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

2024年2月 第2期(总第7期)

2024年2月26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
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

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

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

导读：1 月，有安全研究人员发现超级巨型数据库，该库整合过去几年的泄露数据，来源涵盖多家互联网公司和应用，文件体积高达 12TB，涉及 260 亿条泄露数据记录。就当前数据看，来自腾讯QQ的泄露数据记录最多，共计 14 亿条，还有来自众多公司和组织的泄露数据记录，包括：微博（5.04 亿）、网易（2.61 亿）、京东（1.42 亿）、优酷（1 亿）等。

关键词：数据泄露

1.史上最大规模数据泄露库曝光，腾讯、微博等在列

1 月 23 日消息，安全研究人员Bob Dyachenko和Cybernews团队近日发现超级巨型数据库，该库整合了过去几年的泄露数据，泄露来源涵盖多家互联网公司和应用，文件体积高达 12TB，涉及 260 亿条泄露数据记录，是迄今为止最大的泄露数据库，被称为“数据泄露之母”（Mother of all Breaches，MOAB）。

就当前数据来看，MOAB中来自腾讯QQ的泄露数据记录最多，共计 14 亿条，还有来自众多公司和组织的泄露数据记录，也有来自美国和其他国家政府机构的数据记录。具体包括：微博（5.04 亿）、MySpace（3.6 亿）、Twitter（2.81 亿）、网易（2.61 亿）、Deezer（2.58 亿）、LinkedIn（2.51 亿）、AdultFriendFinder（2.2 亿）、Adobe（1.53 亿）、Canva（1.43 亿）、京东（1.42 亿）、VK（1.01 亿）、优酷（1 亿）、DailyMotion（8600 万）、Dropbox（6900 万）、Telegram（4100 万）等。

研究人员认为其由恶意黑客或数据掮客编纂而成，汇集了来自数千次先前数据泄露事件的记录，虽然其中可能包含大量重复数据，但仍让人担忧。研究人员表示，由于泄露数据来源的多样性和复杂性，安全从业者和执法机构很难溯源该数据库背后的黑客。（来源：新浪科技）

境内前沿观察二：政策立法

导读：1 月，新技术应用赋能发展方面，国务院印发《关于进一步优化政务服务提升行政效能推动“高效办成一件事”的指导意见》，要求全面强化政务服务数字赋能，提出按照成熟稳定、适度超前的原则，创新开展大数据、区块链、人工智能等新技术应用，推动政务服务由人力服务型向人机交互型转变，由经验判断型向数据分析型转变。工信部等七部门印发《关于推动未来产业创新发展的实施意见》，指出大力发展未来产业，是引领科技进步、带动产业升级、培育新质生产力的战略选择，要求坚持包容审慎的治理理念，探索跨部门联合治理模式，构建多方参与、有效协同的未来产业治理格局。

关键信息基础设施和重要信息系统安全保护相关立法取得进展。交通运输部公布《铁路关键信息基础设施安全保护管理办法》，明确提出铁路关键信息基础设施的网络安全保护等级应当不低于第三级。工信部印发《工业控制系统网络安全防护指南》，防护对象针对工业控制系统以及被网络攻击后可直接或间接影响生产运行的其他设备和系统，要求使用、运营工业控制系统的企业对重要系统应用和数据定期开展备份及恢复测试，确保紧急时工业控制系统在可接受的时间范围内恢复正常运行。

数据跨境流动模式趋向灵活便利。广东省网信办发布通知，明确注册于广东省广州市、深圳市、珠海市等十个城市的个人信息处理者及接收方，可以通过订立《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》

的方式进行粤港澳大湾区内地和香港之间的个人信息跨境流动。中共中央办公厅和国务院办公厅印发的《浦东新区综合改革试点实施方案（2023—2027 年）》，要求积极探索优化数据跨境流动管理措施；临港新片区管委会表示将探索建立合法安全便利的数据跨境流动机制；广东省人大常委会通过《南沙深化面向世界的粤港澳全面合作条例》，支持南沙依法开展粤港澳数据流动便利化。

关键词：政务服务数字赋能、未来产业、铁路关键信息基础设施、工业控制系统、数据跨境流动

（一）国家层面动向

1. 国务院印发《关于进一步优化政务服务提升行政效能推动“高效办成一件事”的指导意见》，要求全面强化政务服务数字赋能

1月9日，国务院印发《关于进一步优化政务服务提升行政效能推动“高效办成一件事”的指导意见》，对深入推动政务服务提质增效，在更多领域更大范围实现“高效办成一件事”作出部署。

指导意见从全面加强政务服务渠道建设、全面深化政务服务模式创新、全面强化政务服务数字赋能、全面推动政务服务扩面增效、全面夯实政务服务工作基础五方面提出工作要求。

其中，全面强化政务服务数字赋能方面，指导意见指出要着力提升政务数据共享实效。完善政务数据共享责任清单机制，依托全国一体化政务服务平台数据共享枢纽，汇总政务数据共享需求，分批纳入国务院部门数据共享责任清单和垂直管理信息系统对接清单，推动国务院部门数据按需向地方回流和直达基层。持续提升政务数据质量，从源头加强数据治理，围绕企业和个人两个全生命周期编制“一企一档、一人一档”数据规范，推动实现“一数一源一标准”。依法依规共享使用政务数据，加强全流程安全管理，加大对涉及商业秘密、个人信息等数据的保护力度。按照成熟稳定、适度超前的原则，创新开展大数据、区块链、人工智能等新技术应用，推动政务服务由人力服务型向人机交互型转变，由经验判断型向数据分析型转变。（来源：中国政府网）

2. 两部门印发《浦东新区综合改革试点实施方案（2023－2027 年）》，积极探索优化数据跨境流动管理措施

1 月 22 日消息，中共中央办公厅、国务院办公厅印发《浦东新区综合改革试点实施方案（2023－2027 年）》。

实施方案明确五项主要任务，包括加大规则标准等开放力度，打造制度型开放示范窗口；完善科技创新体系，建设开放创新生态；深化人才发展体制机制改革，加快建设高水平人才高地；深化政府职能转变，激发各类经营主体活力；深化人民城市建设实践，探索超大城市治理新路。

实施方案提出，探索构建数字经济规则体系，实行分类分层的新型数据交易机制，依托数据交易所提升数据可信流通能力。探索数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制。探索数据资产管理、数字身份国际认证等，推动数字贸易交付和结算便利化，建设数字贸易服务平台。支持中国（上海）自由贸易试验区临港新片区探索建立安全便利的数据流动机制，允许在符合法律法规要求、确保安全前提下提升数据跨境流动的便利性。研究高标准且与国际接轨的数据安全管理规则体系，创新数据监管机制，积极探索优化数据跨境流动管理措施。（来源：中国政府网）

（二）部委层面动向

1. 七部门印发《关于推动未来产业创新发展的实施意见》

1 月 18 日，工信部、教育部、科学技术部等七部门印发《关于推动未来产业创新发展的实施意见》，指出大力发展未来产业，是引领科技进步、带动产业升级、培育新质生产力的战略选择。

意见提出全面布局未来产业、加快技术创新和产业化、打造标志性产品、壮大产业主体等六项重点任务，以及加强统筹协调、加大金融支持、强化安全治理、深化国际合作四项保障措施。具体要求强化安全治理。坚持包容审慎的治理理念，探索跨部门联合治理模式，构建多方参与、有效协同的未来产业治理格局。加强伦理规范研究，科学划定“红线”和“底线”，构建鉴别-评估-防御-治理一体化机制。引导企业建立数据管理、产品开发等自律机制，完善安全监测、预警分析和应急处置手段，防范前沿技术应用风险。（来源：工信部）

2. 工信部印发《工业控制系统网络安全防护指南》

1 月 19 日，工信部印发《工业控制系统网络安全防护指南》，旨在进一步指导企业提升工控安全防护水平，夯实新型工业化发展安全根基。指南围绕安全管理、技术防护、安全运营、责任落实四大方面，提出 33 项指导性安全防护基线要求，适用于使用、运营工业控制系统的企业，防护对象包括工业控制系统以及被网络攻击后可直接或间接影响生产运行的其他设备和系统。

系统数据安全方面，指南要求定期梳理工业控制系统运行产生的数据，结合业务实际，开展数据分类分级，识别重要数据和核心数据并形成目录。围绕数据收集、存储、使用、加工、传输、提供、公开等环节，使用密码技术、访问控制、容灾备份等技术对数据实施安全保护。法律、行政法规有境内存储要求的重要数据和核心数据，应在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。

应急处置方面，指南要求制定工控安全事件应急预案，明确报告和处置流程，根据实际情况适时进行评估和修订，定期开展应急演练。当发生工控安全事件时，应立即启动应急预案，采取紧急处置措施，及时稳妥处理安全事件。重要设备、平台、系统访问和操作日志留存时间不少于六个月，并定期对日志备份，便于开展事后溯源取证。对重要系统应用和数据定期开展备份及恢复测试，确保紧急时工业控制系统在可接受的时间范围内恢复正常运行。（来源：工信部）

3. 财政部印发《关于加强数据资产管理的指导意见》

2023 年 12 月 31 日，财政部印发《关于加强数据资产管理的指导意见》。

指导意见明确十二项主要任务，包括依法合规管理数据资产、明晰数据资产权责关系、完善数据资产相关标准、加强数据资产使用管理、加强数据资产应急管理、完善数据资产信息披露和报告、严防数据资产价值应用风险等。

数据安全方面，指导意见要求数据资产各权利主体建立健全全流程数据安全管理机制，提升安全保护能力。对经认定失去价值、没有保存要求

的数据资产，进行安全和脱敏处理后及时有效销毁，严格记录数据资产销毁过程相关操作。数据资产各权利主体均应落实数据资产安全管理责任，按照分类分级原则，在网络安全等级保护制度的基础上，落实数据安全保护制度，把安全贯彻数据资产开发、流通、使用全过程，提升数据资产安全保障能力。数据资产各权利主体应分类分级建立数据资产预警、应急和处置机制，深度分析相关领域数据资产风险环节，梳理典型应用场景，对数据资产泄露、损毁、丢失、篡改等进行与类别级别相适应的预警和应急管理，制定应急处置预案。（来源：财政部）

4. 交通运输部发布《铁路关键信息基础设施安全保护管理办法》

1月3日，交通运输部公布《铁路关键信息基础设施安全保护管理办法》（交通运输部令2023年第20号）。办法共6章30条，主要围绕铁路关键信息基础设施认定、运营者责任和义务、保障和监督、法律责任等方面作出规定。

办法明确，国家铁路局负责制定铁路关键信息基础设施认定规则，并报国务院公安部门备案，抄送国家网信部门。国家铁路局根据认定规则，负责组织认定铁路关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门，抄送国家网信部门。

办法压实运营者责任和义务，规定铁路关键信息基础设施的网络安全保护等级应当不低于第三级。运营者的主要负责人对所运营的铁路关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络

安全事件处置工作，组织研究解决重大网络安全问题。运营者应当为每个铁路关键信息基础设施明确安全管理责任人。

办法强化铁路关键信息基础设施监督管理和保障。规定国家铁路局应组织建立铁路关键信息基础设施网络安全监测预警制度；建立健全铁路关键信息基础设施网络安全事件应急预案体系，定期组织应急演练；定期组织开展铁路关键信息基础设施网络安全检查检测等内容。（来源：交通运输部）

5. 国务院国有资产监督管理委员会发布通知，强调健全完善数据资产交易流转定价

1 月 20 日，国务院国有资产监督管理委员会发布《关于优化中央企业资产评估管理有关事项的通知》，旨在推动国有经济布局优化和结构调整，助力企业实现高质量发展，优化企业国有资产评估管理。

通知要求健全完善知识产权、科技成果、数据资产等资产交易流转定价。中央企业及其子企业发生知识产权、科技成果、数据资产等资产转让、作价出资、收购等经济行为时，应当依据评估或估值结果作为定价参考依据。经咨询 3 家及以上专业机构，确难通过评估或估值方式对标的价值进行评定估算的，依照相关法律和企业章程履行决策程序后，可以通过挂牌交易、拍卖、询价、协议等方式确定交易价格。许可使用知识产权、科技成果、数据资产，可以采用销售额或利润提成、许可入门费加销售额或利润提成等方式确定许可费用。（来源：国务院国有资产监督管理委员会）

（三）地方层面动向

1. 贵州省印发《贵州省关于加强数字政府建设实施方案》

2023 年 12 月 27 日，贵州省人民政府印发《贵州省关于加强数字政府建设实施方案》。

方案明确八方面内容，包括建设完善全省一体化的数字政府基础设施体系；建设完善全省一体化的数据资源体系；建设完善全省一体化的核心门户体系；建立健全数字政府安全保障体系；建立健全数字政府制度规则体系；有序推进政府数字化履职能力体系建设；以数字政府建设引领驱动经济社会数字化发展；加强党对数字政府建设工作的领导。

建立健全数字政府安全保障体系方面，方案要求：（一）强化安全管理责任。厘清政务信息系统全生命周期管理职责边界，落实主体责任和监督责任。构建跨地区、跨部门、跨层级的安全协同联动机制。建立数字政府安全风险评估、责任落实和重大事件处置机制。落实关键信息基础设施运营者的主体责任；（二）严格落实安全制度。建立健全数据采集、存储、共享开放、销毁等全过程管理制度和标准，完善网络安全、保密监测预警和密码应用安全性评估制度，定期开展网络安全、保密和密码应用检查，强化关键信息基础设施网络安全等级保护；（三）提升安全保障能力。建立健全动态监控、主动防御、协同响应的数字政府安全技术保障体系，强化日常监测、通报预警、应急处置能力。保障电子文件形成、传输、存储等全流程的安全合规，加强新技术在安全领域的应用，提升数字政府整体安全防护能力；（四）提高自主可控水平。加快推进数字政府建设领域安

全可靠技术和产品应用，加强相应运维保障能力建设，切实提高自主可控水平。开展对新技术新应用的安全评估，加强监督管理。（来源：贵州省人民政府）

2. 四川省印发《关于推进数据要素市场化配置综合改革的实施方案》

1 月 2 日，四川省大数据中心、四川省发展和改革委员会、四川省经济和信息化厅、中共四川省委网信办四部门印发《关于推进数据要素市场化配置综合改革的实施方案》。

方案提出强化数据要素供给、构建数据要素流通体系、推动数据要素创新应用、构建数据制度标准规范、健全数据安全治理体系五项主要任务。

数据安全治理体系方面，方案要求：（一）加强网络数据安全监管。建立数据安全联管联治机制，强化分行业监管和跨行业协同监管。健全数据安全风险评估、信息共享、监测预警和应急处置机制；（二）建立数据安全技术体系。构建云网数一体化协同安全保障体系，强化对算力资源和数据资源的安全防护。落实国产密码应用要求，加强数据安全存储、可信传输、数据存证等方面的国产化数据安全基础设施建设。促进可信身份认证、接口鉴权、算法核查等新技术应用；（三）探索个人信息安全认证和评估制度。推动行业建立个人信息长效保护机制，健全个人信息安全事件投诉、举报、报告和责任追究制度。建立个人信息定期审计操作规范，推动数据处理者落实个人信息保护主体责任，按照个人授权范围依法依规采集、持有、托管和使用数据。（来源：四川省大数据中心）

3. 广东省网信办发布关于落实《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》的通知

1 月 4 日，广东省网信办发布关于落实《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》的通知。

通知明确注册于广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市的个人信息处理者及接收方，可以通过订立《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》的方式进行粤港澳大湾区内地和香港之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。通知明确备案工作采取电子版预审与纸质版查验相结合的方式。备案流程包括材料提交、材料查验及反馈备案结果、补充或者重新备案等环节。（来源：网信广东）

4. 浙江省发布《关于加快人工智能产业发展的指导意见》

1 月 10 日，浙江省人民政府办公厅发布《关于加快人工智能产业发展的指导意见》，提出力争成为全球重要的人工智能产业发展新高地。

指导意见明确五大发展方向，包括加快核心技术突破，打造人工智能技术创新策源地；强化核心要素供给，打造人工智能基础支撑最优地；加速创新场景赋能，打造人工智能创新应用先行地；推动融合集群发展，打造人工智能产业发展聚集地；构建最优产业生态，打造人工智能创新创业首选地。

指导意见要求加强安全和伦理治理。尊重人工智能产业发展规律，保障个人隐私和数据安全，防范和打击违法行为，构建安全有序发展环境。

探索建立人工智能监管与治理体系，依法依规实行包容审慎监管。发挥省科技伦理委员会作用，加强人工智能伦理安全规范及社会治理实践研究，面向重点领域开展伦理审查和安全评估。推动相关高校院所、企业等按规定设立人工智能伦理（审查）委员会。（来源：浙江省人民政府）

5. 山东省发布《关于加快数字经济高质量发展的意见》

1 月 9 日，中共山东省委、山东省人民政府发布《关于加快数字经济高质量发展的意见》。

意见提出七大主要任务，包括突破重点数字产业，壮大数字经济核心动能；深化产业数字赋能，拓展数字经济发展空间；加快数字技术创新，打造数字经济关键引擎；激活数据资源价值，释放数字经济要素红利；完善数字基础设施，筑牢数字经济发展底座；健全数字治理体系，完善数字经济制度支撑；优化数字发展环境，营造数字经济优良生态。

意见要求筑牢数据资源安全屏障。加强数据分级分类管理，健全数据安全防护管理和审计制度。强化数据安全态势感知和监测预警，构筑公共数据全生命周期安全防护体系。建好工业领域数据安全监测平台，提升区域性、规模性工业数据安全风险的信息获取、分析研判和预警处置能力。依托省工业大数据安全科研机构，开展数据安全政策咨询、风险评估等服务能力建设。（来源：山东省人民政府）

6. 广东省通过《南沙深化面向世界的粤港澳全面合作条例》，支持南沙依法开展粤港澳数据流动便利化和跨境应用

1 月 19 日，广东省人大常委会通过《南沙深化面向世界的粤港澳全面合作条例》，旨在落实《广州南沙深化面向世界的粤港澳全面合作总体方案》，将南沙打造成为立足湾区、协同港澳、面向世界的重大战略性平台。条例共 8 章 58 条，对南沙科技创新、产业发展、开放合作、规则衔接等内容作了全面系统规定，将于 3 月 1 日起施行。

条例明确，广东省人民政府及有关部门应当主动对接、积极吸纳高标准国际经贸规则，支持南沙加强与港澳在投资和贸易、市场准入、政务服务、法律服务等方面的规则衔接和机制对接，促进各类要素跨境便捷流动和优化配置，提高对外开放水平。支持南沙依法开展粤港澳数据流动便利化和跨境应用。支持在南沙合作设立的教育机构、科研机构等平台按照国家数据和网络安全管理要求建设专用科研网络，实现科学研究数据依法跨境互联互通。鼓励在南沙设立符合国家规定的数据出境申报安全评估专业服务机构，在数据出境安全评估、个人信息出境标准合同备案等方面提供服务。（来源：广东省人大常委会）

7. 浙江金华市印发《金华市公共数据授权运营实施细则（试行）》

1 月 12 日，浙江省金华市人民政府办公室印发《金华市公共数据授权运营实施细则（试行）》，围绕职责分工、授权程序、授权运营行为规范、授权运营域、数据安全、监督管理六方面作出规定。

数据安全方面，实施细则要求：（一）公共数据授权运营坚持统筹发展和安全的原则，按照“公共数据分类分级”要求，加强公共数据全生命周期安全和合法利用管理，确保数据来源可溯、去向可查、行为留痕、责任可究；（二）公共数据主管部门应根据《浙江省公共数据授权运营管理办法（试行）》相关要求，加强数据安全管理。应建立授权运营域安全管理制度，健全安全保障措施，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入、数据泄露等危害网络及数据安全的风险。定期组织授权运营单位开展安全培训、应急演练和攻防演练；（三）公共数据主管部门应会同网信、保密、密码管理、公安、国家安全等单位，按照“一授权一预案”要求，结合授权运营的应用场景制定应急预案，并组织应急演练。未制定应急预案的，不得开展授权运营工作。发生数据安全事件时，公共数据主管部门应按照应急预案启动应急响应，采取相应的应急处置措施，防止危害扩大，消除安全隐患；（四）公共数据授权运营安全坚持“谁运营谁负责、谁使用谁负责”的原则。授权运营单位主要负责人是运营公共数据安全的第一责任人。授权运营单位应建立健全高效的技术防护和运行管理体系，完善安全制度，确保公共数据安全，切实保护个人信息；（五）授权运营单位应制定授权运营安全应急处置预案并组织应急演练，加强防攻击、防泄露、防窃取的监测、预警、控制和应急处置能力建设。（来源：浙江省金华市人民政府）

8.《临港新片区数据跨境流动分类分级管理办法（试行）》发布，打造更加开放的跨境数据流通高地

1 月 19 日，国际数据经济产业创新大会在临港新片区召开。会上发布《临港新片区数据跨境流动分类分级管理办法（试行）》，并介绍数据跨境流动工作情况。

据介绍，该办法将进一步指导和帮助在新片区范围内注册登记的或在新片区开展数据跨境流动相关活动的企业、事业单位、机构协会和组织等数据处理者。办法以企业共性需求最迫切的细分领域为切入口，对跨境数据进行分类管理，同时将跨境数据从高到低依次分为核心数据、重要数据、一般数据 3 个级别，核心数据禁止跨境，重要数据形成重要数据目录，一般数据形成一般数据清单。

此外，临港新片区管委会将探索建立合法安全便利的数据跨境流动机制，对依据办法开展的数据跨境流动进行日常监督管理，提供数据跨境流动合规服务，指导数据处理者开展数据出境风险自评估。充分依托前期开展数据跨境流动试点积累的经验，遵循“从企业到行业，从案例到清单，从正面到负面”的原则，以行业为维度，以企业数据跨境需求场景为切入口，有序推进一般数据清单和重要数据目录的编制工作。2024 年，临港新片区将率先围绕智能网联汽车、金融理财、高端航运、国际贸易、生物医药、文化出海等重点领域的具体场景，组织行业龙头企业和专家组成工作组，陆续发布一批一般数据清单和重要数据目录。（来源：中国（上海）自由贸易试验区临港新片区管理委员会）

9. 天津市印发《天津市公共数据授权运营试点管理暂行办法》

1 月 30 日消息，天津市政府办公厅近日印发《天津市公共数据授权运营试点管理暂行办法》。办法深入贯彻落实习近平总书记关于数字中国建设的重要论述和党中央、国务院关于加快培育数据要素市场的决策部署，落实中央和市委经济工作会议精神，围绕解决“如何释放数据要素价值”和“如何保障数据安全”，提出了“场景牵引、试点先行、市区联动、权责清晰”的公共数据授权运营思路，从“授权运营程序及要求”“数据管理和利用”“安全管理”“考核评估”等方面明确了运营试点建设的实践路径，促进公共数据多场景应用、多主体复用，为推进本市数据要素市场化配置改革，发挥数据要素乘数效应，服务经济社会高质量发展夯实基础。

下一步，天津市数据局将落实国家数据局和市委、市政府工作要求，高标准推进公共数据授权运营工作，繁荣产业生态。一是开展授权运营试点遴选。按照“成熟一个，启动一个”的原则，分批次有序启动授权运营试点建设。二是提升公共数据供给能力。加强公共数据汇聚治理，扩大数量、提升质量、拓展类型，打破“数据壁垒”，推进公共数据与社会数据融合应用。三是开展“数据要素×”典型案例征集。聚焦全市高质量发展“十项行动”和赋能“三量”“三新”，激励社会各界共同挖掘打造一批示范性强、显示度高、带动性广的典型应用场景，培育一批数据商，提升数据服务发展的能力。四是强化授权运营安全监管。完善授权运营监督管理和考核评估体系，推动数据安全防护技术升级，压实数据安全责任，保障公共数据安全。（来源：天津市数据局）

境内前沿观察三：治理实践

导读：1 月，国家互联网信息办公室公布 2023 年网络执法情况。2023 年，全国网信系统共约谈网站 10646 家，责令 453 家网站暂停功能或更新，下架移动应用程序 259 款，关停小程序 119 款，会同电信主管部门取消违法网站许可或备案、关闭违法网站 14624 家，督促相关网站平台依法依约关闭违法违规账号 127878 个。同时，因信息内容安全相关违法行为，网信部门对百度、必应、夸克、抖音、新浪微博、腾讯微信等多家大型网络平台均开展网络执法。此外，国家网信办还指导属地网信办依法依规查处一批怠于履行网络安全和数据安全义务的违法违规企业。

江苏、四川、内蒙古自治区等 13 个省市先后成立数据局，可以预见，2024 年，国家及地方数据局将在推动数字经济发展、激活数据要素价值方面发挥更大作用。

结合 1 月公布的行政案件，除《网络安全法》第二十一条、《数据安全法》第二十七条以及《个人信息保护法》第六十六条规定的安全保护要求外，有两点需要注意：1. 应高度重视系统开发测试环节安全，包括测试数据、测试账号安全。1 月披露的案件中，涉及的相关违法行为包括“开发系统互联网测试阶段未对相关数据进行加密，未落实安全保护措施”“在对系统测试过程中，将有权限的测试账号设为弱口令，且系统正式使用后未将测试账号进行清空删除处理”；2. 在收到公安机关限期整改或责令改正的要求后，应当及时按要求进行整改，避免进一步承担法律责任。1 月案

件中涉及的违法行为包括“某公司在收到公安机关下发整改通知书责令限期整改，并被处以警告后，未按要求对OA办公系统存在的网络安全隐患进行整改”“三家企业先期收到公安机关下发的《阿拉善盟公安局限期整改通知书》的情况下，仍未开展计算机信息系统等级保护工作”。

此外，针对中国银行存在的“迟报重要信息系统重大突发事件”等九项违法行为，中信银行存在的“数据中心机房演练流于形式，部分演练为虚假演练、实际未开展”等六项违法行为，国家金融监督管理总局对中国银行、中信银行分别处以430万元、400万元罚款。

关键词：开发测试、拒不改正、网络执法、个人信息保护、数据局

（一）公安机关治理实践

1. 浙江省公安机关2023年侦破网络违法犯罪案件5333起

1月11日，浙江省公安厅公布“净网2023”专项行动成绩单。全省公安机关坚持以人民为中心,坚持守土有责、守土尽责,深入开展“净网2023”专项行动，坚持重拳出击、以打开路，全力侦破黑客攻击、侵犯公民个人信息、网络黑灰产、网络赌博、网络淫秽、网络涉枪爆、网络诈骗等群众反响强烈、影响突出的涉网案件，2023年以来，全省共侦破网络违法犯罪案件5333起,移送起诉犯罪嫌疑人6409名,切实提升了人民群众获得感、幸福感和安全感。

同步公布全省网安部门侦破的十大典型案例，分别是：（1）杭州拱墅警方侦破王某等人侵犯公民个人信息案；（2）杭州上城警方侦破祁某等人非法控制计算机信息系统案；（3）余姚警方侦破潘某等人非法获取计算机信息系统数据案；（4）温州龙湾警方侦破叶某等人侵犯公民个人信息案；（5）湖州警方侦破闫某等人非法获取计算机信息系统数据案；（6）海宁警方侦破陈某破坏计算机信息系统案；（7）绍兴越城警方侦破袁某等人帮助信息网络犯罪活动案；（8）金华金东警方侦破王某等人破坏计算机信息系统案；（9）台州路桥警方侦破周某等人提供侵入、非法控制计算机信息系统程序、工具案；（10）松阳警方侦破刘某等人侵犯公民个人信息案。（来源：浙江公安）

2. 因不履行网络安全保护义务，北京市公安局对多家公司作出处罚

1月8日,公安部网安局公布四起不履行网络安全保护义务被处罚案例。

案件一：2023年6月，昌平网安部门检查发现，昌平某生物技术有限公司存在数据泄漏的情况，其委托另一软件公司研发的“基因外显子数据分析系统”包含公民信息、技术等信息，涉及泄露数据总量达19.1GB。经检查，该软件公司在开发系统互联网测试阶段，未对相关数据进行加密，未落实安全保护措施，属于未履行数据安全保护义务。北京市公安局昌平分局依据《数据安全法》第四十五条第一款规定，给予警告并处罚款五万元的行政处罚。

案件二：2023年7月13日，朝阳网安部门检查发现，朝阳某教育公司数据被泄漏到境外非法网站上，该公司的一个客户关系管理系统内存储的该公司员工账号以及对应客户姓名、手机、下单时间、成交金额等12余万条信息被泄漏。经现场检查发现,因该公司技术人员在对系统测试过程中，将有权限的测试账号设为弱口令，且系统正式使用后未将测试账号进行清空删除处理。该公司未建立数据安全管理制度和操作规程，系统未进行网络安全评估，同时此账号因弱口令被黑客破解造成大量公民个人信息被盗取泄漏，涉嫌违反《数据安全法》第二十七条之规定。北京市公安局朝阳分局给予该公司罚款五万元的行政处罚。

案件三：2023年8月1日，一境外论坛发布题为“某教育站点教70多万订单信息”的帖文，疑似北京某教育公司发生数据泄露，针对此情况，

海淀网安部门立即开展核查处置工作。经查，该公司教务排课系统在账号密码传输前未进行加密传输，存在账号密码爆破的可能。黑客可通过爆破手段获取账号密码，通过访问导出大批量后台数据，造成数据泄漏。该公司未建立全流程数据安全管理制度、未落实网络安全等级保护制度、未履行数据安全保护义务，违反《数据安全法》第二十七条、第四十五条之规定。北京市公安局海淀分局对该公司给予罚款五万元，直接负责的主管人员罚款一万元的行政处罚。

案件四:2023 年 9 月 14 日,房山网安部门在对某科技公司检查时发现，该公司网站网页源代码被篡改，网站链接跳转到境外赌博网站，易引发网络赌博或网络诈骗案件。经查，该科技公司没有建立管理制度，没有定期开展漏洞扫描，未依法采取防范计算机病毒和网络攻击、网络侵入等技术措施，导致网站前端源代码泄漏，造成网站内容被篡改，违反《网络安全法》第二十一条规定，属于不履行网络安全保护义务行为，北京市公安局房山分局对运营者责令改正，给予警告处罚。（来源：公安部网安局）

3. 因拒不履行网络安全保护义务，海南省琼海市公安局对某公司罚款 5 万元

1 月 26 日消息，海南省琼海市公安局对一家不履行网络安全保护义务的公司依法处以 5 万元罚款。

2023 年 2 月，琼海市公安局在开展全市网络安全隐患检查时发现某公司未落实网络安全等级保护制度要求，导致其 OA办公系统被黑客植入勒索病毒，造成不良影响，当即下发整改通知书责令该公司限期整改，同时依

法给予警告处罚。2024 年 1 月份，琼海市公安局在工作中发现该公司OA办公系统再次被攻击并被植入违法信息，随即组织技术人员对该公司进行指导并检查，发现该公司未按要求对其OA办公系统存在的网络安全隐患进行整改，造成此次严重影响。

经查，该公司未采取相应的网络安全防护措施，违反《网络安全法》相关规定，琼海市公安局依法给予该公司罚款五万元，直接负责人罚款一万元的行政处罚。（来源：网信海南）

4. 因拒不履行网络安全保护义务，内蒙古自治区阿拉善盟公安局对三家企业作出处罚

1月18日,内蒙古自治区阿拉善盟公安局技侦网安支队在工作中发现，内蒙古泰升实业集团有限公司、内蒙古灵圣作物科技有限公司、内蒙古紫光化工有限公司 3 家企业，在先期收到阿拉善盟公安局下发的《阿拉善盟公安局限期整改通知书》的情况下，仍未开展计算机信息系统等级保护工作。26 日，技侦网安民警依据《网络安全法》对以上三家企业分别给予罚款 2 万元，企业法人分别给予罚款 5 千元的行政处罚。（来源：阿拉善网警）

5. 因未履行个人信息保护义务，内蒙古赤峰市喀喇沁旗公安机关对 14 家机构作出处罚

1 月 30 日消息，因未履行个人信息保护义务，内蒙古赤峰市喀喇沁旗公安机关对 14 家机构作出处罚。

近期，喀喇沁旗公安机关多次接到辖区居民被装修推销电话骚扰的警情。报警者反映推销人员对其个人及住房情况非常了解，怀疑其个人信息已遭泄露，担心财产和人身安全。通过侦察，喀喇沁旗公安局捣毁张某为首的以“信息共享”为名侵犯公民个人信息的犯罪团伙，共抓获犯罪嫌疑人 18 名，查获公民个人信息 100 余万条，扣押涉案电脑、手机等物品 68 件。经查，该犯罪团伙依托涉案的售楼企业、装修公司，通过“买卖、交换”等非法途径获取特定自然人信息，以“数据分筛、介绍客户、品牌融推”等所谓的“信息共享”方式传播扩散，并以此为目标客户进行“精准”业务推销，严重干扰居民正常生活秩序，对公民个人信息安全构成威胁。

经法院审判，犯罪团伙中张某因犯侵犯公民个人信息罪，被处有期徒刑六个月，并处罚金人民币六万元。未构成犯罪的温某、王某、马某等 16 人，根据《网络安全法》第四十四条、第六十四条第二款之规定，依各违法情节，分别处 2 千到一万元不等罚款。

公安机关同时开展一案双查，14 家相关企业因未全面履行《个人信息保护法》规定的个人信息保护义务，依据该法第六十六条第一款之规定，喀喇沁旗公安网安部门依法责令相关企业进行改正并给予行政警告，对相关责任人员总计罚款 6.8 万元。（来源：公安部网安局）

6. 重庆警方依法查处一起用 AI 技术炮制谣言信息典型案例

1月2日消息,重庆市梁平公安机关近日依法办理一起为吸引流量获利，利用AI技术生成谣言信息并在网络平台发布的案件。

2023 年 12 月 25 日，网民在某知名网络平台发布一篇题为“重庆巫溪一民房发生爆炸事故，4 人不幸遇难，官方紧急介入调查”的谣言信息，全文 500 余字，文中以新闻报道的口吻称重庆巫溪“突发爆炸事故，现场情况十分惨烈”“发现了 4 名遇难者，其中包括一名儿童”“疑似与居民私拉乱接电线有关，调查组将进一步搜集证据”。

经查，网民康某某在网络上得知在某知名网络平台创作发布文章，可以根据阅读、评论、转发数量等获取收益，为了获取更多流量，赚取更多收益，康某某在毫无事实根据的情况下，在手机上利用AI应用自动生成文章，编造重庆巫溪发生爆炸造成 4 人死亡的谣言，并在某知名网络平台发布。12 月 28 日，康某某因涉嫌虚构事实扰乱公共秩序被梁平区公安局依法行政拘留。（来源：重庆网警）

7. 四川公安查处两起利用 AI 编造、传播网络谣言案件

1 月 11 日，公安部网安局发布消息称，2023 年 12 月以来，四川公安机关聚焦扰乱网络公共秩序等突出问题，积极开展打击整治网络谣言专项行动，截止目前，依法查处造谣传谣网民 33 人，清理网络谣言信息 743 条，关停违法违规账号 20 个。同时公布两起利用AI文章生成软件编造、传播网络谣言的典型案例。

案例一：2023 年 11 月，薛某以营利为目的，利用AI文章生成软件一键生成《一旦要打仗，启动一级战备，专家建议老百姓冲在最前线，报效祖国》的文章，并发布在某平台上，吸引网民阅读赚取流量获取收益。该谣言文章引发大量网民阅读浏览，阅读量达 11 万余人次，造成了恶劣的社会

影响。四川宜宾公安依据《治安管理处罚法》第二十五条对薛某进行行政处罚，并对其造谣网络账号采取关停措施。

案例二：2023 年 12 月 20 日，刘某群为博取流量，获得平台浏览奖励，将 2023 年 12 月实际发生在江西某地已被处理的“校园霸凌事件”截取相关事件图片后，利用AI小程序自动编辑功能，嫁接为发生在德阳某学校的“校园霸凌”虚假信息。他制作了标题为《12 岁女生被 8 人轮流扇耳光 3 小时，致耳膜穿孔》的文章在某平台发布，引发大量网民关注，对社会秩序、校园治理造成严重的负面影响。目前四川德阳公安依据《治安管理处罚法》第二十五条对刘某群进行行政处罚，并对其造谣网络账号采取关停措施。（来源：公安部网安局）

8. 因与公司发生矛盾，辽宁一男子利用漏洞致公司 200 台电脑瘫痪

1 月 12 日消息，辽宁一男子假扮“黑客”入侵公司服务器，恶意破坏公司网络，禁用公司 200 台电脑的域名解析功能，给公司造成混乱和损失。

1 月初，盘锦市兴隆台公安分局接到辖区内某企业报案称，其公司的网络遭到人为恶意破坏，造成公司网络瘫痪，无法正常运营生产。接到报案后，网安大队民警立即开展侦查工作。该公司聘请专业鉴定机构进行固定证据后，民警前往该公司将涉嫌破坏计算机信息系统罪的阿聪传唤至盘锦市公安局执法办案中心接受讯问。

经查明，该男子因工作矛盾心生怨恨，为报复他人，使用公司内部网络管理账号，登录网关管理系统，私自禁用公司 200 台电脑的域名解析功

能，造成上述电脑无法连接互联网，另外还禁用了公司 83 个VPN账户，导致VPN账户使用者无法通过VPN连接入公司内网。经讯问，犯罪嫌疑人对其犯罪事实供认不讳。1 月 8 日，犯罪嫌疑人已被盘锦市兴隆台区人民检察院批准逮捕，案件正在进一步侦办中。（来源：辽宁党建网）

9. 公安部网安局通报钟某团伙利用信息网络寻衅滋事案

1 月 3 日，公安部网安局通报钟某团伙利用信息网络寻衅滋事案。

近日，一则“温州帮竟然是缅北电诈后台”的虚假信息在互联网上大量传播，引发广泛关注。经公安机关调查，2023 年 9 月，犯罪嫌疑人钟某注册登记某信息科技公司，在网络平台注册“钟XXXX商”“钟XX置业”等130 余个账号。

2023 年 11 月 23 日，钟某收集缅北电信网络诈骗热点话题小道消息，编造内容为“缅北电信网络诈骗幕后是温州资本、温州帮在支持、运作”的虚假信息。然后，他采取自己演绎、讲解的方式，拍摄、剪辑了“缅北电诈团伙背后有温州帮、温州资本介入”“温州帮成为电信诈骗领域的一支生力军并给缅甸电诈恶行提供资金支持”等虚假视频信息，并指使员工转发、传播。犯罪嫌疑人吴某某、苏某某在钟某的指使下，组织其手下员工将该虚假信息编辑渲染后，在网络平台上大肆开展转发、传播。截至 2023 年 12 月 6 日，该虚假视频信息总计播放量为 324.9 万次，被点赞 11.8 万次、评论 1.2 万次、转发 12.1 万次、收藏 2.5 万次，造成恶劣影响，严重扰乱了社会公共秩序。

犯罪嫌疑人钟某编造、散布虚假网络信息，犯罪嫌疑人苏某某、吴某某组织人员在网络上大肆散布虚假信息，造成严重后果，其行为已触犯《刑法》，涉嫌寻衅滋事罪。浙江省温州市公安局鹿城区分局依法立案侦查。日前，经检察机关批准，犯罪嫌疑人钟某、苏某某、吴某某已被依法执行逮捕。案件正在进一步侦办中。（来源：公安部网安局）

（二）网信部门治理实践

1. 全国网信系统持续推进网络执法，查处各类网上违法违规行为

1 月 31 日，国家互联网信息办公室公布 2023 年网络执法情况。2023 年，全国网信系统共约谈网站 10646 家，责令 453 家网站暂停功能或更新，下架移动应用程序 259 款，关停小程序 119 款，会同电信主管部门取消违法网站许可或备案、关闭违法网站 14624 家，督促相关网站平台依法依约关闭违法违规账号 127878 个。

针对百度、必应、夸克浏览器等网站平台未按照法律法规要求尽到管理义务，在搜索环节呈现法律、法规禁止发布或传输的信息问题，国家网信办指导属地网信办分别依法约谈相关网站负责人，责令其限期整改，从严处理责任人，并分别给予罚款行政处罚。

针对抖音、新浪微博、腾讯微信等网站平台存在法律、法规禁止发布或者传输信息的问题，国家网信办指导属地网信办分别依法约谈相关网站负责人，责令其限期整改，处置相关账号，从严处理责任人，并分别给予罚款行政处罚。

针对快手、网易、小红书等网络平台履行主体责任不力，对其用户发布的信息未尽管理义务，造成血腥暴力、虚假信息、煽动对立等不良信息在网上传播；拼多多、淘宝、大众点评等生活服务类平台审核机制不完善，造成封建迷信、低俗色情信息在网上传播等问题，国家网信办指导属地网信办分别依法约谈相关网站负责人，责令其限期整改，处置相关账号，从严处理责任人，并分别给予警告、罚款等行政处罚。

维护网络安全、数据安全、个人信息安全方面。国家网信办根据网络安全审查结论及发现的问题和移送的线索，依法对知网（CNKI）违法处理个人信息行为作出网络安全审查相关行政处罚的决定。国家网信办指导属地网信办依法依规查处一批怠于履行网络安全和数据安全义务的违法违规企业，下架一批违法违规处理个人信息的移动应用程序，下架一批未按国家有关规定开展安全评估工作，存在较大安全风险的移动应用程序。

持续推进网络执法监督检查方面。国家网信办持续加强网络执法监督检查力度，不断强化日常监督检查、重点案件督查督办，积极开展执法人员能力建设，持续推进严格规范公正文明执法。各级网信部门严格落实法律法规规章规定，从线索核查、办理程序、法律法规适用、保障当事人权益等方面不断规范网络执法行为、提升案件办理质量，从“快、准、严、效”上下功夫，确保案件事实认定清楚、证据确凿充分、适用法律准确、程序合规合法、处罚精准适当。（来源：网信中国）

2. 国家网信办查处一批生活服务类违法违规平台账号

1 月 8 日，国家互联网信息办公室发布消息表示，自“清朗·生活服务类平台信息内容整治”专项行动启动以来，累计清理违法不良信息 790 万余条，处置账号 170 万余个，关闭网站 562 家，下架应用程序 201 个。同时通报部分典型案例，包括依法关闭为线下违法活动引流的平台及账号，严管地图导航、实用工具、健康资讯类平台传播违法不良信息，严肃查处传播违规营销信息的电商平台和店铺，依法处罚发布封建迷信信息的日历平台，集中整治搜索环节呈现违法信息问题，严厉打击推广招募网络水军行为等。（来源：中国网信网）

3. 中央网信办启动“清朗·2024 年春节网络环境整治”专项行动

1 月 29 日，中央网信办决定即日起开展为期 1 个月的“清朗·2024 年春节网络环境整治”专项行动，重点整治以下 6 方面问题：（一）宣扬猎奇行为、违背公序良俗问题；（二）散播网络戾气、煽动群体对立问题；（三）炮制虚假信息、恶意营销炒作问题；（四）色情赌博引流、网络诈骗问题；（五）鼓吹炫富拜金、无底线追星问题；（六）危害未成年人身心健康问题。（来源：网信中国）

4. 北京网信办公布北京数据出境安全评估、标准合同等制度落地情况

1 月 9 日，北京市网信办公布数据出境安全评估、标准合同等数据出境制度落地情况。数据出境安全评估方面，截至目前，已有 117 家在京企事

业单位正式提交数据出境安全评估申报材料，包括小米、联想、京东、美团、奔驰、宝马、苹果等国内国际知名企业。其中奥迪汽车、三星中国、葛兰素史克等45家单位的数据出境安全评估申请已被国家网信办受理；施耐德电气、瑞士再保险、联邦快递等39家单位获批通过安全评估。个人信息标准合同方面，诺华诚信成为全国首家通过订立标准合同实现个人信息合规出境的企业。（来源：网信北京）

5. 重庆市互联网信息办公室通报多款存在违法违规收集使用个人信息的App

1月10日，重庆市互联网信息办公室组织对人民群众关注度高的生活服务类、日常工具类等App、微信小程序开展检查检测，发现“唔姆”“觉晓法硕”等145款App（小程序）存在未公开收集使用规则、违反必要原则收集等违法违规问题。相关App（小程序）开发者应严格参照问题清单限期15日内完成整改，并将整改报告加盖公章反馈重庆市互联网信息办公室。（来源：网信重庆）

6. 重庆市通过首批企业个人信息出境标准合同备案

1月13日消息，重庆建设•雅马哈摩托车有限公司、达飞信息科技（重庆）有限公司提交的个人信息出境标准合同通过重庆市互联网信息办公室组织的备案审核，是重庆市首批通过订立标准合同实现个人信息合规出境的企业。（来源：网信重庆）

7. 因存在弱口令漏洞，重庆市长寿区网信办依法约谈区属某事业单位

1 月 12 日消息，重庆市长寿区网信办近日通过网络安全巡查发现，区内某事业单位办公系统存在 HTTP 弱口令漏洞。1 月 11 日，长寿区网信办依据《网络安全法》《党委（党组）网络安全工作责任制实施办法》等有关规定，对该事业单位及其主管部门进行约谈，要求该单位及其主管部门严格落实网络安全工作主体责任和本行业本领域网络安全指导监管责任，紧紧围绕网络安全风险防范，举一反三，开展自查整改。涉事单位表示，将开展全面网络安全隐患排查，增强网络安全防护，限期整改完毕。（来源：网信重庆）

8. 重庆市网信部门严厉打击网络违法违规行为，2023 年开展行政处罚案件 38 起

1 月 23 日消息，重庆市网信部门公布 2023 年网络执法情况。2023 年，重庆市网信部门累计约谈网站 310 家，暂停功能或更新网站 23 家，依法关闭违法违规账号 530 个，警告网站 326 家，关闭违法违规网站 227 家，向有关部门移交案件线索 2840 条，开展行政处罚案件 38 起，其中罚款处罚 10 起。

重庆市网信部门依法查处违反互联网网络安全的违法违规行为。一是严肃查处运营主体怠于履行网络保护义务的行为。针对渝北某培训中心、巴南一生产公司等 14 家企业怠于履行网络安全和数据安全保护义务，依法对其采取罚款、行政警告、处理责任人、责令整改等措施。

二是严厉打击网络数据泄露行为。针对未履行网络安全和数据安全保护义务，导致数据泄露等严重违法违规情形的重庆两家网络科技公司，作出罚款20万元的行政处罚。

三是严肃查处违法违规收集用户个人信息行为。针对涉及违规收集用户个人信息，未建立健全隐私保护政策、用户信息保护等制度的“小火车外卖”App运营主体重庆某科技公司、黔江某房地产开发公司等5家公司作出行政处罚，并责令改正。

四是约谈整改一批存在网络安全风险的平台。针对南岸区、巴南区、渝中区、大渡口区、长寿区、丰都县等区县部门业务系统存在网络安全风险，网信部门依法约谈相关部门负责人，责令其限期整改；针对“重庆市民通”“企伴商家版”“事考帮”“金标尺教师”“金标尺公考”等App违规收集用户个人信息，依法进行约谈，责令其限期整改。（来源：网信重庆）

9.因违规收集个人信息，重庆市云阳县网信办对“小世界交友”App作出行政警告处罚

1月31日消息，因违规收集使用个人信息，重庆市云阳县网信办对“小世界交友”App依法作出行政警告处罚。

经查，“小世界交友”App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、方式和范围等；违反必要原则，收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；未建立健全应急预案、用户信息保护等相关制度，违反《网络安

全法》《个人信息保护法》等互联网法律法规。云阳县网信办依法约谈该App负责人，责令限期整改，并给予行政警告处罚，严格督促该公司进一步加强App运营管理，落实好个人信息保护、网络数据安全等相关法律法规要求，健全完善相关管理制度，切实履行好网络平台主体责任。（来源：网信重庆）

10.因未尽消费者个人信息保护义务，上海市网信办依法处罚一批单位

1月29日消息，“亮剑浦江”专项行动期间，上海市区两级网信、市场监管部门累计检查企业6043家，依法对520余家企业进行约谈，查处各类个人信息保护案件50余件。部分企业虽然已被约谈要求整改或接受过普法培训，仍然存在对消费者个人信息收集存储不合规、制度规范不健全、管理措施不到位、安全防护不严密等问题。上海市网信办依法对一批未有效履行消费者个人信息保护责任、存在严重问题的知名企业予以行政处罚。部分典型案例如下：

在收集环节，强制要、过度取个人信息问题依然存在。如，某餐饮企业的外送微信小程序在收货地址填写环节，强制用户同意打开精准位置权限，否则无法添加收货地址，属于对消费者非必要个人信息强制索权。

在存储环节，大量个人信息未加密处于“裸奔”状态。如，某火锅餐饮连锁企业存储的手机号码、邮箱号码等1.5亿条会员个人信息以及包括身份证号码在内的18万条本公司员工个人信息；某停车扫码SaaS平台存储的8000条包括手机号码在内的车主信息、196万条车牌信息；某大型商

超购物企业存储的39万条家庭卡用户的手机号码、身份证号码等个人信息；某房产中介企业收集的200万条用户数据中的20万条客户手机号码等个人信息；某少儿培训机构存储的 4 万条学生姓名、监护人手机号码等个人信息，均未按规定采取加密、去标识化等安全保护措施。

在使用传输环节，企业随意授权放权管理不到位。不少企业在个人信息的使用和传输环节内控制度不严格，存在诸多薄弱问题。如企业内部操作权限设置不合理，在没有授权审批流程的情况下，相关工作人员可以导出包括手机号码在内的用户个人信息，容易导致数据被滥用；有房产中介企业经纪人在查看后台客源信息时，可以看到跨区域的用户手机号码等个人信息。

在管理制度上企业关于个人信息保护措施明显缺失。被处罚的企业普遍存在个人信息保护制度不完善的问题，大多未制定个人信息数据分类分级管理、数据访问权限管理、安全应急预案等制度，部分未按照法律规定确定个人信息保护责任人，建立数据资产管理、数据安全人员管理、数据合作方管理等制度。

在安全防护上网络信息系统存在安全漏洞。被处罚的企业存储使用大量消费者个人信息的网络信息系统都不同程度存在安全漏洞，如一家房产中介企业的网络安全高危漏洞达到 7 个，还有中低危漏洞 8 个，易被不法分子利用，存在大量数据被泄漏或被窃取等安全风险。（来源：网信上海）

11. 因泄露公民个人信息，湖南省衡阳市网信办对某科技公司罚款10万元

1月30日消息，因开发应用的网站数据库存在未授权访问的漏洞，导致公民个人信息泄露，湖南省衡阳市网信办依据《数据安全法》对北京某科技公司予以行政处罚。

经调查核实，该科技公司于2023年1月开发一家网站，存储了包含用户姓名、手机号、电子邮箱等在内的大量个人信息。该科技公司在开展数据处理活动时，未建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的措施保障数据安全。同时，在开展数据处理活动时未加强风险监测，造成个人信息泄露等问题，该网站存在未履行数据安全保护义务的违法行为。针对以上违法情况，衡阳市网信办依据《数据安全法》第四十五条有关规定，对该科技公司作出责令改正，给予警告，并处人民币10万元罚款的行政处罚。（来源：网信湖南）

（三）通信管理部门治理实践

1. 工信部、多地通信管理局通报问题APP

（1）工信部

1月22日，工信部通报侵害用户权益行为的APP（SDK）（2024年第1批，总第36批）。工信部近期组织第三方检测机构对用户反映突出的开屏弹窗“乱跳转”、“关不掉”以及违规收集使用个人信息等问题进行检查，共发现31款APP及SDK存在侵害用户权益行为，包括弹窗信息窗口“乱跳

转”误导用户、开屏信息窗口“乱跳转”误导用户、信息窗口未提供关闭或退出标识、超范围收集个人信息、违规收集个人信息、APP 强制、频繁、过度索取权限等。相关 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）上海市

1 月 4 日，上海市通信管理局 2023 年向社会公示四批共 91 款存在侵害用户权益行为的应用。在规定的二次整改期限内，经核查复检尚有 19 款应用未按照要求落实整改，涉及违规、超范围收集个人信息，App 强制、频繁、过度索取权限，未明示个人信息处理规则，未合理申请使用权限，强制用户使用定向推送功能，未提供注销功能，未承诺投诉处理时效等违法违规行为。

上海市通信管理局依据《网络安全法》《电信和互联网用户个人信息保护规定》《移动智能终端应用软件预置和分发管理暂行规定》等法律和规范性文件要求，已对上述应用在全国范围内主流应用市场进行下架处理。

（3）浙江省

1 月 5 日，浙江省通信管理局通报 2023 年第 11、12 批 19 款侵害用户权益行为的 APP。浙江省通信管理局组织第三方检测机构对群众关注的实用工具、网上购物、本地生活等类型 APP 进行检查，发现部分 APP 存在违规收集个人信息、强制频繁过度索取权限、频繁自启动和关联启动等问题。浙江省通信管理局书面要求违规 APP 开发运营者限期整改。

截至目前，尚有 19 款 APP 未按要求完成整改，予以通报处理。相关 APP 开发运营者在 1 月 15 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。（来源：工信部、上海通信圈、浙江省通信管理局）

（四）其他部门治理实践

1.多地成立省级数据局

（1）江苏省

1月5日消息，江苏省数据局已正式挂牌，是2023年国家数据局正式揭牌后成立的第一个省级数据局。江苏省政务服务管理办公室官网（http://jszwb.jiangsu.gov.cn/index.html）已更新为“江苏省数据局（江苏省政务服务管理办公室）”。

（2）四川省

1月11日，四川省数据局在成都正式挂牌。

（3）内蒙古自治区

1月11日，“内蒙古政府办公厅”微信视频号发布一则内蒙古自治区人民政府人事任免消息，任命自治区政务服务与数据管理局局长、副局长、大数据中心主任等职务。

（4）青海省

1月15日，青海省数据局揭牌成立，负责青海省数字基础设施、数据基础制度、数据共享开发利用、数据安全以及政务服务和公共资源交易监督管理等工作，承担着统筹推进数字青海、数字经济、数字社会发展职责。

（5）上海市

1 月 15 日消息，上海市数据局已正式揭牌成立，将完善上海大数据管理机构的设置和职能配置，在协同联动下再次促进上海数据要素生态的创新和发展，同时对全国后续开展的市县机构改革起示范作用。

（6）河北省

1 月 15 日，河北省数据和政务服务局正式揭牌成立。新组建的省数据和政务服务局主要负责统筹推进数字河北、数字经济、数字社会、数字政府规划建设和政务服务工作。

（7）云南省

1 月 15 日，云南省数据局正式挂牌。根据党中央、国务院批准的云南省机构改革方案，新组建的云南省数据局由省发展改革委管理，规格为副厅级。

（8）广东省

1 月 18 日，广东省政务服务和数据管理局正式挂牌成立。2024 年，广东省政务服务和数据管理局将履行好统筹推进数字广东、数字政府、数字经济、数字社会规划建设的职责，出台数字广东建设 2024 年工作要点，启动数字广东建设“十五五”发展规划编制。

（9）天津市

1 月 19 日，天津市数据局正式挂牌，将进一步加强天津市数据管理职责的整合优化，协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字天津、数字经济、数字政府、数字社会建设发展，以数字天津建设新成效，服务全市高质量发展“十项行动”。

（10）福建省

1 月 21 日，福建省数据管理局正式揭牌。

（11）湖北省

1 月 25 日，湖北省数据局正式挂牌成立，主要负责协调全省数据基础制度建设，统筹全省数据资源整合共享和开发利用，推进数字湖北、数字经济、数字政府、数字社会规划和建设。

（12）河南省

1 月 25 日，河南省数据局揭牌成立，统筹推动数字河南、数字经济、数字社会建设，立足河南实际，加强对数据基础制度、数据要素市场、数字产业化、产业数字化、数字社会、数字基础设施等领域的研究推进。（来源：青海省人民政府、福建日报、湖北省人民政府、河南省人民政府等）

2. 商务部：将探索建立以自由流动为基本原则、统筹安全和个人信息保护的数据跨境流动治理体系

1 月 19 日消息，商务部部长王文涛就“加快建设贸易强国”相关问题答记者问时表示，商务部将从升级货物贸易、创新服务贸易、发展数字贸易、深化国际合作以及维护贸易安全五个方面着手推动贸易强国建设。

数字贸易方面，商务部将出台数字贸易改革创新发展政策，明确我国数字贸易发展的制度和政策框架，进一步加强系统谋划、政策创新和跨部门跨领域统筹协调。做强做优国家数字服务出口基地，在数字服务市场准入、国际规则对接、跨境数据流动、数据规范化采集和分级分类监管等方面先行先试，培育科技、制度双创新的数字贸易集聚区。积极参与全球数

字贸易治理，立足自身制度框架，对接国际高标准经贸规则，探索建立以自由流动为基本原则、统筹安全和个人信息保护的数据跨境流动治理体系。（来源：商务部）

3. 国家金融监管总局：将加强网络安全和数据安全风险监管

1 月 25 日，在国务院新闻办举行的金融服务经济社会高质量发展新闻发布会上，国家金融监督管理总局新闻发言人、统计与风险监测司负责人表示，国家金融监督管理总局将持续加强监管引领，引导金融机构提升服务质效，全面加强风险管理。

一是持续推动银行业保险业数字化转型。开展数字化转型评估工作并纳入到银行保险机构信息科技监管评级中，引导金融机构加强顶层设计和统筹规划，科学制定发展战略，加大资源要素投入，实现经营管理和服务变革。

二是增强数字赋能成效。充分调动金融机构积极性和主动性，不断优化数字金融产品和服务，做好科技创新、先进制造、绿色发展和中小微企业等重点领域的金融支持，有效降低企业融资成本；同时积极拓展互联网移动终端等服务渠道，通过数字手段触达传统金融服务难以覆盖的客群，持续提高金融服务的普惠性和可获得性。

三是提升行业风险防控能力。推动银行保险机构将数字化风控工具嵌入业务流程，充分运用数字化能力提高风险管理和内控合规水平。

四是加强网络安全和数据安全风险监管。推动银行保险机构提高网络安全风险的日常监测和应急处置能力，有效保护数据安全和客户信息，强化数字生态场景下的科技外包风险管理。

五是规范数字创新，守住风险底线。要求银行保险机构建立稳健的业务审批流程，对新产品、新业务、新模式带来的技术和业务逻辑变化进行评估，确保新技术投产运用的审慎性和合规性，牢牢守住数字化转型过程中的风险底线。（来源：国家金融监督管理总局）

4. 因涉及信息安全风险，国家金融监管总局对中国银行、中信银行处以罚款

1 月 5 日，国家金融监督管理总局公开对中国银行股份有限公司、中信银行股份有限公司的行政处罚信息。

中国银行存在以下违规违法事实：（一）部分重要信息系统识别不全面，灾备建设和灾难恢复能力不符合监管要求；（二）重要信息系统投产及变更未向监管部门报告，且投产及变更长期不规范引发重要信息系统较大及以上突发事件；（三）信息系统运行风险识别不到位、处置不及时，引发重要信息系统重大突发事件；（四）监管意见整改落实不到位，引发重要信息系统重大突发事件；（五）信息科技外包管理不审慎；（六）网络安全域未开展安全评估，网络架构重大变更未开展风险评估且未向监管部门报告；（七）信息系统突发事件定级不准确，导致未按监管要求上报；（八）迟报重要信息系统重大突发事件；（九）错报漏报监管标准化（EAST）数据。

中信银行存在以下违规违法事实：（一）部分重要信息系统应认定未认定，相关系统未建灾备或灾难恢复能力不符合监管要求；（二）同城数据中心长期存在基础设施风险隐患未得到整改；（三）对外包数据中心的准入前尽职调查和日常管理不符合监管要求，部分数据中心存在风险隐患；（四）数据中心机房演练流于形式，部分演练为虚假演练，实际未开展；（五）数据中心重大变更事项未向监管部门报告；（六）运营中断事件报告不符合监管要求。

国家金融监督管理总局根据《银行业监督管理法》第二十一条、第四十六条和相关审慎经营规则，对中国银行、中信银行分别处以 430 万元、400 万元罚款。（来源：国家金融监督管理总局）

5. 证监会要求蜜雪冰城就赴港上市提供补充说明材料，涉数据安全与个人信息保护问题

1 月 19 日，证监会发布《境外发行上市备案补充材料要求公示》，要求蜜雪冰城针对赴港上市事宜补充提供五方面说明材料。其中，就数据安全与个人信息保护问题，要求蜜雪冰城说明开发、运营的网站、APP、小程序等产品情况，收集和存储用户信息规模、数据收集使用情况，是否存在向第三方提供信息的情形，以及上市前后个人信息保护和数据安全的安排或措施。（来源：中国证券监督管理委员会）

6. 住房和城乡建设部办公厅通报房地产中介行业侵犯公民个人信息违法违规典型案例

1 月 22 日，住房和城乡建设部办公厅通报 5 起房地产中介行业侵犯公民个人信息违法违规典型案例。

一、上海德佑房地产经纪有限公司员工非法对外出售公司内部业主信息案。上海德佑房地产经纪有限公司员工陈某、祝某某、马某合谋对外出售公司掌握的房屋业主信息来获利。三人通过马某的员工账号和权限访问公司大数据信息平台，查询并导出挂牌房屋的业主信息，将信息对外出售获取好处费。至案发，陈某从祝某某处获取好处费 20 万元，陈某给予马某好处费 6 万元。仅 2021 年 4 月，陈某对外发送信息共计 12716 条。2021 年 11 月，司法机关以侵犯公民个人信息罪判处陈某有期徒刑三年六个月，并处罚金人民币十万元；判处祝某某有期徒刑三年，并处罚金人民币八万元；判处马某有期徒刑一年十个月，并处罚金人民币五万元。

二、房地产经纪从业人员沈某某采取购买、收受、交换等方式非法获取公民个人信息案。2017 年至 2019 年，沈某某先后在无锡畅盛房地产经纪有限公司、无锡沪联房地产经纪有限公司、无锡链铺网络科技有限公司、无锡大玩家房地产营销策划有限公司等从事房产销售相关业务。期间，沈某某采用购买、收受、交换等方式，从周某某等人非法获取多个楼盘业主的公民个人信息，包括小区名称、门牌号、业主姓名、联系电话等，共计 78100 余条，并提供给他人共计 8600 余条。2020 年 12 月，司法机关以侵犯公民个人信息罪判处沈某某有期徒刑三年，并处罚金人民币二万元。

三、中山市裕丰房地产咨询有限公司员工非法购买公民个人信息案。2019 年 9 月，中山市裕丰房地产咨询有限公司西区翠景分公司员工黄某，为谋取利益，在添加谭某某微信号后，通过微信转账的方式向谭某某购买大量中山市相关楼盘小区住户的公民个人信息，包括公民姓名、住址、联系电话、房产面积等，共计 53590 条。2020 年 6 月，司法机关以侵犯公民个人信息罪判处黄某有期徒刑三年，并处罚金人民币五千元。

四、柯某利用“房利帮”网站非法获取、出售业主房源信息案。2016 年 1 月起，柯某开始运营“房利帮”网站并开发同名手机 APP，以对外售卖二手房租售房源信息为主营业务。运营期间，柯某对网站会员上传真实业主房源信息进行现金激励，吸引掌握该类信息的房地产中介人员注册会员并向网站提供信息，有偿获取大量包含房屋门牌号码及业主姓名、电话等非公开内容的业主房源信息，共计 30 余万条，以会员套餐方式出售获利达人民币 150 余万元。2019 年 12 月，司法机关以侵犯公民个人信息罪判处柯某有期徒刑三年，缓刑四年，并处罚金人民币 160 万元。

五、湖南省湘西自治州宜居房产经纪服务有限公司蔡某某私自留存业主信息开展业务案。湖南省湘西自治州宜居房产经纪服务有限公司负责人蔡某某在某售楼部从事房地产销售期间，利用职务之便，未经售楼部及业主同意，复印了 1095 条小区业主姓名、门牌号、房产面积、联系电话等资料。后蔡某某成立湘西自治州宜居房产经纪服务有限公司，利用这些业主信息资料开展房屋中介业务，用于在日常经营活动中给业主打电话，询问房屋是否需要出售、出租等。2022 年 3 月，司法机关以侵犯公民个人信息

罪判处蔡某某有期徒刑一年，缓刑一年，并处罚金人民币一千元。（来源：住房和城乡建设部）

7. 四川省成都市新都区检察院办理一起利用技术手段非法窃取公民个人信息案

1 月 5 日消息，四川省成都市新都区检察院近日办理一起利用技术手段非法窃取公民个人信息案。案中，网络黑客共攻击涉及全国 21 个省市的社保、医疗等共计 29 个行业的 51 个系统，非法获利 500 余万元。

经查，王某等人于 2021 年初至 2022 年 7 月通过网络渠道委托黑客，利用搜集到的各种政府、企业网络平台的接口漏洞，通过对接口进行数据抓包、参数解析等，开发出 100 余款黑客软件。王某等人利用相关黑客软件，先后入侵全国 21 个省市的社保、医疗等共计 29 个行业的 51 个系统，“爬取”包括姓名、身份证号、手机号码、工作单位、家庭成员、社保缴纳等在内的公民个人信息，并贩卖给相关催债公司。被盗的公民个人信息被催债公司大规模用于数据画像，勾勒人物关系和活动轨迹，由此通过手机短信、微信、抖音等社交平台向欠款人的社会关系人发送催债信息。通过梳理固定涉案数据、司法鉴定意见及审计的获利情况，该院认定该团伙非法获利达 500 余万元。

从数据掮客、黑客、网络催债公司三类人员着手，新都区检察院对从信息盗取源头到提供、倒卖、购买终端全链条各环节的 10 名犯罪嫌疑人提起指控，法院最终以侵犯公民个人信息罪判处王某等人有期徒刑三年至十个月不等。对作为催债公司中下层员工的犯罪分子，新都区检察院在训诫

后依法作出不起诉决定。同时，针对办案中发现的系统数据管理缺失、政务平台运维机制不完善等问题，新都区检察院于2023年9月向该区医保局制发检察建议，积极推动相关部门修补网络安全漏洞、加强保密安全培训、健全公民个人信息保护制度。（来源：正义网）

境外前沿观察：月度速览十则

导读：1 月，欧盟《网络安全条例》生效，为欧盟各机构、机关、办事处、部门搭建共同的网络安全框架，进一步提高欧盟机构内部的网络安全恢复能力和事件响应能力。欧盟《数据法》生效，构建公共机构访问和使用私营部门所持数据的机制。

美国商务部公布拟议规则《采取额外措施应对与重大恶意网络行为相关的国家紧急状态》，要求美国云服务厂商强化外国用户身份验证，限制外国行为者通过访问美国云数据中心进行人工智能模型训练。中国外交部表示，人工智能发展治理攸关全人类的命运，需要的是群策群力协调应对，而不是脱钩断链、围栏筑墙。

CyberED 公司预测 2024 年十大网络安全威胁趋势，高级勒索软件位居首要威胁，人工智能驱动的网络攻击、远程工作基础设施漏洞利用、供应链网络攻击等同样在列。欧洲央行宣布将在 2024 年对 109 家银行进行网络弹性测试，将模拟网络攻击情景，测试银行在遭受大规模攻击后的响应和恢复能力。伊朗核设施“震网”病毒事件查明，系美国、以色列利用荷兰间谍向伊朗纳坦兹核设施的电脑系统投放“震网”病毒所致。

关键词：欧盟《网络安全条例》、欧盟《数据法》、电子数据跨境调取、网络攻击、“震网”病毒、ChatGPT 数据安全执法

1. 欧盟《网络安全条例》生效

1 月 7 日，欧盟《网络安全条例》生效，旨在确保欧盟各机构、机关、办事处、部门采取共同的网络安全规则和措施搭建框架，进一步提高欧盟机构内部的网络安全恢复能力和事件响应能力。条例要点包括：（1）将“欧盟机构、机关和办事处的计算机应急响应组织”更名为“网络安全服务机构”，保留其“CERT-EU”简称，CERT-EU 将成为欧盟威胁情报、信息交换和事件响应的协调中心；（2）设立机构间网络安全委员会（IICB），推动并监测本条例的实施，指导 CERT-EU 工作，在 2024 年 9 月 8 日前向欧盟各机构、机关、办事处、部门发布指导方针，帮助其落实条例规定的义务；（3）建立网络安全风险管理、治理和控制框架。欧盟各机构、机关、办事处、部门应在 2025 年 4 月 8 日前建立网络安全风险管理、治理和控制框架，并至少每 4 年根据不断变化的网络安全风险审查该框架；在 2025 年 7 月 8 日前进行网络安全成熟度评估，并确保在此之后定期（至少每两年一次）进行评估；在 2025 年 9 月 8 日前，采取适当技术、操作和组织措施，加强网络安全风险管理、治理和控制，防范或尽量减少网络安全事件影响；在 2026 年 1 月 8 日前，制定改善网络安全计划，并获得领导层批准；在发生重大安全事件时向 CERT-EU 报告。（来源：欧盟委员会）

2. 欧盟《数据法》生效

1 月 11 日，欧盟《数据法》正式生效，将于生效之日起 20 个月后，即 2025 年 9 月 12 日起正式施行。该法要点包括：（1）赋予用户在各云数据处理服务提供者之间切换的能力；（2）构建公共机构访问和使用私营部门所持数据的机制；（3）制定使联网设备用户能够访问联网设备和相关服务所产生数据的措施；（4）制定防范非法数据传输的保障措施；（5）为各部门之间重复使用数据制定互操作性标准。（来源：欧盟委员会）

3. 美国商务部公布拟议规则《采取额外措施应对与重大恶意网络行为相关的国家紧急状态》，以限制外国实体利用美国云服务发展其人工智能技术

1 月 29 日，美国商务部公布拟议规则《采取额外措施应对与重大恶意网络行为相关的国家紧急状态》。拟议规则明确要求美国云服务厂商在提供云服务时，通过“了解你的客户程序或客户识别程序”验证注册或登录美国云计算账户的外国人身份，限制外国行为者对美国云服务产品的访问，并要求详细报告训练人工智能大模型的外国交易信息，以保护美国的网络安全和利益。此外，还设定识别外国用户的最低标准，并要求云计算公司每年进行合规性认证。

1 月 26 日，美国商务部长吉娜·雷蒙多表示，云计算服务新规旨在要求美国云计算公司确定包括中国在内的外国实体是否正访问美国云数据中

心来完善其人工智能模型，“我们不能让非国家行为体、中国或那些我们不想让他们访问我们云空间的人以此来训练他们的模型”。

1 月 29 日，中国外交部表示，人工智能发展治理攸关全人类的命运，需要的是群策群力协调应对，而不是脱钩断链、围栏筑墙。我们敦促美方，不要违背科技发展的客观规律，切实尊重市场经济和公平竞争的原则，为加强人工智能领域的国际协调合作创造良好条件。（来源：美国联邦公报、中国外交部）

4.《美国政府与澳大利亚政府为打击严重犯罪而获取电子数据协议》生效

1 月 30 日，《美国政府与澳大利亚政府为打击严重犯罪而获取电子数据协议》生效。美国司法部表示，协议将重塑并强化双方在处理恐怖主义、儿童性虐待等严重犯罪方面的国际合作，允许美国和澳大利亚执法机构更及时地访问伙伴国家服务提供商持有的电子数据，提升预防、侦查、起诉严重犯罪以及维护国家安全的能力，同时引入严格的隐私保护和监督机制。协议规定：（1）受本协议约束的命令应当遵照签发方的国内法发布，并有合理正当理由作为支撑，包括犯罪事实清楚可信以及正在调查的犯罪行为具备明确性、违法性和严重性；（2）受本协议约束的命令，在执行命令之前或在与执行命令有关的程序中，应接受法院、法官、治安法官或其他独立机构根据签发方的国内法进行审查或监督；（3）签发方可以直接向适用的提供者发出符合本协议的命令，命令应由签发方的指定机构传送，双方

的指定机构可通过相互协商，为此类机构规定规则和条件。（来源：美国司法部）

5. 美国 CISA 发布《2023 年度回顾》

1 月 17 日，美国网络安全和基础设施安全局（CISA）发布《2023 年度回顾》，展示 2023 年 CISA 在保护国家免受网络安全威胁方面所做的工作，总结网络安全、人工智能安全、关键基础设施保护等领域取得的成就，其要点包括：（1）促进安全设计原则。2023 年 4 月，CISA 发起“安全设计活动”，作为政府推动安全软件开发的一部分，以努力实现安全、可靠和韧性的未来。2023 年 10 月，CISA 和 17 个国内及国际合作伙伴联合发布新版《改变网络安全风险的平衡：安全设计软件的原则和方法白皮书》，敦促软件制造商改进设计和开发计划，生产安全设计产品；（2）引领人工智能应用与安全治理。2023 年 11 月，CISA 发布《人工智能路线图》，凸显美国国土安全部等政府机构为确保人工智能安全开发和部署所做的努力，并利用人工智能潜力优化网络防御；(3)降低勒索攻击风险。2023 年 3 月，CISA 启动“勒索提前通知计划”，通过警告组织提前识别勒索软件以降低攻击风险，计划启动以来共计发出 1000 多份通知；（4）支持关键基础设施安全保护。CISA 加强与易受网络攻击但安全资源贫乏的行业组织接触，包括供水和废水行业、中小学教育行业、医疗保健和公共卫生行业以及选举安全领域组织。2023 年，CISA 组织开展 6700 多次利益相关者与政府、

私营部门参与者的交流互动，涵盖网络安全威胁信息共享与网络安全服务推广。（来源：美国 CISA）

6.CyberED 公司发布《2024 年网络安全预测》，高级勒索软件位居首要威胁

1 月 2 日，CyberEd 公司发布《2024 年网络安全预测》（Cybersecurity Predictions for 2024）。

报告认为，2024 年十大网络安全威胁趋势分别是：（1）高级勒索软件。网络犯罪分子将使用先进的勒索软件策略、人工智能和深度伪造技术来增强他们的目标定位能力；（2）人工智能驱动的网络攻击。人工智能可用于自动化攻击，创建更有说服力的网络钓鱼活动并为社会工程提供深度伪造内容；（3）远程工作基础设施漏洞利用。黑客将瞄准远程工作基础设施，利用 VPN、云服务和远程桌面协议中的漏洞；（4）供应链网络攻击。针对第三方供应商和软件供应商的网络攻击将会加剧；（5）关键基础设施目标。对能源网、医疗保健系统、废水处理设施和交通网络等关键国家基础设施的网络攻击将会增加；（6）物联网设备漏洞。物联网设备将成为黑客想要创建大规模僵尸网络并获取网络访问权限的目标；（7）移动设备漏洞利用。随着对移动设备的依赖性日益增加，针对这些平台的攻击预计将大幅上升，包括对移动操作系统、应用程序、5G 等移动通信技术中漏洞的利用；（8）数据隐私泄露。网络犯罪分子将结合被盗信息建立更完整的身份信息以进行身份盗窃和金融欺诈；（9）国家支持的网络战。包括间谍活动、破坏活

动和影响力活动在内的网络战活动将会增加；（10）量子计算和密码学。组织将开始为后量子密码学做准备，以确保未来的通信安全。（来源：CyberEd）

7. 欧洲央行宣布，2024 年将对 109 家银行进行网络弹性测试

1 月 3 日,欧洲央行宣布将在 2024 年对 109 家银行进行网络弹性测试。测试包括以下内容：（1）模拟网络攻击情景，测试银行在遭受大规模攻击后的响应和恢复能力；（2）测试银行在识别和报告网络安全事件方面的能力；（3）针对核心银行业务系统、基础设施、网络环境进行安全渗透测试；（4）检查网络安全防护系统的完整性、有效性和恢复备份系统的能力等。此外,将有 28 家银行接受强化评估,需提交关于应对网络攻击的额外信息,以保证与其他监管活动的高效协调。（来源：欧洲央行）

8. 伊朗核设施“震网”病毒事件查明：系美以利用荷兰间谍投放病毒

1 月 8 日，荷兰《人民报》发布报道称，美国和以色列在 2007 年利用一名荷兰情报局的内线，对伊朗研发核武器的设施投入电脑病毒，导致伊朗核工业进展被迫延迟一年多。荷兰间谍埃里克·范·萨本利用进出伊朗纳坦兹核设施的便利，往该设施内的电脑系统投放“震网”病毒，使将近一千个核离心机自爆，对伊朗的核工业发展带来重大挫折。美国和以色列制定的具体方案是，制作“震网”病毒，在关键时刻关闭阀门，使得核离

心机无法出气，在系统显示一切正常情况下因气压过高自爆。报道称，多名荷兰情报人员表示，对于荷兰参与的这一针对伊朗的“战争行径”，荷兰情报部门实际上并不了解美国和以色列的具体计划，荷兰政府更是不知情。（来源：观察者网）

9.芬兰云服务商遭勒索攻击，导致瑞典众多公共机构系统瘫痪

1 月 22 日，芬兰云托管服务提供者 Tietoevry 发表声明，表示旗下位于瑞典的一个数据中心受到勒索攻击，导致大量客户受影响。受影响客户包括瑞典知名薪酬和人力资源公司 Primula,该公司客户涵盖瑞典大部分大学和 30 多家政府机构，攻击事件导致这些机构的员工无法提交事假申请或报销申请。自发现勒索攻击之后，Tietoevry 立即隔离受影响平台，公司其他部分未受影响。（来源：Tietoevry 官网）

10.意大利数据保护局认定 OpenAI 违反隐私法

1 月 29 日，意大利数据保护局发布《ChatGPT：意大利数据保护局通报 OpenAI 违反隐私法》，指出自 2023 年 3 月 30 日对 OpenAI 颁布临时禁令以来，根据相关事实调查结果，有证据表明 OpenAI 存在 GDPR 违规行为；若不服违规行为指控，OpenAI 可在 30 日内提交申诉；意大利数据保护局将在最终裁决中参考欧洲数据保护委员会 ChatGPT 工作组的调查结果。(来源：意大利数据保护局)

行业前沿观察一：2024 年中央一号文件发布，哪些内容和网络安全有关？

导读:党的十八大以来第 12 个指导“三农”工作的中央一号文件于 2024 年 2 月 3 日由新华社受权发布,提出有力有效推进乡村全面振兴“路线图”。其中，涉及数字化与网络安全的内容都有哪些呢？

有志愿者在的地方，处处有温暖；有志愿者在的地方，人人皆力量。冬去春来，全国网安联志愿服务队开展了一场又一场的志愿服务活动，完成了一个又一个公益项目，为全国网络安全志愿服务事业做出了极为重要的贡献。让我们一起回顾网安联志愿服务的 2023 年吧！

1. 2024 年中央一号文件发布，哪些内容和网络安全有关？

党的十八大以来第 12 个指导“三农”工作的中央一号文件于 2024 年 2 月 3 日由新华社受权发布，提出有力有效推进乡村全面振兴“路线图”。

这份文件题为《中共中央 国务院关于学习运用“千村示范、万村整治”工程经验有力有效推进乡村全面振兴的意见》，全文共六个部分，包括：确保国家粮食安全、确保不发生规模性返贫、提升乡村产业发展水平、提升乡村建设水平、提升乡村治理水平、加强党对“三农”工作的全面领导。

其中，涉及数字化与网络安全的内容主要有：

（八）落实防止返贫监测帮扶机制。加快推动防止返贫监测与低收入人口动态监测信息平台互联互通，加强跨部门信息整合共享。

（十三）推动农村流通高质量发展。实施农村电商高质量发展工程，推进县域电商直播基地建设，发展乡村土特产网络销售。

（十七）推进农村基础设施补短板。持续实施数字乡村发展行动，发展智慧农业，缩小城乡“数字鸿沟”。实施智慧广电乡村工程。鼓励有条件的省份统筹建设区域性大数据平台，加强农业生产经营、农村社会管理等涉农信息协同共享。

（二十四）建设平安乡村。持续开展打击整治农村赌博违法犯罪专项行动，加强电信网络诈骗宣传防范。

（二十七）完善乡村振兴多元化投入机制。发展农村数字普惠金融，推进农村信用体系建设。

2. 落地生根，开向全国——网安联·2023 年度网络安全志愿服务工作回眸

有志愿者在的地方，处处有温暖；有志愿者在的地方，人人皆力量。

志愿服务是社会文明进步的重要标志，是加强精神文明建设的重要内容，是新时代文明实践工作的重要抓手。而在这个新时代，社会发展、国家发展离不开互联网的发展，网络空间是否安全也深深影响着国家和社会的安全。

习近平总书记多次强调，没有网络安全就没有国家安全。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

为贯彻落实习近平总书记关于网络强国的重要思想和有关网络安全的重要论述，近年来，网安联大力开展网络空间安全志愿服务工作，组建网安联志愿服务队，培育发展全国范围的网络安全志愿服务力量，帮助广大群众深入了解网络安全的重要性、掌握必要的网络安全技能，服务国家网络安全和信息化事业高质量发展。

2023 年 3 月 2 日，民政部发布《关于学习贯彻习近平总书记重要指示精神深入开展学雷锋志愿服务活动的通知》，要求深入开展学雷锋志愿服务活动。通知指出，要推动志愿服务与互联网深度融合，进一步提升志愿服务信息化水平。要依托城乡社区综合服务设施、乡镇（街道）社工站等广泛设立志愿服务站点，拓展群众身边的志愿服务参与平台。

网安联积极响应《通知》要求，在持续开展原有的系列公益志愿活动和网民网络安全感满意度公益调查活动的基础上，2023 年立足北京、广东面向全国开展了网络安全志愿服务站、网络安全公益讲师等新的工作，并由志愿服务部人员承接了广州市天河区新时代文明实践中心实践活动项目，打造志愿服务品牌。

冬去春来，我们一起走过了充实的 2023 年，这一年里，全国网安联志愿服务队开展了一场又一场的志愿服务活动，完成了一个又一个公益项目，为全国网络安全志愿服务事业做出了极为重要的贡献。下面，我们就一起回顾网安联志愿服务的 2023 年吧~

一、播火种·益万民｜系列网络安全公益志愿服务活动

进机关、进企业、进校园、进社区、进乡村.....宣讲会、公益讲座、集市展位宣传、科普嘉年华、入户宣传.....2023 年，全国网安联志愿服务队深入一线开了系列网络安全公益志愿服务活动，广泛宣传网络安全知识，为广大群众、组织或社区提供网络安全方面的帮助和支持。

以北京、广东为主，回顾网安联 2023 年度部分活动：

2023 年 2 月 3 日，广州市番禺区·《科普网络文明 提高时代素养》网络安全知识讲座成功举办，以帮助青少年树立网络安全意识，提高网络防沉迷意识，引导青少年正确认识网络、运用网络，营造安全、文明、和谐的网络环境。

2023 年 3 月，网安联（广州）网络安全志愿服务队受邀参加“雷锋精神代代传，文明建设志愿行”学雷锋日公益集市活动，设置摊位宣传网络安全，为广大群众提供网络安全知识科普和相关咨询服务。

2023 年 3 月，网安联网络安全志愿服务队协同网警，开展网络安全进养老院活动，为长者们宣传普及用网安全和个人信息安全保护知识。

2023 年 4 月，网安联（广州）网络安全志愿服务队协同越秀网警参加志愿集市，开展“全民国家安全教育日”网安知识宣传活动，助力增强全民国家安全意识和素养。

2023 年 5 月，第五届广东科普嘉年华活动在广东科学中心举办，网安联广东、广州志愿服务队参加活动，并在会场设置网络安全知识宣传（青少年防沉迷）摊位，开展科普主题网络安全知识宣传活动。

2023 年 5 月，网安联广东、广州网络安全志愿服务队走进花都区，与花都网警联合开展花都区“六一”儿童节暨青少年网络安全主题教育活动，助力增强青少年网络安全意识和防护技能，建立、健全教育网络系统。

2023 年 5 月，网安联·网络安全志愿服务活动走进写字楼开展网络安全宣传进企业活动，进一步普及网络安全知识，提高企业对电信网络诈骗犯罪的鉴别能力和防范意识。

2023 年 6 月，“防范金融诈骗 构建美好社区——金融知识万里行暨反电信网络诈骗宣传活动”举行，居民们通过学习网安联印发的网络购物防骗、青少年防沉迷、养老防诈骗等宣传资料，加深了对网络风险的认知。

2023 年 6 月，“防范金融诈骗 构建美好社区——金融安全知识科普社区行暨反电信网络诈骗宣传活动”走进广州市越秀区建设街党群服务中心，通过丰富多元的宣传和互动形式，提高社区居民抵御电信网络诈骗、金融风险陷阱能力。

网络无边，安全有界。2023 国家网络安全宣传周期间，网安联多地志愿服务队协同网警、网信部门等开展的网络安全系列宣传活动，进一步向社会大众普及网络安全知识，帮助群众提升网络安全意识和防护技能，营造安全有序和健康向上的网络环境。

2023 年 9 月，“耆乐融融，敬老助老”敬老月社区志愿服务大行动启动仪式成功举行，仪式上宣布成立“网安联·绿网使者”志愿服务队（广州队），该队伍由广州网络空间安全公益讲师组成，为长者开展网络安全宣讲等网络安全相关志愿服务。

2023年10月,“金融安全知识科普社区行暨反电信网络诈骗宣传活动”,走进了越秀区黄花岗街党群服务中心，为参加活动的市民讲解预防电信网络诈骗的知识和金融诈骗相关信息，进一步增强广大群众防范电信网络诈骗意识。

2023 年 11 月，网安联·网络安全志愿服务队组织网络空间安全公益讲师，协同网警开展了“防范新型诈骗 筑牢安全阵线”网络安全主题讲座，以新型网络诈骗案例分析为切入点，向社区居民宣传科普不法分子的诈骗手段以及如何通过法律途径维护自身权益。

2023年11月,北京石景山枫一社区新时代文明实践站开展了主题为“打击整治养老诈骗 维护老年人合法权益”的普法宣传活动，介绍了针对老年人朋友常见的网络电信诈骗以及以人工智能(AI)技术为代表的新型诈骗手段，帮助老年朋友提高防范意识和反诈能力。

2023 年 11-12 月，北京网络空间安全协会网安联志愿者服务队开展系列“进社区”网络安全公益宣传活动，通过多个活动的开展，为海淀区、石景山区、老通州区等多区的街道社区居民宣传网络电信诈骗知识，以及人工智能（AI）换脸新技术等新型网络诈骗手段，帮助大家了解最新网络安全动态，提高网络安全意识和防范技能。

二、扎深根·发新芽｜网安联·网络安全志愿服务站

2023 年，在全国各级公安网警、网信、民政等部门的支持和指导下，“网安联·网络安全志愿服务站”开始建立，目前已在全国多个省市挂牌设站。

网络安全志愿服务站作为政府公共服务延伸到社区的工作平台，承担配合相关党政部门开展网络安全治理的公共职能，致力于推动社区网络安全宣传教育及志愿服务工作，同时根据网民群众在信息服务、发声反馈、维权等方面的需求，畅通居民网络安全求助以及维权举报渠道，搭建服务站交流平台及评价机制。

2023 年 3 月，广州市越秀区建设街大马路社区网络安全志愿服务站挂牌成立，为社区居民提供网络安全相关便民服务。

2023 年 3 月，广州医科大学附属肿瘤医院网络安全志愿服务站正式挂牌成立，以助力提升医院职工及患者网络安全意识和安全防护技能，保障职工及患者在网络空间的合法权益。

2023 年 4 月，“网安联·网络安全志愿服务站”正式入驻时代邻里控股有限公司和广州有好戏网络科技有限公司。

2023 年 5 月，北京市公安局丰台分局右安门派出所、北京网络空间安全协会、北京市丰台区右安门窦珍志愿服务联合会三方召开座谈会，就共建“网安联·网络安全志愿服务站”，打造全国网络安全志愿服务站标杆案例等事宜进行深度洽谈。

2023 年 5 月，花都区青少年网络安全主题教育活动暨网络安全志愿服务站授牌仪式在花都区新时代文明实践中心成功举办，服务站成立后常态化组织服务站志愿者，开展网络安全知识宣传等网络安全志愿服务活动。

2023 年 5 月，揭阳市崇善网络安全志愿服务站签约成立，标志着“网安联·网络安全志愿服务站”正式走进广东揭阳，服务揭阳群众。

2023 年 6 月，广东食品药品职业学院签约网络安全志愿服务教育基地（服务站），切实提升在校师生的网络安全意识以及网络安全防护能力，以多种形式进行网络安全科普教育。

2023年7月,湖北省信息网络安全协会与安徽中科晶格技术有限公司、银河水滴共建的“110 数智网安实训平台”和“数智网安江陵实训基地”正式授牌，该平台和基地借助网安联大平台及网安联志愿服务队资源，整合资源、优化配置，提高网络安全保障能力和水平。

2023 年 8 月-10 月，借助“2023 网民网络安全感满意度调查活动”，全国多个省市的企事业单位、志愿服务机构申请成立“网安联·网络安全志愿服务站”，推动当地网络安全志愿服务事业发展，服务群众、服务社会、服务国家。

2023 年 11 月，北京网络空间安全协会与东北大学秦皇岛分校计算机与通信工程学院团委签订了“共建网络安全志愿服务站合作协议”，并在学院正式挂牌。帮助学院全校师生提高网络安全法律法规意识、反诈意识和防范能力，树立正确的网络安全观。

三、播火种·树品牌｜网民网络安全感满意度调查活动

为全面了解、反映广大网民对我国网络安全状况的感受和看法，向各级党政有关部门开展互联网治理与监管提供详实的网情民意支撑，2023 年，网安联连续第六年牵头组织开展网民网络安全感满意度调查大型公益活动暨“我为群众办实事”实践活动，助力提升网民群众获得感、幸福感、安全感和满意度。

2023 网民网络安全感满意度调查活动（以下简称“2023 调查活动”）由全国 135 家网络安全行业协会及相关机构、公益组织共同发起，开展了调查活动第二个五年计划（2023-2027）开局之年的系列活动，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，共收获全国网民参与答题总样本量 224.7269 万份。

经过第一个五年的积累，2023 调查活动首次尝试让志愿服务团队作为深入一线采集样本的主力军。在两个阶段的采集工作中，参与采集的网络安全志愿服务站、志愿团队、志愿者等志愿力量结合本地的活动，通过“边调查、边学习、边宣传”逐步熟悉网络志愿服务工作，进一步完善全国各地相关网络志愿服务工作的机制和服务流程。

2023 年调查活动中，组委会成功组织全国各省市的网安联·志愿服务站（队）、志愿者、公益讲师、公益宣传员等基层力量，进机关、进网站、进企业、进校园、进社区，深入一线开展问卷调查，服务广大人民群众，让网络空间安全更加深入人心，形成全国一道网络志愿服务靓丽风景线，吸引了众多原本网络安全意识淡薄的人参与活动，提高网络安全意识，并成为了传播网络安全知识的公益宣传员。为网络强国和网络文明建设注入志愿服务新力量，同时推动全国范围内有意向的志愿服务团队从传统服务向“传统+网络”服务转型升级。

四、筑同心·凝斗志｜网络安全志愿者培训会、交流会

2023 年，是网安联鼓足干劲大力开展网络安全志愿服务工作的一年，进入新的轨道，采用新的机制，也引入了一股“强而新”的志愿服务力量。如何让这股来自全国各地各类人群汇聚而成的新力量，高效率高质量的完成网络安全志愿服务工作？网安联秘书处志愿服务部为此策划开展了多场次、多系列的培训/交流活动。

2023 年 6 月，“网安联志愿服务交流会”召开，网络安全志愿服务站、志愿团队、社工、企业、社区、艺术团的志愿代表相聚线上线下，分享介绍、交流互动，进一步推进“网安联·网络安全志愿服务站/教育基地”建设工作，宣导网络安全公益讲师认证申报事项，推进 2023 网民网络安全感满意度调查活动启动工作。

2023 年 8 月，2023 网安联工作年会系列活动在广州隆重举行，来自全国各地的网络安全行业协会及相关机构、志愿团队齐聚一堂，碰撞思想火花，在研讨期间，就进一步贯彻习近平总书记对深入开展学雷锋活动作出的重要指示和关于走好网上群众路线重要论述等问题展开分析和讨论，并实地参观了作为实践基地试点之一的广州市越秀区建设街大马路社区服务站。

网络安全志愿服务培训会

为进一步帮助加入网安联·网络安全志愿服务工作的全国各地志愿组织及个人更好地了解、开展相关工作，在日后活动中能更好运用发挥自身能力，切实为广大网民群众提供优质、全面的网络安全志愿服务，2023 网安联·网络安全志愿服务培训第一、第二期分别于 2023 年 7 月、8 月通过全国线上连线的形式成功举办。

培训会就网安联志愿服务、网络安全志愿服务站的建设、网络安全公益讲师、网安联小程序的志愿服务板块和操作使用、2023 年网民网络安全感满意度调查活动等内容进行了详细介绍讲解，帮助大家快速了解网安联的网络安全志愿服务体系，让大家快速掌握相关操作及活动组织开展事项。

会议还向大家介绍了网络安全志愿服务队、志愿服务站、网民网络安全感满意度调查活动之间的关系，帮助大家梳理思路，明确方向。

网络空间安全公益讲师培训

2023 年 8 月，网安联·网络安全志愿服务培训（第三期）成功举行，重点为网络空间安全公益讲师及其认证的相关内容。来自全国各省市的志愿组织、部分网安联成员单位的志愿者和相关人员参加培训。

天河区新时代文明实践中心实践活动项目筹备会

2023 年，广州市天河区委宣传部筹备建设天河区新时代文明实践中心，由广东省网络空间安全协会承担系列活动项目的策划和执行，以实践中心为圆点辐射全区乃至全市、全省开展丰富多彩的主题活动。

2023年12月，网安联秘书单位-广东省网络空间安全协会会长黄丽玲、党支部书记林勇忠以及协会秘书处、志愿服务部一行应邀到访广州市天河区文化馆，与广州市天河区委宣传部文明科、志愿服务中心领导以及天河区文化馆馆长陈岚以及文化馆志愿服务部、运营部相关负责人进行座谈，就天河区新时代文明实践中心的建设以及系列文明实践活动项目进行交流讨论。

行业前沿观察二：各地协会动态

导读：新年伊始，各地协会开展了精彩纷呈的活动。北京网络空间安全协会守护年初岁尾，走进什刹海社区，为老人们网络安全保驾护航；广东省网络空间安全协会召开第二届第六次会员代表会议暨第二届理事会第十次会议；上海市信息安全行业协会举行“豌豆杯”2024 迎新掼蛋邀请赛；陕西省信息网络安全协会举办年会，并进行会员表彰和精彩的主题发言；湖北省信息网络安全协会召开第三届一次会员大会，产生新一届协会领导班子和理事会成员；海南省网络安全和信息化协会举办了第六届海南省网络安全五指山论坛暨协会首届年会；新疆互联网协会表扬会单位中国移动新疆分公司的范勇樟，满腔热忱带头铺路为人人。

1.北京：守护年关网络安全，为老人保驾护航

北京网络空间安全协会与什刹海社会心理服务中心共同开展反诈宣传活动。

随着科技的飞速发展，互联网已经深入到我们生活的方方面面，而老年人作为社会的重要一环，却常常成为网络诈骗的目标。为此，北京网络空间安全协会联合什刹海社会心理服务中心，以“打击整治养老诈骗，维护老年人合法权益”为主题，开展了一场意义非凡的反诈宣传活动。

岁末年关之际，为了有效增强社区广大中老年朋友防范网络电信诈骗的能力，保障老年人的合法权益，北京网络空间安全协会携手什刹海社会心理服务中心，在该中心开展了此次宣传活动。活动结合当前新型的AI技术等手段在诈骗中的应用，由协会志愿服务部高级公益讲师郭会甫进行了深入浅出的讲解。他分享了《养老诈骗知多少》和《警惕“AI换脸”新骗局》等内容，详细介绍了针对老年人的常见网络电信诈骗以及以人工智能(AI)技术为代表的新型诈骗手段。

在宣传活动中，郭老师不仅提示在场居民下载“国家反诈中心”APP，还传授了如何保护个人信息、如何识别和避免诈骗的一些实用技巧。他强调了不贪图小便宜、不轻信“熟人”、多方核实确认对方真实身份、不轻易转账不汇款的重要性，帮助老年朋友提高安全防范意识和防骗能力。

活动的交流互动环节更是精彩纷呈。中老年朋友们纷纷发言，分享自己的见解和经历。他们列举了各种新型电诈手段，提出了对AI诈骗手法的

疑问，并咨询防范措施。活动现场还发放了龙年气球，寓意着祝愿居民在龙年幸福安康。整个活动现场气氛热烈，圆满成功。

（来源：北京网络空间安全协会）

2. 广东：协会召开第二届第六次会员代表会议暨第二届理事会第十次会议

1 月 19 日下午，广东省网络空间安全协会（以下简称协会）第二届第六次会员大会暨第二届理事会第十次会议在广州召开，广东省公安厅原常务副厅长、协会原名誉会长张圣钦，广东省民政厅社会组织管理局原副局长徐祖平，协会会长黄丽玲出席大会。省协会各常务副会长、副会长、常务理事、理事、会员单位代表参加会议。协会党支部专职副书记、副秘书长黄汝錫主持会议。

广东省网络空间安全协会会长黄丽玲致欢迎辞，代表协会感谢出席第二届第六次会员代表会议暨第二届理事会第十次会议的各位来宾。黄丽玲表示，新的一年，协会将在广东省社会组织管理局的领导下，坚持能力建设、规范协会运作，在核心团队 20 多年社团运作和行业经验的沉淀积累的基础上继续努力，把已有的各个核心工作品牌活动做得更好、更强！

广东省公安厅原常务副厅长、协会原名誉会长张圣钦在大会上表示，17 年来自己见证了协会的发展壮大，为协会如今的好成绩感到高兴。当前网络安全事业的发展面临挑战，形势紧迫，网络诈骗层出不穷，严重威胁

广大群众的财产安全，新时代的网络战更是一场看不见硝烟的战争，影响社会安全和国家安全。没有网络安全就没有国家安全，网络发展那么快，管理工作必须要跟上。

广东省民政厅社会组织管理局原副局长徐祖平提到，协会是我省社会组织标杆，是广东省优秀社会组织、双5A级社会组织、广东省社会组织先进党组织，这些荣誉得来不易。协会依法依章，诚信自律办会，在党和政府的支持下，取得了一系列创新成果，开展了信创大赛、网民网络安全感满意度调查活动、安满周、数据安全保障高研班等一批特色鲜明、影响广泛、口碑优良的品牌项目；成立了广东省科协信创联合体、广东省网络空间安全协会网安联科技服务站；发布了《网络志愿服务规范》等多项团体标准，为网络安全领域的发展做出了贡献。

大会还听取并审议第二届理事会2023年工作报告、财务报告、监事报告。

协会黄丽玲会长总结时，点明新一年的工作方向：2024年协会将加大力度在会员发展和服务上进行更多的投入，接下来会成立会员中心，将协会平台上的资源更多地往会员服务体系来倾斜。2024年协会将致力于把会员部做大做强，改造成一个会员中心，更好地服务会员。并表示希望协会在接下来发展过程中能够得到各会员单位的加持，也同时能够带着所有会员单位走向一个更新的发展平台！

（来源：广东省网络空间安全协会）

3. 上海：“豌豆杯”2024 迎新掼蛋邀请赛圆满落幕

为提升会员单位企业形象，丰富会员单位企业文体活动，1 月 27 日，由上海市信息安全行业协会、上海金融信息行业协会、上海市信用服务行业协会联合主办，上海豌豆信息技术有限公司独家冠名，紫羚云特别支持的“豌豆杯”2024 迎新掼蛋邀请赛在上海市虹口区桥牌协会顺利开赛，来自金融信息、信息安全、信用服务行业的共 24 支队伍参赛。

赛事伊始，比赛裁判丁老师为大家讲解了重点赛事规则，上海豌豆信息技术有限公司 COO 宋娅莉女士宣布“豌豆杯”2024 迎新掼蛋邀请赛正式开赛。

比赛期间，各参赛队伍以牌会友，配合默契，现场不乏紧张激烈的对决博弈和互相交流的欢声笑语，充分展现了运筹帷幄，决胜千里的精神风采。本次比赛以《竞技掼蛋竞赛规则（试行）》为准，采用积分编排赛制，经过 5 轮激烈角逐，最终决出了冠亚季军。

赛后，上海豌豆信息技术有限公司营销部总监鲁彦呈先生为冠亚季军颁奖，紫羚云&速邦咨询联合创始人兼副总裁梁灵鸽女士为 4-11 名颁发了纪念品。

本次赛事的开展，不仅寓教于乐，丰富了行业企业的文体活动，更为参赛各方提供了展现自我，结交朋友，提升同行交流的机会。在此新春之际，协会也祝愿大家在新的一年里保持积极向上、敢打敢拼的精神风貌，为行业和企业高质量发展再建新功。

（来源：上海市信息安全行业协会）

4. 陕西：协会年会成功举办

1 月 18 日下午，陕西省信息网络安全协会年会成功举办。陕西省委网信办陈亚东总工程师、陕西省公安厅网安总队刘战胜队长、陕西省大数据局吴晨二级巡视员，陕西省卫生健康信息中心吴德刚副主任、陕西省大数据产业协会曹栋梁名誉会长、陕西省文物考古工程协会赵强秘书长、协会专家咨询委员会全体专家、协会医疗健康专委会专家、协会高等教育专委会专家、地市网安协会协会领导、副理事长单位、理事单位、协会会员单位代表等共 150 余人参加了此次大会。

孙大跃会长总结协会 2023 年工作以及安排协会 2024 年主要工作，淡战平秘书长汇报协会 2023 年财务情况。

协会为了表彰 2023 年优秀理事单位、优秀会员单位、优秀用户单位、优秀个人、技术创新、安全服务和安全管理单位，经单位自荐、专家评选，产生了 12 个单位奖和 1 个个人奖，由孙大跃会长和专家委员会几位专家代表为获奖单位和个人颁发牌匾。

协会是平台、是桥梁、是纽带，为了更好的服务用户和会员，协会和深信服公司经过多次研究探讨，拟创建陕西省信息网络安全协会网络安全监测平台，并在会上举行了签约仪式。随后深信服徐诗运总经理和孙大跃会长分别做发言。

会上陕西云长信息科技有限公司总经理王涛和陕西省数字证书认证中心股份有限公司销售经理王保江为大家做专题演讲。会议最后邀请协会网

络安全咨询委员会几位专家进行技术交流与研讨。（来源：陕西省信息网络安全协会）

5. 湖北：协会第三届一次会员大会暨换届大会成功召开！

2024 年 1 月 19 日下午，湖北省信息网络安全协会第三届一次会员大会暨换届大会举行。

省委网信办、省公安厅、高校代表及全体会员单位代表出席会议，共同见证湖北省信息网络安全协会新一届领导班子的诞生。

大会听取并审议了协会第二届理事会工作与财务情况报告、党组织负责人开展党建工作有关情况通报。并成立“湖北省信息网络安全协会医卫分会”，其中医卫分会主要成员有，华中科技大学同济医学院附属协和医院、华中科技大学同济医学院附属同济医院、华中科技大学同济医学院附属梨园医院、武汉市中西医结合医院（武汉市第一医院）、江汉大学附属医院、武汉市卫生健康信息中心、武汉大学中南医院、武汉儿童医院、武汉市肺科医院、武汉市第八医院（肛肠医院）。

大会选举产生新一届协会领导班子以及理事会成员。中科安信科技有限公司总经理王耀发当选湖北省信息网络安全协会新一届理事会会长，湖北省楚天云有限公司总经理徐博、杭州安恒信息技术股份有限公司总经理彭建军、湖北天地和兴科技有限公司总经理汪立志、武汉卓讯互动信息科

技有限公司董事长刘亚卓、湖北省信息网络安全协会资深专家刘明当选副会长，安徽中科晶格技术有限公司杨育金当选协会监事。

为更好推动协会发展，提高工作效率。大会还宣读了第三届秘书处人事任命，任命刘莉为协会秘书处秘书长、刘长久为协会秘书处副秘书长，刘刚剑任协会秘书处副秘书长，蔡思任协会党支部副书记兼财务主管，任命唐红玲为协会秘书处办公室主任。

湖北省信息网络安全协会新一届理事会会长王耀发发表连任发言时指出，作为湖北省信息网络安全协会，要精准把握当前工作面临的新形势、新任务，增加工作针对性，推动大数据战略计划纵向发展，大力构建网络安全保障体系。今后，协会将继续学习贯彻习近平总书记关于网信工作的重要指示和全国网信工作会议精神，带领全体会员坚定履行建设网络强国、筑牢国家网络安全屏障的职责使命，坚决贯彻落实党中央关于网络安全工作的决策部署，引导会员单位提升产业基础研发能力、推动核心技术，协同攻关继续做好网络安全新职业建设系列工作；推动网络安全教育、技术、产业融合发展；加强全民网络安全宣传教育，提高人民群众网络安全意识和防护技能。

湖北省公安厅网安总队相关领导就目前协会的网络安全工作提出几点要求：明确指导思想，坚持学习贯彻落实习近平总书记有关网络安全工作的指示批示精神；围绕为民服务，坚持以问题为导向，高度重视关键信息基础设施防护、电信网络诈骗、青少年网络保护等问题；应用新型技术，用超前意识抵御风险、化解问题。围绕最新情况，通过协会，各单位组织

开展交流讨论，针对网络安全发展提出规划、做出保障，有效增强新型技术实用性。

（来源：湖北省信息网络安全协会）

6. 海南：第六届海南省网络安全五指山论坛暨海南省网络安全和信息化协会首届年会在海口举行

1 月 19 日，由中共海南省委网络安全和信息化委员会办公室指导，海南省网络安全和信息化协会主办的第六届海南省网络安全五指山论坛暨海南省网络安全和信息化协会首届年会在海口举行，会议以“自贸港数据流动保护创新发展”为主题，旨在完善《海南自由贸易港建设总体方案》要求的“数据安全有序流动”制度设计，通过研究数据流动保护技术来促进数据产业发展。来自国家数据安全机构、网信领域的领导和专家、海南省党政、金融、电信、医疗、教育、政法等行业和企事业单位主管网络安全和信息化建设的领导和业务骨干共 300 余人参加了本次活动。

海南省委网信办副主任黄坚敏在致辞中提到，省网信协会要认真贯彻落实省委、省政府决策部署，紧密结合海南自贸港建设，充分发挥搭平台、建桥梁、促发展的职能作用，更加广泛地汇聚网信人才，更加有效地凝聚社会合力，协助网信部门充分发挥海南自贸港政策优势，以创新技术促进数据安全有序流动，助力数字经济高质量发展。

海南省委深改办副主任廖增梁在致辞中表示海南已进入高质量发展期，通过对地方特色产业赋能，加大应用场景的构建，做好风险防控，全面提升海南数字经济产业发展的竞争力。

海口市政府副秘书长黄德禧为论坛致辞，他表示应加快推动数字经济产业高质量发展，打造跨境数据有序流动，积极推进人工智能应用，为海南相关产业发展带来新的机遇，实现互利共赢。

中国电子信息产业发展研究院副总工程师兼网络安全研究所所长刘权院士在致辞中谈到海南应创新数据新产业新模式，激活数据要素，打造独特的数据产业模式。

年会上，受协会理事长林明瑜委托，常务副理事长李春报总结了 2023 年度协会工作，并向大会报告了年度财务情况。会议选举组成了新一届监事会，同时表彰了 2023 年度先进个人和团体。

论坛上还同时召开了自贸港数据流动保护创新发展闭门会议。

（来源：海南省网络安全和信息化协会）

7. 新疆：“移”心为民|行而不辍 履践致远 范勇樟 满腔热忱 我为人人

2022 年 5 月加入喀什叶城县棋盘乡欧壤（4）村驻村工作队。他是队长的好助手、同事的好搭档、村民的好朋友，他往深里走、往实里走、往心

里走，他家至户察，带头搞建设，让村庄旧貌换新颜，携手村民走上康庄大道。

东奔西走听诉求。范勇樟通过入户调查，直接深入了解农户的生活状况、困难诉求以及他们的思想动态，及时进行记录和整理，为今后工作提供了重要的参考依据。入户工作还加强了与村民之间的互动与沟通，形成了牢固的情感纽带。

与民携手齐修路。村庄里巷道的路面损坏严重，给村民的通行带来极大的不便。范勇樟与工作队同事积极筹划，购买水泥、召集泥瓦工，对路面进行修复，周边村民亦纷纷自发地从家中带来木材，协助工作队完成水泥路面的围闭工作，避免车辆和行人误入，确保修复工作的顺利进行。

扶困助老不停歇。每年作物成熟时，范勇樟与工作队员都会帮助村里外出打工的村民和行动不便的老人采收作物，在全体人员的共同努力下，作物被有序地收割、捆扎和搬运，确保了丰收成果创收最大化。

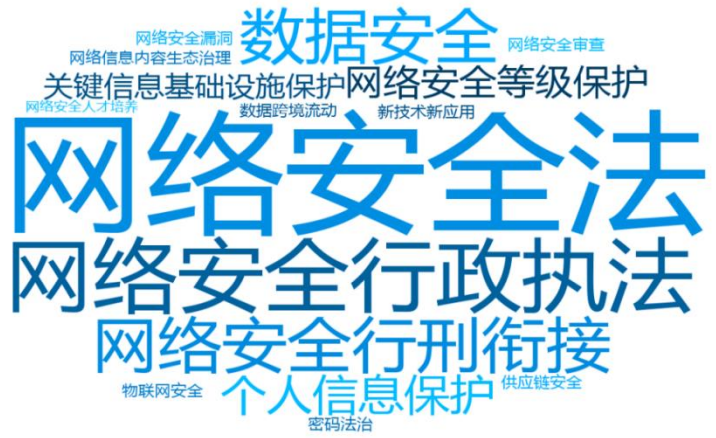
背对城市的霓虹，走向乡村的月光，挑起担子，播希望之种，挽起袖子，铺振兴之路，移动人始终心系基层，日夜不息，风雨兼程，只为绘就更美好的明天。

（来源：新疆互联网协会）

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

……