某单位重要信息系统数据恶意篡改案件开展“一案双查”，发现该

单位存在网络日志不足6个月等违法行为，天津警方依据《网络安全法》第二十一条、第五十九条处以罚款。

国家网信办公布对知网的网络安全审查相关行政处罚结果，针对14款APP存在的个人信息保护相关违法行为，作出责令停止违法处理个人信息行为，并处人民币5000万元罚款的行政处罚。工信部、多地通信管理部门及网信部门均发布针对APP、小程序或SDK的执法检查情况，充分说明移动应用程序仍是各部门监督检查的重点。

结合9月公布的行政案件中的违法行为，企业在开展合规工作时应注意以下方面：1.建立数据安全管理制度，组织数据安全教育培训；2.采取加密等技术措施保障数据安全；3.对数据处理活动开展风险监测和定期风险评估，及时处置SQL注入漏洞、弱口令等风险隐患；4.采取监测、记录网络运行状态、网络安全事件的技术措施，留存相关网络日志不少于六个月；5.重视系统开发测试、运维阶段安全，确保建立全流程的网络与数据安全保障体系；6.发生安全事件时，立即采取处置措施，向有关主管部门报告；7.提供系统运维、数据处理等服务时，按照法律法规要求和合同约定履行安全保护义务；8.作为网络产品提供者时，发现网络产品存在安全风险立即采取补救措施，及时告知用户并向有关主管部门报告。

关键词：净网2023、一案双查、网络产品提供者、APP、系统运维、弱口令、数据安全管理制度、数据安全培训

（一）公安机关治理实践

1. 上海公安机关：累计对 2800 余家单位开展执法检查

8 月 31 日，上海公安机关召开新闻发布会，通报上海警方根据公安部夏季治安打击整治专项行动部署，持续深入推进“砺剑 2023”系列专项行动，聚焦与人民群众生产生活紧密相关的网络谣言、网络暴力、网络黑客、网络侵公、网络黑产等网络乱象，依法严厉打击各类涉网犯罪的措施成效和典型案例。

其中，保障数据安全方面，发布会指出，对于大量存储公民信息等重要敏感数据的行业，上海警方一直十分关注，切实履行安全监管职责。上海警方全力推动网络安全等级保护覆盖范围，组织全市重点单位落实网络安全等级保护工作，开展定级备案、测评整改，指导重点单位提升网络和数据安全防护水平；依托等级保护工作，落实数据安全存储、数据加密传输等技术标准，建设数据安全使用、数据安全运维等工作制度，帮助重点单位提升数据安全保护能力。

公安机关持续深入推进网络安全监督检查，对重点单位“应检尽检”，今年以来，累计对 2800 余家单位开展执法检查，下发限期整改通知书 960 余份。同时，指导有关企业深入排查并消除在安全制度、技术措施等方面存在的风险隐患，从源头上强化网络安全和数据安全防护能力。其中，对于某科技发展有限公司在实际运维过程中，发生遭黑客入侵，重要数据被

窃取的安全事件中，存在不履行网络安全保护义务等违法行为，根据《网络安全法》第五十九条第一款之规定，对该公司责令改正，处罚款人民币五万元的行政处罚，同时对直接负责的主管人员处罚款人民币一万元的行政处罚。

此外，公安机关还与包括快递、电商平台在内的300余家重点单位建立网络安全信息通报预警机制，在网络安全信息共享、风险预警提示方面畅通沟通渠道，形成应急处置机制，一旦发现数据安全隐患和风险，能够第一时间发现、第一时间预警、第一时间处置。（来源：上海网警）

2. 江苏公安“净网2023”专项行动取得显著成效

9月14日，江苏省公安厅召开专题新闻发布会，通报全省公安机关在打击网络犯罪、整治网络乱象、服务经济社会发展等方面取得的成效。

据通报，公安部组织开展“净网2023”专项行动以来，江苏公安机关紧密结合夏季治安打击整治行动，紧盯“网络十大乱象”，全面强化网上打击整治，不断深化网络生态治理，累计侦破涉网犯罪案件2.3万余起，行政处罚违法违规互联网运营单位368家次，下架违规APP应用422款，整改网络安全高危隐患2783个，公安部先后26次发来贺电或通报表扬。

发布会从净化网络环境、维护数据安全、严查黑产黑市、改善网络生态四方面进行详细介绍。其中，江苏公安机关紧盯当前黑客攻击破坏最新动向，强化行业协作，组织专项集群会战，重拳打击利用黑客手段危害安全生产、窃取民生数据、攻击关键信息系统等犯罪活动，共侦破此类案件

202 起，打掉犯罪团伙 35 个，并主动向 118 家行业单位发出黑客攻击预警。坚持依法治网、依法管网，会同网信、通管等部门开展约谈、通报、处罚、下架等一系列监管措施，全力防范化解网络与数据安全威胁风险。针对问题频发、疏于监管的平台企业，启动“一案双查”，共查处网络服务提供者违法案件 153 起，着力压实平台企业网络安全主体责任。（来源：江苏网警）

3. 北京警方通报打击整治网络乱象专项行动成果

9 月 15 日消息，北京警方通报打击整治侵犯公民个人信息、网络“黑灰产”、电信网络诈骗等网络乱象专项行动成果。

打击网络犯罪方面，北京警方破获案件 1000 余起，对 800 余名犯罪嫌疑人采取刑事强制措施，并同步公布三起典型案件，一是成功打掉两个利用计算机软件非法抢占热门景区门票并倒卖牟利的犯罪团伙；二是打掉侵害中小企业利益非法入侵计算机信息系统团伙；三是破获利用外卖软件敲诈勒索案。

整治网络生态方面，北京警方会同网信、宣传部门持续加强对网络直播、视频娱乐、求职交友等领域平台的联合执法检查力度，督导全市重点互联网企业完善网站安全审核制度，优化审核机制，集中清理各类违法有害信息。督导企业集中清理违法有害信息 45 万余条，关闭相关账号 1.1 万余个。针对数据安全、系统安全风险进行排查整改，共开展安全监督检查

1100 余家次，安全评估 1000 余家次，对发现的隐患漏洞及时督促整改。（来源：首都网警）

4. 河南公安深入推进“净网 2023”专项行动

9 月 17 日消息，2023 年以来，河南公安机关持续严打网络违法犯罪，全面治理网络乱象，不断净化网络生态，深入推进“净网 2023”专项行动。

专项行动以来，河南公安机关聚焦打击整治“网络水军”“网络侵公”“网络黑客”“网络诈骗”等突出违法犯罪，坚持出重拳、破案件、打团伙，持续发起集群打击，成功侦破一批网络违法案件，抓获一批违法犯罪嫌疑人，集中打掉一批违法犯罪团伙，其中，开封公安机关打掉一个针对特定行业电脑投放可任意窃取、修改存储数据木马病毒的犯罪团伙，抓获团伙核心成员 5 人，查明直接受害企业、商家 500 余家；安阳公安机关打掉一个利用群控设备为“带货主播”提供虚假增粉、点赞、评论等“刷量控评”服务，诱导网民购买商品进而牟利的违法犯罪团伙，打掉“网络水军”窝点 5 个，抓获犯罪嫌疑人 15 名，摧毁作案网站平台 5 个，查扣相关手机设备 150 余部。

专项行动中，河南公安机关坚持依法管网、依法治网，不断强化网络安全监督检查和行政执法，监督指导网络运营者、数据处理者落实主体责任，清理一批网上违法信息，关停一批违法网站、栏目，查处一批网络违法案件，有力净化网络空间环境。其中，三门峡公安机关对不履行网络实

名制义务，导致提供的移动互联网应用程序分发服务存在安全风险的某公司依法予以行政处罚。

同步公布一批河南公安机关“净网 2023”专项行动典型案例。（来源：河南网警）

5. 江苏公安机关公布多起不履行数据安全保护义务行政执法案例

9 月 6 日，公安部网安局发布消息称，《数据安全法》施行近两年来，江苏公安机关网安部门聚焦信息数据泄露、滥用、篡改等行业领域问题乱象，加大监督检查、通报预警和行政执法力度。警方严厉惩治不履行数据安全保护义务的违法行为，全面压紧压实网络运营单位数据安全主体责任，已累计依据《数据安全法》办理行政案件 336 起。同步公布五起不履行数据安全保护义务被罚案例：

案例一：宿迁某医学检验机构不履行数据安全保护义务案。该机构运营的医学检验信息平台存在 SQL 注入漏洞、弱口令等网络安全隐患，且未建立数据安全管理制度，未组织数据安全教育培训，未采取相应技术措施保障数据安全，未对其数据处理活动开展风险监测和定期风险评估，可致敏感业务数据泄露，涉嫌未履行数据安全保护义务。宿迁公安机关依据《数据安全法》第四十五条规定，对该机构予以行政警告并处罚款 10 万元。

案例二：成都某科技有限公司不履行数据安全保护义务案。江苏苏州公安网安部门工作发现，成都某科技有限公司在为苏州某信息科技股份有限公司相关系统运维过程中，未建立健全全流程数据安全管理制度，为图

工作方便，私自将该公司30余万条运营数据上传至互联网，且未落实任何技术防护措施保障数据安全，未对其数据处理活动开展风险监测，可致该批数据泄露，涉嫌未履行数据安全保护义务。苏州公安机关依据《数据安全法》第四十五条规定，对该公司予以行政警告并处罚款5万元。

案例三：泰州某不动产登记中心和北京某科技发展研究中心不履行数据安全保护义务案。江苏泰州公安网安部门工作发现，当地某不动产登记中心的“业务练兵系统”存在Elasticsearch未授权访问安全漏洞，且未建立健全全流程数据安全管理制度，未落实有效的数据安全防护措施，可致该系统中存储的24万余条业务数据泄露,涉嫌未履行数据安全保护义务。泰州公安机关依据《数据安全法》第四十五条规定，对该不动产登记中心予以行政警告并责令改正；对该系统的建设运维单位北京某科技发展研究中心予以行政警告并处罚款5万元。

案例四：盐城某医药公司不履行数据安全保护义务案。江苏盐城公安网安部门在对当地某医药公司检查时发现，该公司医疗健康信息的会员管理系统存有大量公民个人信息，经现场检测发现该系统存在网络安全漏洞，且该公司未建立数据安全管理制度，未组织开展数据安全教育培训，也未采取相应技术措施保障数据安全，涉嫌未履行数据安全保护义务。盐城公安机关依据《数据安全法》第四十五条规定，对该公司予以行政警告并责令限期改正。

案例五：南通某科技有限公司不履行数据安全保护义务案。江苏南通公安网安部门对当地某科技有限公司检查时发现，该公司对包含生产工艺

流程、操作手册、员工个人信息等数据的MySQL数据库（数据量达百万条），未建立数据安全管理制度，也未采取相应技术措施保障数据安全，并且存在使用“弱口令”即可登录平台、访问数据的情况，涉嫌未履行数据安全保护义务。南通公安机关依据《数据安全法》第四十五条规定，对该公司予以行政警告并责令限期改正。（来源：公安部网安局）

6. 因存在数据泄露隐患，北京网安适用《数据安全法》处罚两家违法单位

9月16日消息，北京市公安局昌平、朝阳两分局网安部门近日充分运用《数据安全法》，对未制定数据安全管理制度、未充分落实网络安全管理等级保护制度的相关违法企业依法给予行政处罚。

案例一：北京市公安局昌平分局网安部门工作中发现，辖区内某软件有限公司研发的“某数据分析系统”存在数据泄露隐患。经查，该公司研发的“数据分析系统”内存有用户姓名、基因数据等数据信息。通过进一步核实，该系统内数据信息未采用加密措施，系统服务器未采取任何网络防护和技术防护措施，造成19.1GB公民隐私数据暴露在互联网。北京市公安局昌平分局根据《数据安全法》第二十七条、第四十五条第一款之规定，给予该企业警告，并处罚款五万元，责令限期改正。

案例二：北京市公安局朝阳分局网安部门接市公安局网安总队通报，辖区某科技公司存在数据泄露隐患，经查，该科技公司一款APP产品后台存储的客户姓名、手机号、微信账号、邮箱等信息46万余条数据被暴露在

互联网上，该数据一旦被不法分子获取，将导致大量公民个人信息泄露，给广大人民群众个人合法权益造成重大影响，北京市公安局朝阳分局根据《数据安全法》第二十七条、第四十五条第一款之规定，给予该科技公司警告的行政处罚。（来源：公安部网安局）

7. 因导致用户设备被漏洞利用攻击，一网络产品提供者被处罚

9 月 17 日消息，在公安部指导下，四川成都、乐山、凉山等地网安近日对某型网络设备WEB管理页面被攻击篡改案件开展“一案双查”，该网络设备产品服务商因未履行网络安全保护义务被依法调查。

本案中，四川网安工作发现，成都、乐山、凉山等地某型网络设备WEB管理页面被攻击篡改，发布违法有害信息。属地网安迅速行动，取得关键线索，最终锁定犯罪嫌疑人。经审讯，犯罪嫌疑人利用该型网络设备固件存在的已知公开漏洞，在互联网实施远程扫描和漏洞利用，将未修补漏洞的设备WEB管理页面篡改为有害信息网页。目前，该案正在进一步侦办中。

为彻底消除网络安全隐患，成都、乐山、凉山网安启动“一案双查”程序，对该型网络设备产品服务商涉嫌未履行网络安全保护义务展开调查。经查，成都某科技有限公司作为该型网络设备的四川区域代理商，未履行网络安全保护义务，在已知所代理网络设备存在漏洞情况下，未采取必要的安全保护管理和技术措施，未及时将设备漏洞和补救措施告知用户，导致网络安全风险防范传导链条断裂，用户设备被漏洞利用攻击，并造成现实危害。目前，该公司已被依法予以行政处罚。（来源：公安部网安局）

8. 江西南昌网安部门走访全市 MCN 机构

9 月 20 日消息，为进一步规范辖区内网络直播行业，依法防范打击利用网络直播平台实施的各类违法犯罪活动，根据《网络安全法》，结合夏季治安打击整治行动工作要求，南昌网安部门近日会同网信办，联合派出所，对全市网络直播平台开展网络安全监督检查和交流。

此次检查针对以下几个方面逐项开展检查：危害舆论环境、网络秩序等突出问题；内容管控不到位，甚至故意放宽审核规则，纵容危险物品和违禁物品交易；赌博；诈骗；血腥暴力；淫秽色情；“擦边球”等低俗内容传播泛滥；制作、传播网络谣言；网络主播制作、上传、推广违法违规信息；网络主播在重大舆情事件中从事参与蹭热点、做流量相关违法活动。（来源：南昌网警）

9. 因导致信息系统被入侵，天津警方对一单位进行处罚

9 月 25 日消息，天津南开警方近日对一单位进行行政处罚。

前段时间，天津公安南开分局网络安全保卫支队接到线索：辖区内某单位的重要信息系统数据遭到恶意篡改，严重危害网络安全。南开分局网络安全保卫支队立即启动“一案双查”，就该单位网络安全风险隐患问题进行调查，查处其网络运营者未履行网络安全保护义务一案。

南开分局网络安全保卫支队通过现场查看该单位制度类文件，并经过比对、分析发现，该单位运营使用的信息系统存在多重问题：一是防范网络侵入技术措施不完善，物理网络环境内部存在监测漏洞；二是监测、记

录网络运行状态的网络日志不足6个月；三是对于安全缺陷、漏洞等风险，该单位未立即采取补救措施亦未向有关部门报告，信息系统持续“带病”运营，给了不法分子可乘之机。依据《网络安全法》第二十一条、第五十九条之规定，南开分局对该单位及相关主管人员分别予以罚款伍万元和贰万元的行政处罚。（来源：公安部网安局）

10. 公安机关依法严厉打击缅北涉我国电信网络诈骗犯罪取得重大战果

9月3日，在公安部和云南省公安厅的组织部署下，西双版纳公安机关依托边境警务执法合作机制，与缅甸相关地方执法部门开展联合打击行动，一举打掉盘踞在缅北的电信网络诈骗窝点11个，抓获电信网络诈骗犯罪嫌疑人269名。其中，中国籍186名、缅甸籍66名、越南籍15名、马来西亚籍2名，幕后“金主”、组织头目和骨干21名，网上在逃人员13名，包括1名潜逃19年的命案在逃人员。现场查获电脑、手机、手机卡、银行卡和诈骗话术脚本等一大批作案工具。目前，中国籍犯罪嫌疑人已移交我方，公安机关将彻查其违法犯罪事实，依法予以严惩。

今年以来，缅北涉我国电信网络诈骗犯罪多发高发，由此衍生了偷渡、非法拘禁等一系列犯罪活动，严重侵害我国人民群众财产安全和合法权益，广大群众深恶痛绝。公安部对此高度重视，全面加强对缅北涉我国电信网络诈骗犯罪的综合研判，认真分析诈骗手法类型，查清诈骗窝点和人员情况，收集固定犯罪证据。近期，公安机关侦查梳理出一批缅北涉我国违法

犯罪线索，相关诈骗窝点主要涉及冒充领导熟人、虚假投资理财、冒充电商物流客服等诈骗犯罪，关联全国电信网络诈骗案件1100余起，涉案金额1.2亿元。在充分掌握犯罪事实和证据基础上，公安部部署指挥云南公安机关加强边境警务执法合作，联合缅甸相关地方执法部门成功打掉上述诈骗窝点，狠狠打击了诈骗分子嚣张气焰，形成强大震慑。（来源：公安部）

11. 最高检、公安部启动第三批5起特大跨境电信网络诈骗犯罪案件联合挂牌督办

9月12日，最高人民检察院、公安部联合挂牌督办第三批5起特大跨境电信网络诈骗犯罪案件，分别是福建莆田“9.06”电信网络诈骗案、重庆沙坪坝“5.11”电信网络诈骗案、江苏江阴“6.16”电信网络诈骗案、浙江温州“8.26”电信网络诈骗案、四川乐山“1.12”电信网络诈骗案。

这批案件均系境外电信网络诈骗集团的重点案件，多为组织境内人员通过偷越国（边）境方式赴境外参与诈骗犯罪活动，内部组织架构严密，境内外协同配合，参与人员众多，涉案金额巨大，有的集团还涉及非法拘禁、故意伤害等严重暴力犯罪，社会影响极为恶劣。

最高检、公安部有关部门负责同志表示，全国检察机关、公安机关将以联合督办为重要抓手，用足用好现有法律武器，持续保持对境外电信网络诈骗集团的高压严打态势，依法从重打击境外协同人员特别是提供偷越国（边）境、“跑分”洗钱、架设GOIP、收集公民个人信息等支持帮助的

团伙和人员，加强追赃挽损工作，做到“打财断血”，努力夺取电信网络诈骗犯罪打击治理新胜利。（来源：公安部）

12. 山东烟台网安部门打掉一黑客犯罪团伙，涉案资金 30 亿

9 月 5 日消息，山东烟台网安部门近日打掉一有组织牟取非法利益的黑客犯罪团伙。

2022 年 11 月下旬，山东烟台某网络科技有限公司报案，称其公司在网络上架设的数字藏品网站遭受黑客攻击，网站后台无法正常登录，同时存有 17 万网站会员信息及数字藏品交易数据的数据库被人清空，导致网站无法正常运营，受损会员近万人，网站主页也被署名“XX安全团队”的网页替换，对方以恢复网站数据名义向网站运营人敲诈勒索人民币 50 万元。

烟台网警随即开展侦查工作，发现国内多家网站被该黑客组织植入木马病毒。因案情重大，烟台网警会同芝罘警方成立专案组，由省公安厅挂牌督办。近日，专案组在部、省两级网安部门统一指挥下，在江苏、安徽等地警方的大力配合下，集中开展收网抓捕行动，成功打掉以犯罪嫌疑人王某为首的黑客犯罪团伙。

经查，自 2021 年以来，以王某为首的黑客犯罪团伙，通过网络渗透等攻击手段连续作案 300 余起，受害网站遍布国内十余省市地区，涉案金额超过 30 余亿元。（来源：公安部网安局）

13. 广东网警打掉 22 个“网络水军”团伙， 涉案金额 5.3 亿元

9 月 5 日消息，广东网安部门近期对刷量控评“网络水军”犯罪活动开展集群打击，并公布行动成果。其中，广东东莞网安部门组织全市 17 个镇街分局开展三波次集中收网打击行动，成功打掉犯罪团伙 22 个，依法刑事拘留嫌疑人 89 名，涉案金额达 5.3 亿元。

案例一：东莞网安部门查明，某“网络水军”团伙技术人员伊某自 2021 年 5 月至今先后搭建了 3 个专门“刷单”的平台，并分别给赖某某、李某某、叶某某等人运营。该团伙利用刷单平台，组织商家和刷手在网络平台上大量进行虚假购物、发布虚假评价并从中赚取刷单佣金，伊某从中抽取 30%利润。目前，属地公安机关已捣毁作案窝点 4 个，现场扣押作案电脑、手机、银行卡一批，涉案金额共 5700 余万元。

案例二：东莞网安部门查明，刘某乐开办电子商务公司，招聘员工通过各网络平台引流接单，再通过自动刷单软件为知名电商平台的网店商家提供“有偿刷单”的非法业务，使商家的店铺成交量、好评率、店铺权重得到提高，从而增加商家的商品销量。2023 年 7 月，东莞网安部门联合大朗分局开展收网行动，抓获嫌疑人 35 名，涉案金额共约 4000 万元。

案例三：东莞网安部门查明，陈某、李某等人注册某科技公司，专门在网络上发广告，组织水军人员为医疗机构、车企等商家在网络平台进行删除、屏蔽和降权下沉等操作，有偿提供信息删除服务。经统计，该团伙从 2022 年 3 月至今有偿删帖约 1.1 万次，非法获利约 53 万元人民币。（来源：网信广东）

14. 江苏警方公布打击网络违法犯罪 6 起典型案例

9 月 14 日，江苏公安机关公布打击网络违法犯罪 6 起典型案例，分别是：（1）镇江公安机关侦破王某顺提供网上“代骂”服务非法牟利案；（2）无锡等地公安机关依法查处编造发布“断供潮”谣言非法牟利水军团伙；（3）苏州公安机关侦破利用木马手段盗取快递面单的黑客案件；（4）徐州公安机关破获王某等人建立网络交易平台倒卖敏感公民个人信息案；（5）常州公安机关摧毁一条骗取未成年人微信账号的黑灰产业链；（6）镇江公安机关依法对不履行网络信息安全管理义务造成网络谣言大范围传播的某网站平台予以行政处罚。（来源：江苏警方）

15. 张家界警方全链条团灭 1600 余台非法侵入计算机系统终端案

9 月 20 日消息，按照公安部“净网 2023”和夏季治安打击整治专项行动的总体部署，湖南省张家界市公安局永定分局近日成功破获 1 起利用黑客软件，绕过某直播平台安全机制，非法获取旅游推广直播间观众（含播主粉丝）信息，再低价倒卖给本地旅行社的团伙案件，查获软件开发运营、技术支持、代理推广等各环节犯罪嫌疑人 21 名。

自 2023 年 2 月份以来，张家界市政府有关部门多次接到从事旅游直播的从业者举报称：自己的隐私直播间客源被人用黑客软件截流，再将被截流客源以不合理低价卖给本地旅行社，增加直播获客成本，给直播间造成巨大经济损失，同时刻意压低客源转交价格，导致低价团滋生、严重扰乱旅游经营秩序、旅客出游感受极差等系列恶果。

经查，微信用户李某在朋友圈公开贩卖“爬虫”软件，并称该软件可以绕开直播平台安全机制，获取到某平台直播间的用户信息（包括账号、昵称、性别、IP属地等非公开的数据）。永定公安办案人员发现李某售卖的两款软件具有非法侵入计算机信息系统，避开系统安全防护措施，非法获取计算机信息系统数据的功能。以姚某远、郭某康为首的软件开发、销售人员，以及李某宇、郭某将等17个省市级代理商，涉及全国各地1600余台终端设备的犯罪链条，浮出水面。

6月13日，李某在张家界落网，经查，仅犯罪嫌疑人李某一人就向本地旅游直播从业人员贩卖达50余人次，违法所得达2万余元，对张家界旅游直播市场造成严重侵害。7月7日，专案组集结警力，奔赴外省对该软件开发销售团伙集中收网。一个以非法入侵计算机信息系统获取他人信息、扰乱旅游市场秩序的团伙至此覆灭。目前，永定公安分局正在进一步深挖下游犯罪，并且报上级部门发起全国集群打击。（来源：公安部网安局）

16. 四川攀枝花警方打掉一犯罪团伙，超1400万部“老年机”被木马控制自动扣费

9月24日消息，四川攀枝花公安机关近日成功破获一起涉网络黑灰产特大案件。

2022年6月，攀枝花公安部门接警称，居民张先生的一台“老年机”话费越扣越多，经营业厅查询是用户订购了“平安天气”“开机提醒”等

小额增值收费业务。但张先生未看到任何有关开通业务的短信，也并非自己订购，便怀疑手机中了病毒。

接警后，民警调查发现，该老人所在的辖区存在众多类似事件，每月被扣除相关增值业务费用都为 1 元至 10 元不等。通过对这些“自动扣费”手机的各方面数据进行研判和追溯，民警发现这些手机网络数据都链接到同一个域名的服务器。经远程勘验，发现该服务器可以提供远程控制手机订购增值业务的功能，进而确定该服务器即为犯罪分子实施犯罪行为使用的木马服务器。网安民警追踪发现，全国竟有 1400 余万部手机被该木马服务器控制，其中涉及四川省的有 60 余万部。

网安民警通过多方调查取证，成功锁定租赁该服务器的犯罪嫌疑人孔某，并以孔某为突破口循线深挖。一个以陈某、高某为首，孔某、胡某、张某、刘某、闫某为骨干的非法控制“老年机”的犯罪团伙逐渐浮出水面。经查明，犯罪团伙与多家手机主板生产商合作过程中，将木马程序植入手机主板内。装有上述主板的手机出售后，陈某团伙通过之前植入的木马程序控制手机回传数据，获取用户手机号码、短信内容等信息，回传至犯罪团伙后台数据库。之后，由该团伙多名运营专员利用手机木马程序，向手机用户发送开通增值订购业务确认的短信，同时控制手机终端自动回复“Y”进行开通，一系列操作完成后再将此次收发的短信记录删除，以做到让手机用户无从察觉。利用这样隐蔽的犯罪手法，该案 4 个犯罪团伙非法牟利上亿元。

2023年年初，专案组抽调精干警力，成功打掉以陈某、杨某、庞某、林某四人为首的4个犯罪团伙，抓获犯罪嫌疑人23名，冻结、扣押涉案资金6000余万元，扣押涉案车辆4台、房产1套。目前，该案已移送起诉12人，取保候审11人，案件仍在侦办中。（来源：公安部网安局）

17. 重庆北碚警方破获多起帮助信息网络犯罪活动案

9月26日消息，重庆市北碚区公安分局近日破获多起利用“手机口”业务帮助信息网络犯罪活动案件，抓获多名犯罪嫌疑人。

“手机口”业务，即嫌疑人同时用两部手机，通过音频线、数据线连接或同时打开扬声器，一部通过网络软件接通境外诈骗分子，一部本地手机拨打国内受害人电话，实现语音中转，并成功掩饰诈骗电话归属地。近年来，公安机关通过开展“断卡”专项行动，重拳打击“黑灰产”“两卡”犯罪，压缩了境外诈骗团伙的生存空间。诈骗分子另辟蹊径通过国内网站、社交软件等发布大量“轻松赚钱”“日结佣金”等虚假招聘广告，诱惑国内网民，使用境外通讯软件勾连，通过虚拟币结算，组织大量年轻人群参与“手机口”业务。

案例一：5月25日，北碚区公安分局在工作中获悉线索，有人使用违法通信软件，通过内地手机参与“手机口”业务进行诈骗。办案民警立即展开调查，最终锁定犯罪嫌疑人蒋某，并于同日将其成功抓获。经查，今年3月中旬，嫌疑人蒋某在网上认识了一个朋友，对方让他准备两部手机，只要插上数据线和音频线，帮忙拨打对方给的号码，就可以轻松挣钱。随

后，嫌疑人蒋某购买了手机，通过“蝙蝠”聊天软件与境外诈骗分子联系，将两台手机通过一条音频线连接，搭建简易组网，然后在手机上下载“阳光”软件，便于境外诈骗分子通过“阳光”软件拨打诈骗电话，从而使诈骗电话在受害人处显示为国内电话，使受害人放松警惕。此外，嫌疑人蒋某还多次向某职业学校学生收购电话卡，为境外诈骗分子提供便利，从中获利。

8月以来，北碚警方抓获犯罪嫌疑人4名，破获利用“手机口”帮助实施诈骗的案件3起。

案例二：4月11日，北碚区公安分局在工作中获悉线索，赵某名下的银行卡可能存在“帮信”嫌疑。在大量工作与前期证据固定之后，办案民警随即依法将赵某抓获并传唤至公安机关接受调查。经查，去年9月，赵某通过张贴在工地墙面上的小广告主动联系对方，将自己的银行卡、身份信息提供给他人，帮助他人利用自己的银行卡转入转出资金，并从中赚取相应利润。经询问，嫌疑人赵某对自己的违法行为供认不讳。目前，该案件已移送审查起诉。

今年以来，北碚区公安分局已破获14起将自己的银行卡转交给他人，为他人信息网络犯罪活动提供支付结算的“帮信案”。（来源：重庆网警）

18. 浙江温州警方打掉一犯罪团伙，专门针对企业投放木马程序

9 月 27 日消息，浙江温州平阳县公安网安部门近日打掉一个专门针对企业投放木马程序的犯罪团伙，抓获涉案犯罪嫌疑人 30 名，退赔退赃 118 万元。

今年 4 月，平阳县公安局网安大队接辖区内某公司财务人员小陈报警，称其电脑被他人非法控制，嫌疑人利用其微信指令出纳小张往不同的银行卡转账，造成经济损失 298.2 万元。

经查，境外诈骗团伙先是通过网络招募境内黑客技术员，制作木马程序。随后将伪装成“***政策计划”的木马程序邮件群发至国内企业邮箱，企业工作人员打开程序，便感染了木马病毒，黑客远程控制其电脑，伪装身份，伺机作案。案发当天，出纳小张就是接收到微信上的”财务小陈“指示，从而进行了三次大额转账。微信上的”小陈“说话语气和断句习惯与平时发邮件时一模一样。利用企业邮箱传播达到远程控制目的后，黑客利用被控制电脑登录企业员工聊天工具，再进行二次传播，并重复上述作案过程，致使该病毒达到量级传播。

结合受害方财务室内监控和涉案电脑勘验结果，民警排除了公司内部人员作案的嫌疑。随后，民警通过对远控软件的层层追踪，彻底弄清楚其流程。犯罪团伙利用微信、邮箱传播，致使受害企业财务人员的计算机被控制，企业财务秘密“一览无遗”。在时机成熟之际，黑客就会模仿财务人员的口吻向出纳发出转账指令，让企业蒙受巨额损失。

对案情抽丝剥茧后，专案民警组织开展收网行动，一举捣毁了一个以廖某为首的黑客工作室和以葛某为首的洗钱团伙，抓获涉案犯罪嫌疑人30名。经审讯，犯罪嫌疑人对其违法犯罪的行为供认不讳。

民警结合案件病毒以及远控端数据源分析，发现辖区内另有预警风险企业23家。平阳公安已实地走访排查13家，并做好对企业财务人员转账规范的提醒工作。（来源：公安部网安局）

（二）网信部门治理实践

1. 国家网信办公布第二批深度合成服务算法备案清单

9月1日，国家互联网信息办公室发布第二批境内深度合成服务算法备案信息（即2023年8月境内深度合成服务算法备案清单），清单涉及共110项深度合成算法产品，主要应用于文本、图像、视频生成，机器翻译，智能对话等多种用途，涉及服务提供者，服务技术支持者两种角色。

国家互联网信息办公室提醒，深度合成服务技术支持者应当按照《互联网信息服务算法推荐管理规定》履行备案和变更、注销备案手续。请尚未履行备案手续的深度合成服务提供者和技术支持者尽快申请备案。（来源：中国网信网）

2. 国家互联网信息办公室公布第一批应用程序分发平台备案编号

9 月 27 日，国家互联网信息办公室公布第一批应用程序分发平台备案编号，涉及小米应用商店、360 手机助手、微信小程序、QQ 小程序、华为应用市场、腾讯手机管家等 26 家应用程序分发平台。

2022 年 8 月 1 日《移动互联网应用程序信息服务管理规定》正式实施以来，国家互联网信息办公室依法依规组织开展应用程序分发平台备案管理工作。根据《规定》有关要求，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）

3. 中央网信办部署开展“清朗·生活服务类平台信息内容整治”专项行动

9 月 28 日，中央网信办发布通知，开展“清朗·生活服务类平台信息内容整治”专项行动。

通知要求，要抓重点问题，聚焦为线下违法活动引流，搜索环节呈现违法信息，发布违规营销信息，组织操纵刷分控评，重点环节推荐低俗不良信息，传播网络迷信信息，散布炫富拜金、暴饮暴食信息等 7 类突出问题，对标对表网络生态治理各项规定要求，加强调查研究，集中排查整治；要抓重点平台，针对团购评价、婚恋交友、搜索引擎、影视点评、天气日历、旅游出行、网络购物、地图导航、本地生活、运动健康、实用工具等

生活服务类平台，压实主体责任，规范信息内容发布；要抓重点环节，紧盯跟帖评论、信息流推荐、直播、短视频、榜单弹窗、高风险产品等，排查风险漏洞，补齐短板弱项。

通知强调，要强化属地监管、压实平台责任，确保专项行动取得扎实成效。各地网信部门要制定细化实施方案，扎实部署推进，组织开展督导检查，加大典型案例通报曝光力度，充分调动各方力量参与治理。各网站平台要健全完善内容管理制度和社区规则，配齐配强内容审核力量，主动探索创新治理举措，实现健康可持续发展。（来源：中国网信网）

4. “清朗·杭州亚运会和亚残运会网络环境整治”专项行动查处一批违法违规网络账号

9 月 29 日，国家互联网信息办公室发布消息称，“清朗·杭州亚运会和亚残运会网络环境整治”专项行动启动以来，各地网信部门指导督促网站平台严格履行主体责任，深入开展清理整治，强化违规问题查处曝光，推动专项行动取得扎实成效。

截至目前，微博、抖音、腾讯、小红书、快手、百度、网易、京东、淘宝、闲鱼等重点平台累计处置违法违规账号 1 万余个，清理相关信息 7.4 万余条，下架违规商品 1.5 万件，发布治理公告 20 期。

同步围绕散布涉亚运会相关谣言信息、恶意质疑攻击参赛人员、挑拨粉丝互撕对立、假冒仿冒账号发布信息等七方面发布部分典型处置案例。（来源：中国网信网）

5. 国家互联网信息办公室对知网依法作出网络安全审查相关行政处罚

9月1日，国家互联网信息办公室发布公告，对知网（CNKI）依法作出网络安全审查相关行政处罚。

根据网络安全审查结论及发现的问题和移送的线索，国家互联网信息办公室依法对知网（CNKI）涉嫌违法处理个人信息行为进行立案调查。经查，知网（CNKI）主要运营主体为同方知网（北京）技术有限公司、同方知网数字出版技术股份有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司三家公司，其运营的手机知网、知网阅读等14款App存在违反必要原则收集个人信息、未经同意收集个人信息、未公开或未明示收集使用规则、未提供账号注销功能、在用户注销账号后未及时删除用户个人信息等违法行为。

国家互联网信息办公室依据《网络安全法》《个人信息保护法》《行政处罚法》等法律法规，综合考虑知网（CNKI）违法处理个人信息行为的性质、后果、持续时间，特别是网络安全审查情况等因素，对知网（CNKI）依法作出责令停止违法处理个人信息行为，并处人民币5000万元罚款的行政处罚。（来源：中国网信网）

6. 网信部门依法查处腾讯QQ危害未成年人身心健康违法案件

9月13日消息，针对腾讯QQ平台“小世界”版块存在大量色情等违法信息，危害未成年人身心健康问题，国家网信办近日指导广东省网信办，

依法约谈腾讯公司相关负责人，依据《未成年人保护法》第一百二十七条，实施行政处罚，责令暂停“小世界”版块信息更新30日，没收违法所得并处100万元罚款。

腾讯QQ平台“小世界”版块存在大量色情引流信息，部分用户在评论区诱导未成年人不良交友、实施性引诱，招募未成年人进行游戏陪玩，严重侵害未成年人合法权益，危害未成年人身心健康，违反《未成年人保护法》第八十条。（来源：网信中国）

7. 海南省网信办通报23款移动应用程序违法违规收集使用个人信息情况

9月1日，海南省互联网信息办公室通报23款移动应用程序违法违规收集使用个人信息情况。

通报指出，针对人民群众反映强烈的移动应用程序（包含App、小程序等）非法获取、超范围收集、过度索取权限等侵害公民个人信息的违法违规现象，海南省互联网信息办公室近期组织对省内用户量大的移动应用程序收集使用个人信息情况进行技术检测，检测结果显示23款移动应用程序均存在不同程度违法违规收集使用个人信息的行为。

针对检测发现的问题，各运营主体应主动与海南省互联网信息办公室联系领取限期整改通知书,并于本通报发布之日起15个工作日内完成整改。逾期未完成整改的将依法予以处置。

移动应用程序存在的问题包括未逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等；在申请打开可收集个人信息的权限或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解等。（来源：网信海南）

8. 因网站被植入非法网站暗链，重庆市巴南区网信办对一企业处以警告

9月7日消息，重庆市巴南区网信办工作发现，属地一生产公司开办的网站存在源代码被植入非法网站暗链的情况，随即开展立案调查工作。

经查，该公司未严格履行网络安全保护义务，运维疏于管理、安全防护措施不到位，导致其网站被植入非法网站暗链，违反《网络安全法》第二十一条、第二十五条规定。巴南区网信办依据《网络安全法》第五十九条规定，对该企业予以行政警告处罚，并责令其限期整改。（来源：网信重庆）

9. 因设置迷惑性按钮诱导消费者“入会”，“胡子大厨”被严肃约谈

9月12日，上海市网信办联合徐汇区网信办依法约谈餐饮连锁企业“胡子大厨”负责人，要求企业立整立改，切实履行个人信息保护义务，维护消费者的合法权益。

此前，根据网民举报，“胡子大厨”在使用第三方技术系统接入的点餐小程序中，设置“迷惑性”按钮，诱导消费者默认勾选加入会员、默认同意会员隐私政策，从而进一步索取消费者手机号码等个人信息。

企业负责人表示，将按照约谈要求，对照问题举一反三、全面整改。上海市网信办同时要求第三方点餐系统技术服务企业优化“会员入会”环节产品模板设计，通过明显标识告知消费者权利和义务，确保消费者的知情权和选择权，全面支持餐饮企业做好消费者个人权益保护。经核查，“胡子大厨”相关问题已完成整改。

上海市网信办相关负责人指出，此类默认消费者同意的“0 元入会”行为，意图通过“迷惑性”业务流程诱导消费者在不经意或未完全了解服务内容的情况下完成对企业的授权，违反《个人信息保护法》的“告知同意”原则。（来源：网信上海）

10. 公民个人信息泄露遭境外披露兜售，上海一政务信息系统技术服务公司被行政处罚

9 月 15 日，上海市网信办公布一起数据安全行政执法案例。

本案中，前期，据有关部门在跟踪调查中发现，上海市某政府信息系统技术承包商违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据泄露，以致成为境外不法分子窃取政务数据的“供应链”入口，相关公民个人信息在境外黑客论坛被披露兜售。针对

问题线索，上海市网信办联合有关部门对涉事公司未严格履行数据安全保护义务的违法行为，开展现场网络安全检查。

经查，该公司主要从事政务信息系统技术支撑工作。2022 年，该公司租用 1 台私有云服务器用于对未交付政务系统的研发测试和演示验收工作，存储了大量公民信息和政务信息，涉及公民个人信息数据 1.5 万余条。现场检查发现，该公司在开展数据处理活动中未能有效履行数据安全和个人信息保护义务，没有建立全流程数据安全管理制度，未采取技术防护措施保障数据安全和公民个人信息安全，导致平台频繁遭受境外远程访问和数据泄露风险。上海市网信办协调有关部门已要求该公司立即下线政府网站页面、关闭相关云服务端口、配合开展网络资产清查，并对该公司作出行政处罚。（来源：网信上海）

11. 上海网信办联合多部门发布《上海市互联网证券信息服务企业合规指引》

9 月 15 日消息，上海市人民检察院近日联合上海市委网信办、上海市证券同业公会，经前期调研走访、专家论证等多个环节，制定发布《上海市互联网证券信息服务企业合规指引》，引导相关企业加强互联网证券信息服务合规建设，维护清朗网络空间和网民合法权益。

指引适用于互联网证券信息服务企业合规建设。提供证券信息服务的本市属地网站平台、“自媒体”以及各类所有制企业，均可参照本指引开展业务合规管理。

指引从有效识别风险、风险评估处置方面提出若干合规建议，具体包括持证、亮牌经营；账号信息真实；内容风险管理；风险合规提示；风险处置机制以及积极配合调查。（来源：网信上海）

12. 上海市网信办、市市场监管局对部分房产中介、汽车 4S 店开展个人信息保护工作联合检查

9 月 26 日、27 日，上海市网信办、市市场监管局执法人员先后对链家地产、中原地产和太平洋房屋 3 家房产中介的线下门店，以及荣威、凯迪拉克和比亚迪 3 家汽车品牌的 4S 门店开展个人信息保护工作现场检查。

前期检测发现，房产中介在个人信息收集环节存在一些普遍性问题，如便民服务功能频繁弹窗索要消费者精准位置信息权限、首次进入小程序未主动提示用户阅读隐私政策、读取应用列表未同步告知用户收集个人信息目的和必要性、未提供有效的账号注销渠道等。汽车 4S 店同样存在干扰用户使用的共性问题，如频繁弹窗提示用户打开位置权限、强制用户同意打开存储权限否则无法使用拍照功能、频繁弹窗提示用户完善资料来收集个人信息、使用预约试驾功能时强制用户注册登录等。现场检查中，未发现以上门店在消费者个人信息存储、使用环节存在相关问题。

被检查企业相关负责人表示，由于对《个人信息保护法》、《消费者权益保护法》等法律规定理解不到位导致问题出现，下一步将按照检查要求，举一反三立即整改。

前期，上海市网信办已会同市市场监管局、市商务委、市房管局，以及市房地产经纪行业协会、市汽车销售行业协会等行业监管主管部门和相关协会，针对房产中介和汽车销售行业，先后组织专场个人信息保护普法培训，上海市93家房地产中介企业、109家汽车销售企业参加。（来源：网信上海）

13. 上海市网信办对属地46款App收集使用个人信息情况开展专项检查

9月28日，上海市网信办发布消息称，为规范App个人信息处理活动，保护公民个人信息合法权益，根据《个人信息保护法》《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，结合12345市民服务热线、市民来信举报等线索，2023年4月至9月，上海市网信办对属地下载量较大及投诉较多的46款App开展了收集使用个人信息专项检查，共发现160余项问题。经过通报和跟进指导，截至目前，各App运营单位均已完成问题整改。

检查发现的常见10种收集使用个人信息问题如下：（1）隐私政策关于个人信息收集使用的说明不完整或与实际情况不一致；（2）用户不同意隐私政策，App拒绝提供服务；（3）未提供用户主动勾选隐私政策、服务协议选项；（4）后台模式下超范围收集个人信息；（5）App收集敏感信息时未同步告知目的和必要性；（6）在用户同意隐私政策前，App已经收集个人信息；（7）App未提供账户注销功能或注销后信息未及时清除；（8）

App 在未涉及业务功能时提前申请可收集个人信息的权限；（9）频繁申请权限干扰用户使用；（10）无隐私政策。（来源：网信上海）

（三）通信管理部门治理实践

1.工信部及多省通信管理局通报或下架侵害用户权益 APP/SDK

（1）工信部

9 月 27 日，工信部信息通信管理局通报 2023 年第 5 批，总第 31 批侵害用户权益行为的 APP（SDK）。

通报指出，工信部近期组织第三方检测机构对群众关注的公共服务、休闲娱乐、酒店餐饮等移动互联网应用程序（APP）、小程序、第三方软件开发工具包（SDK）进行检查，发现 23 款 APP（SDK）存在侵害用户权益行为。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，将依法依规组织开展相关处置工作。

23 款 APP（SDK）包括纷玩岛、中公教育、虎扑、远征手游等，所涉问题包括 APP 强制、频繁、过度索取权限，违规收集个人信息，违规使用个人信息，欺骗误导强迫用户，违规利用个人信息开展自动化决策等。

（2）浙江

9 月 5 日，浙江省通信管理局组织第三方检测机构对群众关注的网上购物、实用工具、即时通信等类型 APP 进行检查，并书面要求违规 APP 开发运营者限期整改。截止 9 月 5 日，尚有 12 款 APP 未按要求完成整改，涉及

违规收集个人信息、APP 频繁自启动和关联启动、超范围收集个人信息等问题。

浙江省通信管理局指出，上述 12 款 APP 开发运营者应在 9 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。

（3）陕西

9 月 6 日，陕西省通信管理局近期组织第三方检测机构对陕西属地 APP 进行检查，截止 9 月 6 日尚有三款 APP 未按照要求完成整改，涉及违规收集个人信息，超范围收集个人信息，违规使用个人信息，强制用户使用定向推送功能，APP 强制、频繁、过度索取权限等问题。

陕西省通信管理局指出，上述 3 款 APP 开发运营者应在 9 月 12 日前完成整改工作，逾期不整改的，将依法依规组织开展相关处置工作。

（4）广东

9 月 14 日，广东省通信管理局发布《关于下架 18 款侵害用户权益 APP 的通报》，指出广东省通信管理局于 8 月 16 日向社会公开通报了 53 款存在侵害用户权益和安全隐患问题的 APP，截至通报规定时限，经核查复检，尚有 18 款 APP 未按照要求完成整改反馈。上述 APP 涉及违规收集个人信息，APP 强制、频繁、过度索取权限，APP 频繁自启动和关联启动等问题。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 予以下架处理。

同日，广东省通信管理局还公开通报25款未按要求完成整改APP，指出近期监测发现114款APP存在侵害用户权益和安全隐患问题，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25款APP未完成整改，现予以通报。被通报的APP应在9月21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，切实维护APP用户合法权益和网络安全秩序。

（5）上海

9月26日，上海市通信管理局发布《关于侵害用户权益行为APP的通报（2023年第三批）》。通报指出，上海市通信管理局近期组织第三方检测机构对本市移动互联网应用程序侵害用户权益行为开展检查。经检测发现26款APP存在“违规收集个人信息”“过度索取权限”等相关问题。已通报相关运营企业，督促存在问题的APP进行整改。截至目前，尚有12款APP未完成整改,上述APP应在10月10日前落实整改工作。逾期不整改的，将依法依规组织开展处置工作。（来源：工信部、地方通信管理局）

2.江苏省信息通信行业“铸网2023”专项行动：累计发现网络安全风险1000余个

9月13日，由江苏省通信管理局主办的全省信息通信行业“铸网2023”专项行动点评会暨实网应急演练成功举办。

根据工信部部署安排，7 月 24 日，江苏省通信管理局联合省工信厅启动“铸网 2023”专项行动，历时 1 个多月，对省内 600 余家基础电信企业、互联网企业以及工业互联网企业近 31 万个联网资产开展全面体检，检查涵盖 13 类不同条线业务，累计发现网络安全风险 1000 余个。（来源：江苏通信业）

（四）其他部门治理实践

1.因重要信息系统突发事件未报告，北京中关村银行被罚 20 万元

9 月 8 日，国家金融监督管理总局北京监管局公开京金罚决字〔2023〕6 号行政处罚决定书，决定书载明，北京中关村银行发生重要信息系统突发事件但未向监管部门报告，严重违反审慎经营规则，国家金融监督管理总局北京监管局依据《银行业监督管理法》第四十六条给予其 20 万元罚款的行政处罚。（来源：国家金融监督管理总局）

2.深圳市人民检察院联合多部门发布《深圳市企业数据合规指引》

9 月 16 日，深圳市人民检察院联合深圳市互联网信息办公室、深圳市司法局、深圳市发展和改革委员会、深圳数据交易所等多部门发布《深圳市企业数据合规指引》，引导企业开展数据合规管理，对涉及数据各场景制定全面详细的规范指引，包括总则、数据安全合规管理组织体系建设、数据合规管理制度体系建设、数据全生命周期合规、数据出境合规和附则。

指引完善数据合规风险防范体系。针对数据审查、收集、使用、储存、交易等场景，精准识别数据全生命周期中的各类安全风险，搭建全流程合规标准规范，为企业开展各类数据活动提供全面、具体、可操作指引。

指引确立数据合规行刑衔接机制，依法明确有关刑事激励措施，对依法需要行政处罚的，可以向有关主管机关提出从轻或者减轻处罚的建议。指引建立数据合规免责容错机制。在“数据交易”环节，指引首次建立企业数据交易的免责事由与容错机制，助力推进数据要素合规高效流通交易，促进数据要素市场发展。（来源：深圳政法）

境外前沿观察：月度速览十则

导读：9 月，欧盟《数据治理法》全面施行，规范公共部门对特定受保护数据的重复使用以及第三方机构的数据中介服务。澳大利亚内政部长介绍本国网络安全战略制定情况，提出 2023 年起在全国范围内建立“六个网络盾牌”，构建网络安全生态系统，加强公民和企业网络威胁教育。迪拜《数据保护条例（修正案）》正式施行，新增企业使用全自动或半自动系统处理数据时应履行的义务。

美国加州司法部与谷歌达成和解协议，针对谷歌在位置数据收集、存储和使用等方面欺骗用户的行为支付 9300 万美元和解款。斯里兰卡政府云系统“兰卡政府云”遭受大规模勒索攻击，四个月未备份数据丢失，疑似因用户点击可疑链接导致。德国 2023 年因数据盗窃、网络间谍破坏活动造成的损失预计将达到 2060 亿欧元，约四分之三的受访公司在过去 12 个月内经历过网络攻击。英国运营关键信息基础设施的组织于 2023 年上半年向政府报告的严重扰乱互联网运营的网络攻击事件数量也较往年有较大增长。

关键词：网络威胁教育、数据治理、人工智能、政务云、网络攻击

1. 澳大利亚计划建立六大网络盾牌，确保国家网络安全

9 月 18 日，澳大利亚内政部长介绍本国网络安全战略制定情况，提出 2023 年起在全国范围内建立“六个网络盾牌”，分别为：（1）加强对公民和企业的网络威胁教育；（2）开发网络安全技术；（3）推进政企合作交换网络威胁情报；（4）保护关键基础设施；（5）构建网络安全生态系统；（6）加强国际合作。战略落地实施大致分为两个阶段，第一阶段为 2022 年至 2025 年，旨在打造战略基础；第二阶段为 2026 年至 2030 年，将全面实现战略目标。（来源：澳大利亚政府）

2. “英美数据桥”正式确定，于 10 月 12 日生效

9 月 21 日，“英美数据桥”正式确定，旨在落实英国科学、创新和技术部于 2023 年 6 月根据《2018 年数据保护法》第 17 条提出的在《欧盟-美国数据隐私框架》下扩展建立英美数据桥的决定。决定自 2023 年 10 月 12 日生效后，英国企业和组织将能根据数据桥安全可靠地将个人数据传输至美国认证组织。在数据桥构建过程中，英国政府对数据接收国个人数据保护、法治建设、尊重人权和基本自由、监管等情况进行评估，确保英国公民根据《2018 年数据保护法》享有的个人数据保护水平不会受到损害。（来源：英国政府）

3. 欧盟《数据治理法》全面施行

9 月 24 日，欧盟《数据治理法》全面施行，要点包括：（1）规范公共部门对于其持有的特定类别受保护数据（如个人数据和商业机密数据）的重复使用；（2）制定适用于数据中介服务的具体规范。数据中介服务作为中立的第三方，将个人和公司与数据用户联系起来；（3）规定由欧盟委员会成立欧洲数据创新委员会，由来自不同机构的代表组成，包括欧洲数据保护委员会、欧洲数据保护监管机构和欧盟网络安全局；（4）制定非个人数据的国际传输规则。（来源：欧盟官网）

4. 迪拜《数据保护条例（修正案）》正式施行，新增人工智能相关规定

9 月 1 日，迪拜《数据保护条例（修正案）》正式施行。修正案新增个人数据控制者和处理者使用全自动或半自动系统处理数据时应履行的义务，个人数据控制者和处理者在首次使用或访问系统时，必须以清晰明确的方式提供通知，告知用户有关系统的技术情况、用户的个人数据处理可能是非人工发起的以及该系统对用户个人数据权利的影响。此外，修正案规定针对人工智能全自动或半自动系统的通用义务，当产品、服务可能对数据主体产生影响时，人工智能系统的开发和利用必须满足技术伦理、公平性、透明度、安全性和责任制等要求。（来源：迪拜国际金融中心管理局）

5. 欧盟委员会发布《关于<协调联盟应对重大跨境关键基础设施中断的蓝图>的理事会建议提案》

9 月 6 日，欧盟委员会发布《关于<协调联盟应对重大跨境关键基础设施中断的蓝图>的理事会建议提案》。提案指出，蓝图旨在实现三大目标：（1）通过更好地了解成员国的重大关键基础设施事件、事件原因及其对运营、战略、政治层面的所有主要利益相关者的潜在后果，提高共享态势感知；（2）确保协调一致的公共沟通，以最大程度确保重大关键基础设施事件发生后向公众传达清晰的信息；（3）通过加强成员国、成员国之间以及与相关联盟机构、机关、办公室、机构的合作来提供有效的事件响应，减轻事件影响，迅速恢复基本服务。（来源：欧盟委员会）

6. 英国 ICO 发布《北爱尔兰警察局数据保护审计报告》执行摘要

9 月 8 日，英国信息专员办公室公布《北爱尔兰警察局数据保护审计报告》执行摘要。执行摘要指出，北爱尔兰警察局数据安全治理流程和问责程序有较大改进空间，同时在数据共享实践等领域的数据保护合规水平有限。要求北爱尔兰警局采取以下行动改善数据保护实践：（1）提升警局处理数据资产的工作透明度，公开数据处理工作报告；（2）确保数据保护影响评估指南中包含数据安全风险管理负责人的具体名录，推进数据安全风险管理工作权责明确；（3）制定全面的数据安全治理培训计划，推动员工了解相应工作职责；（4）完成数据共享审查，确保所有日常个人数据共享活动均经过确认，并制定数据共享协议。（来源：英国信息专员办公室）

7. 德国因数据盗窃、网络间谍破坏活动造成的损失将达到2060亿欧元

9月1日，德国数字协会Bitkom表示，到2023年，数据盗窃、网络间谍破坏活动将给德国造成2060亿欧元损失。Bitkom对1000多家公司的调查发现，约四分之三的受访公司在过去12个月内经历过网络攻击，52%的公司表示“网络攻击威胁到业务存续”。在遭受攻击的公司中，70%的公司报告敏感数据被盗。此外，61%的公司的数字通信受到监控。Bitkom表示，德国经济对于犯罪分子和敌对国家来说是极具吸引力的目标，并且有组织犯罪与国家控制的攻击活动之间的界限正在变得模糊。（来源：德国数字协会Bitkom）

8. 英国2023年关键信息基础设施网络攻击数量创历史新高

9月11日消息，英国关键信息基础设施运营服务组织于2023年上半年向政府报告严重扰乱互联网运营的网络攻击事件数量较往年有较大增长，涉及能源、交通、通信、医疗、政府、教育等多个领域。尽管只有13起影响到国家互联网交换点与回程运营商等运营关键技术服务的组织，但较2022年和2021年分别记录的4次中断有显著增加。

根据《英国网络和信息系统条例》，英国电力、运输、医疗等领域数字服务供应商在网络攻击导致的中断达到一定阈值时，需向行业主管部门报告发生。英国信息通信管理局和信息专员办公室在2023年上半年收到比

往年任何一年都多的报告，这表明数字服务供应商更清晰地意识到自身报告职责，加大检测投资。（来源：The Record 网站）

9. 斯里兰卡国家政务云被攻击，四个月数据被删除

9 月 11 日，斯里兰卡信息与通信技术局（ICTA）证实，斯里兰卡政府云系统“兰卡政府云”（LGC）近日遭受大规模勒索攻击。该国已经启动调查程序，由斯里兰卡计算机网络应急技术处理协调中心（CERT/CC）负责。

经调查，攻击可能始于 2023 年 8 月 26 日，当时一名gov[dot]lk域用户表示在过去几周内收到可疑链接并且可能有人点击了其中一个链接。“兰卡政府云”的服务和备份系统迅速被加密。ICTA估计，所有使用“gov.lk”电子邮件域名的电子邮件地址（5000 个），包括内阁办公室使用的地址，都受到了影响。虽然系统和备份在攻击发生后 12 小时内恢复，但由于系统没有对 2023 年 5 月 17 日至 8 月 26 日期间的数据进行备份，因此所有受影响的账户都永久丢失了该时间段内的数据。

据了解，“兰卡政府云”于 2007 年引入，最初使用Microsoft Exchange 2003 版，在 2014 年升级为Microsoft Exchange 2013 版。这个版本一直在使用，但现在已经过时，不再维护，容易受到各种类型的攻击。尽管ICTA计划从 2021 年开始升级“兰卡政府云”到最新版本（目前是Exchange Server 2019 CU11 Oct21SU），但由于“资金限制和某些以前的董事会决定”，决策一直受到拖延。遭受攻击后，ICTA已经开始采取措施增强“兰卡政府云”安全性。（来源：安全内参）

10. 因非法追踪用户位置数据，谷歌支付 9300 万美元和解

9 月 14 日，美国加州司法部公布关于谷歌位置隐私实践的和解协议。协议指出，谷歌以多种方式在收集、存储和使用位置数据等方面欺骗用户。当谷歌向用户承诺禁用“位置历史记录”功能后，其会通过“网络和应用程序活动记录”功能以及“广告个性化”功能等方式继续收集存储用户位置数据，只有将上述三种功能同时关闭，才能避免个人位置信息的泄露。

协议指出，谷歌必须向加州支付 9300 万美元，并遵守一系列保护加州用户隐私利益的禁令条款，包括：（1）启用与位置相关的账户设置时应向用户显示；（2）提高位置跟踪的透明度；（3）创建网页向用户展示谷歌收集的位置数据以及如何使用的详细信息；（4）向用户披露其位置数据可能用于个性化广告；（6）当谷歌关于地理位置设置和个性化广告的规则出现重大变化前，应获得谷歌内部隐私权工作组的审核和批准。（来源：美国加州司法部）

行业前沿观察一：2023 网络诚信建设专题

样本采集工作启动

导读：9 月 19 日，2023 网民网络安全感满意度调查活动“网络诚信建设专题”样本采集工作启动仪式在京举行。大会总结了 2023 网民网络安全感满意度调查活动第一阶段"网民意见综合采集工作"取得的成效，充分肯定了全国各地网络志愿服务团队在样本采集工作中发挥的重要作用。

“网络诚信建设专题”是网民网络安全感满意度调查活动的重要组成，是了解我国网络诚信建设情况，特别是人民群众对网络诚信建设的认知和感受，评估网络诚信社会建设和治理成效的重要渠道，得到有关部门的高度重视和赞许。每年的调查数据形成《全国网络诚信建设专题调查报告》支撑《中国网络诚信发展报告》，成为中国网络诚信发展状态风向标。《中国网络诚信发展报告 2023》在中央网信办、中央文明办主办的“中国网络文明大会”网络诚信建设高峰论坛上成功发布，引起了社会广泛反响。今年“网络诚信建设专题”将照例形成专题报告，并为《中国网络诚信发展报告 2024》提供高质量的数据支撑。

全国各地网络志愿服务团队第一时间纷纷行动起来，以饱满的热情投入到诚信专题样本采集工作中去。在调查活动第二个五年开启之际，迎来了一个全新的开端，必将为网络志愿服务开启一个崭新的局面。

关键词：网络诚信建设专题，样本采集，启动仪式

1. “2023 网络诚信建设”专题样本采集工作启动仪式在京举行

9 月 19 日，“2023 网民网络安全感满意度调查活动样本采集工作总结暨网络诚信建设专题”样本采集启动仪式在京举行。

在全党全国上下全面贯彻党的二十大精神和践行“大兴调查研究之风”的大背景下，“网民网络安全感满意度调查活动”于 2023 年启动第二个五年计划，进入新里程，绘制新蓝图，推行新标准，启动新机制，奔向新目标。

9 月 13 日至 22 日，“2023 网民网络安全感满意度调查活动”网民意见综合采集阶段工作成功开展，取得系列新成果，活动开展期间热潮不断，网民踊跃参与。迎着二十大“弘扬诚信文化”的呼声，综合采集期间网民热切关注的“网络诚信建设”专题调查定于 10 月 19 至 11 月 7 日独立开展深入调查，以全面了解本年度广大网民的认知感受、意见建议，反映各地区的诚信治理成果，深入推进网络诚信法治建设，积极开展网络诚信宣传引导，持续深化重点领域信用监管。

网络诚信是指具有完全民事行为能力的自然人、法人和非法人组织，在网络空间活动中尊崇道德、遵守法律、履行契约、恪守承诺的状态。

在互联网这个虚拟空间中，网络诚信是社会秩序的时空延伸，是网络文明的显著标志，网络诚信建设已经成为社会信用体系建设和网络空间生态治理发展进步的重要特征。不论是互联网平台相关开发商、运营商，还是网络平台使用者和广大网民，都需要在诚信的环境里才能良性发展、快乐“冲浪”。（来源：网安联）

2. “网络诚信建设”专题支撑《中国网络诚信发展报告 2024》

“网络诚信建设”专题样本采集工作 10 月 19 日在京启动，这是继 2022 年在整个调查活动中成功开展“网络诚信建设”专题调查之后，今年再次设置此项专题调查内容，这是对整个调查活动内容的有力拓展和丰富。今年的“网络诚信建设专题”将与去年一样，为《中国网络诚信发展报告 2024》（以下简称《报告》）提供支撑。

据悉，去年有 36 万网民参与了网络诚信建设调查，取得了丰硕成果，相关调查数据被引用到《中国网络诚信发展报告 2023》，并在由中央网信办、中央文明办主办的“2023 年中国网络文明大会”网络诚信建设高峰论坛上成功发布，引起了社会广泛反响。《报告》编撰单位“中国网络社会组织联合会”相关负责人表示，希望社会各界、广大网民朋友继续踊跃参与“网络诚信建设专题问卷调查”，力争取得更多高质量调查成果。

该负责人表示，作为“网民网络安全感满意度调查”的重要组成“网络诚信调查”专题（调查活动专题二），以丰富的调查成果为编制发布《中国网络诚信发展报告》提供了重要的数据支撑。希望今年的诚信专题调查继续与往年的一样，为《中国网络诚信发展报告 2024》的成功发布提供有效的数据支撑，为共建网上美好精神家园，加快网络强国、数字中国建设作出新的更大贡献。（来源：网安联）

3. “网络诚信建设”专题促进志愿团队转型升级

在今天的启动仪式上，活动组委会负责人黄丽玲女士表示，继调查活动采样工作结束后，又专门安排20天的“网络诚信建设”专题样本采集，有特别的深意蕴含其中。

一是网络诚信建设的重要性日趋凸显。“人无信不立，业无信不兴，国无信不强”，诚信是社会发展的基石，也应是网络空间天朗气清的标配。

二是调查活动今年全面启动志愿服务采集样本，广大志愿服务团队在样本采集工作中发挥了重要作用，但由于各种因素的制约，部分志愿服务团队动员力度不够大，采样成果不显著，启动“网络诚信建设”专题调查，是又一次志愿服务团队实战化演练，对志愿服务团队的动员组织能力、协调沟通能力、新技术运用能力是一次大检验，对志愿团队是一次整体实力的大提升。

三是通过实战化演练，可以帮助更多的志愿服务团队加快志愿服务模式从传统的志愿服务提升到更多通过网络、互联网等多方式，提供网络型的志愿服务，并通过与本地化志愿活动相结合，将网络安全志愿服务常态化开展，为本地的志愿服务工作赋能。

四是吸引更多志同道合的志愿服务团体，共同成长、共同助力国家网络安全建设，服务网民，让网民获得更多表达自己上用网真实感受的渠道和方法。（来源：网安联）

4. 网络诚信领域向上向善形势巩固，2024 调查结果值得期待

近年来，我国网络诚信建设取得积极进展和成效，为网络文明不断注入正能量。2023 年中央网信办、中央文明办主办的“中国网络文明大会”网络诚信建设高峰论坛发布的《中国网络诚信发展报告 2023》（以下简称《报告》）显示，网民对 2022 年网络诚信建设状况满意率达 84.24%，网络诚信领域向上向善形势更加巩固。

《报告》显示，我国网络诚信建设取得的新进展主要有以下四个方面：

一是政策法规不断完善，网络诚信基础进一步夯实。据不完全统计，2022 年，国家制定（修改）出台有关网络诚信的法律 2 部、综合性规划 3 个、司法解释 10 部、涉及网络诚信的行政法规 15 部，与 2021 年相比，增加 12 部行政法规。

二是多措并举协同发力，综合治理效能进一步彰显。相关职能部门聚焦人民群众反映突出强烈的网络乱象，及时部署开展专项行动，深入推进网络综合治理，切实维护社会公共利益和人民群众合法权益。国家有关部门、部分省区市加强平台经济规范引导，建立和完善投诉举报渠道和处理机制，提高公众对网络失信行为治理的参与度，守信互信、共建共享的网络诚信发展态势持续巩固。

三是宣传教育丰富多彩，实践活动影响进一步提升。紧紧围绕“喜迎二十大奋进新征程”主题宣传，举办 2022 年中国网络文明大会网络诚信建设高峰论坛，举办新时代中国网络文明建设成果展，广泛开展中国正能量网络精品征集评选展播活动、“阳光跟帖”行动、“聚辟谣之力扬文明之

光”等系列主题活动，深入实施争做中国好网民工程，网络诚信建设在网络文明建设中的筑基赋能作用进一步彰显。

四是社会主体广泛参与，讲信守约意识进一步增强。互联网平台把诚信经营作为企业生存发展的内生动力，自觉守好网络诚信建设的“第一道防线”；主流媒体多渠道、多形式宣传优秀传统诚信文化；各行业组织协会充分发挥桥梁纽带、行业自律、社会监督作用，广泛凝聚社会力量，携手推进网络诚信建设。网络诚信建设成效得到了广大网民的充分肯定，总体满意度达84.24%。开展多部门协调联动，共享信用信息，实施联合激励惩戒等，形成网络诚信建设强大合力。

《报告》由“中国网络社会组织联合会”编撰发布，系统梳理2022年我国网络诚信建设总体进展和积极成效，总结分析经验和挑战，专题阐释重点热点问题，提出推动网络诚信建设高质量发展意见建议。《报告》以原创性、战略性、权威性研究成果，为政府部门和社会各界了解掌握网络诚信情况提供工作参考和观察窗口，成为展示我国网络诚信发展成就的重要载体。

《报告》的主要调查样本来源于2022网民网络安全感满意度调查活动“网络诚信建设”专题。“2023网络诚信建设”专题样本采集工作于10月19日启动，样本采集继续为《中国网络诚信发展报告2024》提供支撑。网民对今年的网络诚信发展有什么看法和意见？让我们拭目以待。

（来源：网安联）

行业前沿观察二：专业技术评价迫在眉睫

导读：日前，北京网络空间安全协会的一份调研报告显示，当前全国网络空间安全从业人员达 150 余万，全国有 13 个省自治区直辖市开展了网络空间安全专业技术评价工作，为网络空间安全从业人员提供了系统的、科学的、体系化的评价，其余未开通这一渠道的地区，网络空间安全从业人员只能依靠市场化考证认证来验证自己的专业技术能力。随着国家网络空间安全战略的逐步实施，网络空间安全产业快速发展，开展网络空间安全人才专业技术评价工作迫在眉睫。

关键词：网络空间安全，专业技术评价

1. 广东：先行先试，开全国网安人才专业技术评价之先河

2019 年，广东省人力资源和社会保障厅和广东省科学技术协会印发《广东省网络空间安全工程技术人才职称评价改革实施方案》粤人社规〔2019〕34 号），开展网络空间安全工程技术人才职称评价工作，创新推进广东省网络空间安全工程技术人才职称评价工作，广东省网络空间安全工程职称评审委员会办公室设在广东省网络空间安全协会。

《广东省网络空间安全工程技术人才职称评价改革实施方案》是国内首个网络空间安全工程领域职称评价实施方案及标准，从制度上确立了网络空间安全专业技术人员的职业发展通道。

按照《方案》规定，广东省网络空间安全工程领域设置网络空间安全技术研究、网络空间安全技术应用、网络空间安全系统设计、网络空间安全系统评测和网络空间安全管理监测等五个专业。

随着互联网的高速发展，网络空间已成为人类活动的重要空间，网络安全成为国家安全体系的重要组成部分。建立一支规模宏大、结构优化、素质优良的网络安全人才队伍已成为维护国家网络安全和建设网络强国的核心需求。网络安全人才事业已迎来最好的发展机遇。

（来源：广东省网络空间安全协会）

2. 四川：全国首批建成网信职称评价体系

2021 年 1 月，四川省委网信办与四川省人社厅联合印发《四川省网络信息安全专业职称申报评审基本条件（试行）》，在全国首批建成网信职

称评价体系，为全省网信人才开辟了职称评价通道。此举有助于更好地建立网信人才职业标识，切实推动四川网信人才队伍建设与高质量发展。

据介绍，网络信息安全专业职称初定是对网络信息安全专业技术人员的初次职称认定，专业技术人员可通过继续教育、在职培训等方式进一步拓展和优化专业技术知识结构，不断提升能力水平，具备相应条件后，申报高一级职称评审，以适应网信领域新技术新职业新岗位发展需要，更好服务于网络强省、数字四川、智慧社会建设。

党的二十大提出，培养造就大批德才兼备的高素质人才，是国家和民族长远发展大计，要实施更加积极、更加开放、更加有效的人才政策，引导广大人才爱党报国、敬业奉献、服务人民。“这也是全国首次开设网信领域职称初定省级通道，有助于更好建立网信人才职业标识，切实推动四川网信人才队伍建设与高质量发展。”省委网信办相关负责人说道。

按照《通知》，全省各级各类事业单位、国有企业，注册地为我省范围内的非公有制经济和社会组织，以及自由职业者中，从事网络信息安全专业技术工作的专业技术人员，具有相应学历且符合相关条件的，经本人申请，可通过初定取得相应级别的职称。初定职称层级包括员级、助理级、中级三个层级，名称依次为技术员、助理工程师、工程师。

（来源：封面新闻）

3. 江苏：2021 年 9 月网络安全行业拥有独立的评价体系和标准

2021 年 9 月，江苏省专业技术人员职称工作领导小组印发《江苏省网络安全工程专业技术资格条件（试行）》（以下简称《资格条件》），在江苏省工程技术系列职称中增设网络安全工程专业，这标志着江苏省网络安全行业拥有了自己独立的评价体系和标准。

《资格条件》明确网络安全工程专业职称设员级、助理级、中级、副高级、正高级五个层次，对应名称为技术员、助理工程师、工程师、高级工程师、正高级工程师。职称适用对象为本省从事网络安全研究、网络安全产品生产、网络安全技术应用、网络安全服务等方面工作的专业技术人员。

《资格条件》强调德才兼备、以德为先，将品德作为首要考核考察内容，加强政治引领和正面引导，倡导良好作风学风，对于弄虚作假、行为不端的一票否决。

《资格条件》坚持分级评价，立足网络安全行业专业技术人才职业属性和岗位需要，根据对不同层次的人才分工定位，按照“干什么、评什么”的原则，细分评价对象，并分层次制定评价指标。

《资格条件》突出科学评价，以品德、能力、业绩为导向，破除“唯学历”“唯资历”“唯论文”“唯奖项”倾向，根据网络安全行业的实际情况，制定符合人才特点和发展规律的能力素质和业绩成果评价指标，既强调具备一定的理论研究和技术研发能力，更强调在一线的工作能力和解决实际问题的能力，重点评价人才在网络安全领域取得的实际工作业绩和成效，注重成果的应用和转化，注重在政策层面向基层和高技能人才的倾斜。

《资格条件》的出台表明江苏省在网信人才评价体系建设上迈出了坚实的一步。中共江苏省委网信办、省人力资源和社会保障厅共同推动了此项工作，旨在进一步贯彻落实习近平总书记关于网络强国的重要思想和中央、省委关于网信工作的决策部署，落实深化全省职称制度改革和分类推进人才评价机制改革有关要求，面对当前新形势新任务，发挥人才评价“指挥棒”和风向标作用，激发网络安全专业技术人才创新创造活力，提升关键领域核心技术攻关能力和网络安全服务保障能力，为推动江苏省网信事业高质量发展提供有力的人才支撑，切实扛起“争当表率、争做示范、走在前列”使命任务。（来源：央广网）

4. 山东：首次设立网络安全工程职称，填补网信职称评价空白

2022 年 4 月 18 日，中共山东省委网信办、山东省人力资源和社会保障厅联合印发通知，在全省开展网络安全工程职称评价工作。此次设立网络安全工程职称，填补了山东省网信领域职称评价的空白，将有效满足网络安全工程技术人员的职业发展需要，为山东网信事业发展提供有力人才支撑。

通知明确，网络安全工程职称设初级、中级、副高级和正高级，名称依次为网络安全助理工程师、工程师、高级工程师和正高级工程师。在评价范围上，设置网络安全技术研发与应用、网络生态建设与治理两个子专业，涵盖网络安全技术研发、生产、应用，网络数据安全和个人信息保护，网络安全技术体系规划、建设、管理，网络内容建设与管理

等岗位。在评价方式上，适应不同层级网络安全工程技术工作职业特点，建立考试、同行专家评议相结合的评价机制。在评价标准上，破除“唯学历、唯资历、唯论文、唯奖项”倾向，坚持德才兼备、以德为先，突出专业能力和工作实绩，全面推行代表作制度，重点评价网络安全工程技术人才的工作绩效和创新成果。

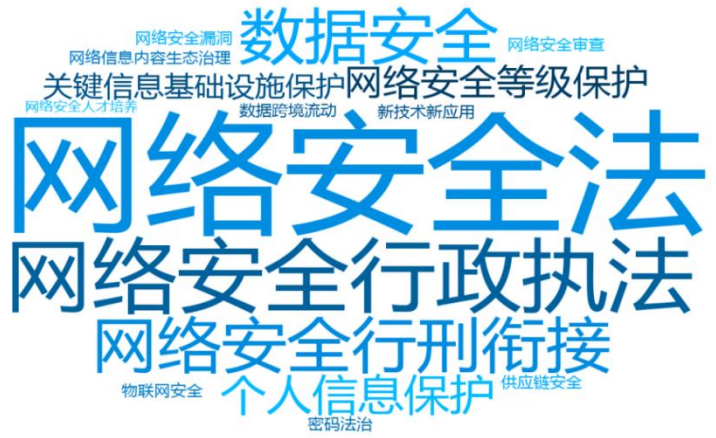
下一步，将研究制定网络安全工程初中级职称考试规定和高级职称评价标准条件，建立继续教育管理制度，搭建继续教育平台，成立高级评审委员会，组织好全省网络安全工程职称首次评价工作。

（来源：网易）

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，切实践行理论研究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 数据存储在境内，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

01 情况调研 — 1 - 3 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

02 风险评估 — 3 - 5 周

03 指导落实整改 — 周期视情况而定

04 出具风险评估报告 — 1 - 2 周

- 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估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

……