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

2024年3月第3期（总第8期）

2024年3月19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

声明：本刊定位于网络与数据安全前沿动态梳理，侧重全面跟踪、及时掌握，如需针对特定领域或前沿动态进行针对性专题研究，请将需求发送至cinsabj@163.com。

目　录

境内前沿观察一：政策立法

导读：2 月，修订后的《保守国家秘密法》正式通过。此次修订高度重视涉密信息系统、涉密数据、网络信息保密管理等方面，要求涉密信息系统规划、建设、运行、维护全流程应当符合国家保密规定和标准，并配备保密设施、设备，明确涉密信息系统定期风险评估要求，避免“带病运行”。

国务院印发《关于进一步规范和监督罚款设定与实施的指导意见》，指出“行政执法工作面广量大，一头连着政府，一头连着群众，直接关系群众对党和政府的信任、对法治的信心。”就网络执法而言，《网络安全法》《数据安全法》《个人信息保护法》均规定了罚款这一行政处罚类型，《个人信息保护法》更加将罚款数额与个人信息处理者上一年度营业额相挂钩，赋予包括公安机关在内的执法部门较大的自由裁量权。因此，严格监督罚款的实施十分重要，《指导意见》要求严格按照法律规定和违法事实实施罚款，不得随意给予顶格罚款或者高额罚款，不得随意降低对违法行为的认定门槛，不得随意扩大违法行为的范围。

其中，临港新片区管委会印发的《中国（上海）自由贸易试验区临港新片区公共数据管理办法》中规定“公共数据授权运营管理部门严格按照‘原始数据不出域，数据可用不可见’要求，在保护个人隐私和确保公共数据安全前提下，开展公共数据授权运营。”天津市商务局、自贸试验区管委会印发的《中国（天津）自由贸易试验区企业数据分类分级标准规范》中给出重要数据识别标准，天津自贸试验区企业掌握的 1000 万人以上个人

信息/100 万人以上个人敏感信息/被国家认定为关键信息基础设施的运营者掌握的个人信息等应识别为重要数据。

此外，贵州省大数据发展管理局印发《贵州算力券管理办法（试行）》。具体来说，“贵州算力券”是一种政策工具和数字化凭证，将用于支持省内外企业、高校、科研机构等购买贵州算力服务时抵扣一定比例服务费用。

关键词：保守国家秘密法、罚款、公共数据开放利用、数据分类分级、算力券

（一）国家层面动向

1.《保守国家秘密法》正式修订通过，完善网络信息、数据保密管理

2 月 27 日，第十四届全国人民代表大会常务委员会第八次会议修订通过《保守国家秘密法》，自 2024 年 5 月 1 日起施行。

此次修订高度重视保密科技创新和科技防护：一是新增条款支持保密科技创新；二是完善保密科技防护制度措施。一方面，规定涉密信息系统规划、建设、运行、维护全流程应当符合国家保密规定和标准，并配备保密设施、设备，明确涉密信息系统定期风险评估要求，避免“带病运行”；另一方面，规定机关、单位加强对信息系统、信息设备的保密管理，建设保密自监管设施，及时发现并处置安全保密风险隐患；三是规范用于保护国家秘密的安全保密产品和保密技术装备管理。

此次修订还进一步完善网络信息保密管理制度：一是明确网络信息的制作、复制、发布、传播等各个环节均应当遵守国家保密规定；二是规定网络运营者应当配合有关部门对涉嫌泄露国家秘密案件进行调查处理；发现利用互联网及其他公共信息网络发布的信息涉嫌泄露国家秘密的，应当及时处置报告，并根据要求删除涉及泄露国家秘密的信息，对有关设备进行技术处理等。此次修订还加强与数据安全法的协同衔接，新增涉密数据管理及汇聚、关联后涉及国家秘密数据管理的原则规定。（来源：中国政府网）

2. 国务院印发《关于进一步规范和监督罚款设定与实施的指导意见》

2 月 9 日，国务院印发《关于进一步规范和监督罚款设定与实施的指导意见》，对行政法规、规章中罚款设定与实施作出全面系统规范。

意见以“罚款设定更加科学，罚款实施更加规范，罚款监督更加有力，全面推进严格规范公正文明执法，企业和群众的满意度显著提升”为主要目标，从依法科学设定罚款、严格规范罚款实施、全面强化罚款监督三方面提出十二项意见。

具体来说，意见要求政府立法要严守罚款设定权限，科学适用过罚相当原则，新设罚款和确定罚款数额时，该宽则宽、当严则严，避免失衡；能够通过教育劝导、责令改正、信息披露等方式管理的，一般不设定罚款。合理确定罚款数额，规定处以一定幅度的罚款时，罚款的最低数额与最高数额之间一般不超过 10 倍。任何行政机关都不得随意给予顶格罚款或者高额罚款，不得随意降低对违法行为的认定门槛，不得随意扩大违法行为的范围。制定罚款等处罚清单或者实施罚款时，要确保过罚相当、法理相融。坚持处罚与教育相结合。（来源：中国政府网）

（二）部委层面动向

1. 中央网信办等四部门联合印发《2024 年提升全民数字素养与技能工作要点》

2 月 21 日消息，中央网信办、教育部、工信部、人力资源社会保障部联合印发《2024 年提升全民数字素养与技能工作要点》。

工作要点部署6个方面17项重点任务。一是培育高水平复合型数字人才，包括全面提升师生数字素养与技能、提高领导干部和公务员数字化履职能力、培育高水平数字工匠、培育乡村数字人才、壮大行业数字人才队伍；二是加快弥合数字鸿沟，包括建设数字无障碍环境、提供普惠包容的公益服务；三是支撑做强做优做大数字经济，包括加快企业数字化转型升级、扩展数字消费需求空间；四是拓展智慧便捷的数字生活场景，包括推动数字公共服务普惠高效、提升重点生活领域数字化水平；五是打造积极健康有序的网络空间，包括营造共建共享社会氛围、构建数字法治道德规范、维护安全有序数字环境；六是强化支撑保障和协调联动，包括完善协同支撑体系、加大优质数字资源供给、积极参与国际交流合作。（来源：中国网信网）

2. 工信部印发《工业领域数据安全能力提升实施方案（2024-2026年）》

2月23日，工信部印发《工业领域数据安全能力提升实施方案（2024-2026年）》。

方案是指导未来三年工业领域数据安全工作的纲领性规划文件，以构建完善工业领域数据安全保障体系为主线，以落实企业主体责任为核心，以保护重要数据、提升监管能力、强化产业支撑等为重点，从总体要求、重点任务、保障措施三方面提出主要内容。

重点任务方面，方案围绕提升工业企业数据保护、数据安全监管、数据安全产业支撑三类能力，明确提出11项任务。其中，关于提升工业企业数据保护能力，提出增强安全意识、开展重要数据保护、强化重点企业管理、深化重点场景保护4项任务；关于提升数据安全监管能力，提出完善政策标准、加强风险防控、推进技术手段建设、锻造监管执法能力4项任

务；关于提升数据安全产业支撑能力，提出加大技术产品和服务供给、促进应用推广和供需对接、健全人才培养体系 3 项任务。（来源：工信部）

3. 国家邮政局发布《寄递服务用户个人信息安全管理办法（征求意见稿）》

2 月 1 日，国家邮政局发布《寄递服务用户个人信息安全管理办法（征求意见稿）》。征求意见稿共三十二条，对经营和使用寄递服务涉及用户个人信息安全的活动以及邮政管理部门监督管理工作作出规定。

征求意见稿明确，除征得用户个人同意外，寄递企业保存用户个人信息的期限不得超过收集之日起三年，法律、行政法规另有规定的，从其规定。保存期限届满，寄递企业应当主动删除用户个人信息。删除个人信息从技术上难以实现的，寄递企业应当停止除存储和采取必要的安全保护措施之外的处理。

征求意见稿规定，寄递企业应当对用户个人信息依法进行去标识化处理。快递电子运单的去标识化应当考虑正常寄递服务的需求。寄递企业授权电商使用本企业的快递单号资源时，应当要求电商对快递电子运单中的个人信息执行去标识化。寄递企业应当与电商等第三方签订协议，明确去标识化执行主体、数据传输以及数据转化等相关事项。（来源：国家邮政局）

4. 自然资源部印发《自然资源数字化治理能力提升总体方案》，要求统筹信息化高质量发展与安全

2 月 5 日，自然资源部印发《自然资源数字化治理能力提升总体方案》，旨在推动自然资源整体治理数字化转型升级，高效保障“两统一”核心职责履行，切实提高政府履职能力、协同共享水平。

总体方案聚焦六方面主要任务，分别是建设集约高效数字化基础设施、完善全域全周期数据要素体系、提高国土空间基础信息平台智能化水平、构建多维数字化应用场景、筑牢全方位安全体系、健全完善制度标准规范体系。

数据要素方面，方案要求为数据驱动的业务规则重构、数据新型生产要素作用发挥、国土空间高效治理奠定基础。包括提升自然资源和国土空间变化态势感知能力，丰富“一张图”数据资源，推进数据汇聚治理融合，创新数据开放共享模式等。安全方面，方案要求统筹信息化高质量发展与安全。包括增强网络安全保障能力，强化数据安全保护能力，健全密码应用保障体系、加强新技术新业态安全保护（云安全、算法安全、模型安全等）。（来源：中国政府网）

5. 财政部发布《关于加强行政事业单位数据资产管理的通知》

2 月 8 日，财政部发布《关于加强行政事业单位数据资产管理的通知》。

通知要求明晰管理责任，健全管理制度。各部门应当根据工作需要和实际情况，建立健全行政事业单位数据资产管理办法，针对数据资产确权、配置、使用、处置、收益、安全、保密等重点管理环节，细化管理要求，明确操作规程，确保管理规范、流程清晰、责任可查。

通知要求规范管理行为，释放资产价值。加强数据资产源头管理，在依法履职或提供公共服务过程中，应当按照规定的范围、方法、技术标准等进行自主采集、生产加工数据形成资产。通过购置方式配置数据资产的，应当按照预算管理规定科学配置，涉及政府采购的应当执行政府采购有关规定。依据《数据安全法》等规定，做好数据资产加工处理工作，提高数据资产质量和管理水平。积极推动数据资产开放共享，在确保公共安全和保护个人隐私的前提下，加强数据资产汇聚共享和开发开放，促进数据资产使用价值充分利用。

通知要求严格防控风险，确保数据安全。各部门及其所属单位要认真贯彻总体国家安全观，严格遵守《网络安全法》、《数据安全法》、《个人信息保护法》等法律制度规定，落实网络安全等级保护制度，建立数据资产安全管理制度和监测预警、应急处置机制，推进数据资产分类分级管理，把安全贯穿数据资产全生命周期管理，有效防范和化解各类数据资产安全风险，切实筑牢数据资产安全保障防线。各部门及其所属单位应当按规定做好国家数据安全风险评估。（来源：财政部）

6. 全国信安标委发布《信息安全技术 云计算服务安全能力评估方法（征求意见稿）》

2 月 4 日，全国信安标委发布《信息安全技术 云计算服务安全能力评估方法（征求意见稿）》。

征求意见稿规定依据GB/T 31168—2023《信息安全技术 云计算服务安全能力要求》，开展评估的原则、实施过程以及针对各项具体安全要求进行评估的方法。适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估，云服务商在对自身云计算服务安全能力进行自评估时也可参考。（来源：全国信安标委）

7.《网络安全技术 生成式人工智能服务安全基本要求》等 17 项网络安全国家标准项目立项

2 月 6 日，全国网络安全标准化技术委员会发布通知，17 项网络安全国家标准项目立项，包括《网络安全技术　生成式人工智能服务安全基本要求》《网络安全技术 软件物料清单数据格式》《网络安全技术 信息过滤产品技术规范》《网络安全技术 数据泄露防护产品技术规范》等。（来源：全国网络安全标准化技术委员会）

（三）地方层面动向

1. 上海市印发《上海市落实<全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案>的实施方案》：探索开展公共数据开发利用

地方立法动向方面，数据仍是不变的热门话题。公共数据的开放利用和安全管理、数据跨境流动、数据分类分级标准成为 2 月上海、天津两地自贸区立法活动的重要关注。

2 月 3 日，上海市人民政府印发《上海市落实〈全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案〉的实施方案》。实施方案从加快服务贸易扩大开放，提升货物贸易自由化便利化水平，率先实施高标准数字贸易规则，加强风险防控体系建设等方面作出规定。

加快服务贸易扩大开放方面，实施方案明确在国家数据跨境传输安全管理制度框架下，金融机构可以向境外传输日常经营所需的数据。金融机构开展数据出境工作，应按照数据分类分级管理及数据安全工作要求，开

展数据出境安全评估、个人信息保护认证和个人信息出境标准合同备案，保证重要数据和个人信息的安全。

率先实施高标准数字贸易规则方面，实施方案明确规范和促进数据跨境流动，探索建立合法安全便利的数据跨境流动机制，提升数据跨境流动便利性。通过加强相关行业出境数据分类指导、发布示范场景、在临港新片区建立数据跨境服务中心等，便利数据处理者开展数据出境自评等数据出境安全合规工作。促进数据开放共享，鼓励公共数据在保护个人隐私和确保公共安全的前提下，按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供，探索开展公共数据开发利用，鼓励开发以数据集为基础的新产品和服务。（来源：上海市人民政府）

2. 临港新片区管委会印发《中国（上海）自由贸易试验区临港新片区公共数据管理办法》

2 月 4 日，临港新片区管委会印发《中国（上海）自由贸易试验区临港新片区公共数据管理办法》，自 2024 年 3 月 5 日施行。

管理办法共七章三十二条，围绕公共数据收集、登记、归集与治理，公共数据共享、开放与应用，公共数据授权运营及公共数据安全等方面作出规定。适用于公共数据的收集、登记、归集、治理、共享、开放、应用、授权运营及安全保障等公共数据全生命周期管理工作。

其中，管理办法明确公共管理和服务机构应当合法、必要、适度地收集公共数据。可以通过共享方式获得公共数据的，应避免通过其他方式重复收集。公共数据授权运营管理部门严格按照“原始数据不出域，数据可用不可见”要求，在保护个人隐私和确保公共数据安全前提下，开展公共数据授权运营。依托安全管控机制和安全服务产品，实施授权数据分类分

级管理，加强公共数据授权全流程安全管控。公共管理和服务机构按照“谁管业务，谁管业务数据，谁管数据安全”的原则明确重要岗位人员的数据安全责任和要求，签署数据安全责任书，并开展数据安全测评和风险评估，保障公共数据安全。（来源：上海市人民政府）

3. 临港新片区管委会印发《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》

2 月 8 日，临港新片区管理委员会印发《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》，旨在进一步指导和帮助数据处理者高效合规地开展数据跨境流动。

办法共七章二十一条，主要围绕职责及分工、数据跨境分类分级管理、重要数据目录管理、一般数据清单管理、监督管理及违规处置作出规定。适用于在临港新片区范围内登记注册的，或在临港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。

办法明确，结合上海“五个中心”建设，围绕汽车、金融、航运、生物医药等重点领域以及临港新片区相关行业的发展要求，以跨境需求最迫切的典型场景为切入口，对跨境数据进行分类管理。按照《数据安全法》要求，跨境数据分级从高到低依次分为核心数据、重要数据、一般数据共 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。

临港新片区管委会负责制定纳入数据出境安全评估管理范围的重要数据目录，并报相关部门备案。同时按照要求制定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，报经市委网络安全和信息化委员会批准后，报相关部门备案。数据处理者对重要

数据目录内的数据，可通过临港新片区数据跨境服务中心申报数据出境安全评估。（来源：临港新片区管理委员会）

4. 天津市商务局、自贸试验区管委会印发《中国（天津）自由贸易试验区企业数据分类分级标准规范》

2 月 5 日，天津市商务局、自贸试验区管委会印发《中国（天津）自由贸易试验区企业数据分类分级标准规范》，适用于天津自贸试验区内企业在生产经营过程中产生、收集、存储、传输和处理的数据的分类分级。涉及国家秘密的数据、政务数据的分类分级不包含在规范适用范围之内。

数据分类方面，标准规范将自贸试验区内企业在生产经营过程中收集、存储、使用、加工、传输、提供、公开的数据按照所属行业性质分类，依次分为三层，每个层级又分成若干类目管理。同一层级的类目构成并列关系，不同层级类目构成隶属关系。一层分类划分为战略物资和大宗商品类、自然资源和环境类、工业类、国防科技工业类、电信类、广电视听传媒类、金融类、交通运输类、卫生健康和食品药品类、公共安全类、互联网服务和电子商务类、科学技术类以及其他数据类共十三类。二层分类是在一层分类的基础上，将十三类数据细分为四十个子类别。三层分类由数据处理者自行决定。

数据分级方面，天津自贸试验区企业数据从高到低分为核心数据、重要数据、一般数据 3 个级别，同时明确重要数据识别标准。根据标准规范明确的统一识别规则，以下数据应识别为重要数据：（一）天津自贸试验区企业掌握的 1000 万人以上个人信息；100 万人以上个人敏感信息；10 万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息；（二）被国家认定为关键信息基础设施的运营者掌握的个人信息；（三）天津自贸试验区企业在研发设计过程、生产制造过

程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据。涉及国家安全的企业供应链相关数据；（四）天津自贸试验区企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。（来源：天津市自贸试验区管委会）

5. 北京市发布《北京市关于进一步优化外商投资环境加大吸引外商投资力度的若干措施》，试点探索便利化数据跨境流动安全管理机制

2 月 7 日，北京市人民政府办公厅发布《北京市关于进一步优化外商投资环境加大吸引外商投资力度的若干措施》。文件围绕提高利用外资质量，保障外商投资企业国民待遇，持续加强外商投资保护，提高投资运营便利化水平，完善外商投资促进方式等方面作出规定。

其中，文件明确要试点探索便利化数据跨境流动安全管理机制。落实网络安全法、数据安全法、个人信息保护法等要求，持续完善“绿色通道”服务机制，进一步做好重点领域外商投资企业数据出境合规指导，为符合条件的外商投资企业提供数据跨境便利化服务，提升审核与备案效率。持续推进本市数据跨境安全与产业发展协同创新中心、跨国企业数据流通中心、数据治理与跨境服务中心等服务平台建设，提供数据跨境流动合规服务。分类分级开展数据出境安全管理，进一步优化数字营商环境。（来源：北京市人民政府办公厅）

6. 贵州省大数据发展管理局印发《贵州算力券管理办法（试行）》

2 月 19 日，贵州省大数据发展管理局印发《贵州算力券管理办法（试行）》。办法指出，贵州算力券是经贵州省人民政府批准，由贵州省大数

据发展管理局实施的一种政策工具和数字化凭证，用于购买符合条件的贵州算力服务或贵州数据交易产品时，给予综合政策激励。

办法规定，算力券包含现金券和实物券两种。需求方和提供方均可申领算力券，但算力提供方不得申领。同一业务只能一方申领。算力券仅限于申领方自己使用，不得转让、赠送、买卖、质押、出借、重复使用等。算力券有效期为 6 个月，自发放之日起计算，逾期未使用的算力券将自动作废。

贵州省大数据发展管理局表示，算力券政策将推动算力产业发展，促进数据资源流通，带动相关产业链发展。通过加大对企业用算的支持，持续激发释放算力需求，牵引带动更多省内外企业使用贵州省算力，吸引更多的企业和机构选择在贵州进行算力投资和布局。（来源：贵州省大数据发展管理局）

境内前沿观察二：治理实践

导读：2 月，最高人民检察院通报依法惩治网络犯罪、助力网络空间综合治理工作进展。据统计，2023 年 1 至 11 月，检察机关共起诉各类网络犯罪 28 万人，同比上升 35.5%，占全部刑事犯罪的 18.8%。最高检表示，网络犯罪不断滋生蔓延，网络诈骗、网络暴力、侵犯公民个人信息等犯罪升级演变。总的看，当前网络犯罪呈多发高发态势。

国家数据局等四部门联合开展全国数据资源情况调查，调研各单位数据资源生产存储、流通交易、开发利用、安全等情况。调查对象包括各省重点数据采集和存储设备商、消费互联网平台和工业互联网平台企业、大数据和人工智能技术企业、应用企业、数据交易所、国家实验室等单位。

浙江省、上海市网信办公布 2023 年执法工作成效。行政指导、行政检查、行政约谈、行政告诫、行政处罚等已成为网络执法的重要方式。2023 年，浙江全省网信部门累计对重点平台企业开展行政指导 300 余次、行政检查 160 余次。对于初次违法、情节轻微且无主观过错、及时改正的新生企业，分类采取行政约谈、行政告诫等柔性执法方式。上海市网信部门依据《个人信息保护法》对一批怠于履行个人信息保护义务的知名企业进行处罚，是地方网信办自主办理的首批系列行政处罚案件。

多地通信管理局发布通知，明确自 4 月 1 日起，对逾期未履行备案手续的境内存量移动互联网应用程序（含APP、小程序、快应用等），将依法采取下架、关停等处理措施，网络接入服务提供者、应用分发平台、智能

终端生产企业应全面落实“先备案后服务”要求，不得为未备案APP提供网络接入、分发、预置等服务。

结合 2 月公布的行政案件，组织在开展网络安全保护工作过程中，应高度重视漏洞安全管理，定期进行漏洞扫描，及时对漏洞进行处置。2 月涉及的行政案件包括“北京某公司所属网站出现涉赌违法信息，经查该公司存在已经半年未进行漏洞扫描等违法行为，被处以警告”“北京某公司网站存在SQL注入漏洞，经查发现存在没有定期开展网络漏洞扫描工作等违法行为，被处以警告”。此外，因存在系统漏洞、弱口令等问题，重庆市涪陵区、高新区、秀山县等地网信部门对某区级行业主管部门、区级部门、图书馆、旅游景区等多家单位进行约谈。

关键词：网络犯罪、网信执法、APP备案、数据资源调查、漏洞管理

（一）公安机关治理实践

1. 广州 20 万网约车司机信息遭公开售卖，犯罪嫌疑人已被警方控制

2 月 20 日消息，广东省广州警方近日查获一起出售网约车司机信息案件，涉及约广州 20 万网约车司机。

近日，有记者在某社交平台上发现，有用户声称持有十几万名广州网约车司机的个人信息，并公开向网友询问变现方法。2 月 18 日，记者与该用户李某某联系，了解到被公开贩卖的个人信息数量庞大，达 20 多万条，包含司机的姓名、手机号、车型和所属平台等，被泄露信息的司机主要源自T3 出行、广州鹏鹏网约车服务有限公司、广州畅风科技有限公司、广州卓越出行汽车租赁有限公司等网约车平台公司。

李某某称自己曾在多家网约车平台工作，由于知道这些信息有用，从一开始便有意导出数据。其表示上述信息是在平台系统不完善时期导出的，或是从能接触到数据的内部人员得到。由于目前自己不再从事网约车平台工作，于是便想将信息出售变现。如按照 3 毛/条的售价计算，李某某每售出一份司机信息包，将获得 5 万至 6 万元的收益。对于购买网约车司机信息包的用途，李某某表示，主要用于平台竞争对手“挖人”或汽车保险推销。其曾向被泄漏信息的司机发送营销短信，用于网约车平台拉新工作。每注册成功一个，将获得 60 元提成。而招募其他平台司机加盟新的平台，成功率在千分之六左右。

2 月 19 日，记者将掌握的信息提供给广州警方。近日，记者从广州警方办案民警处获悉，在接获线索当日，警方便已对此案进行立案侦查。目

前，涉嫌侵犯个人信息的犯罪嫌疑人李某某已被警方控制。（来源：九派财经）

2. 北京网警通报 5 起网络安全行政处罚案例

2 月 26 日消息，北京网警通报 5 起网络安全行政处罚案例。

案例一：北京某科技信息服务有限责任公司所属网站内出现涉赌违法信息。该公司官网为静态页面，涉事服务器为虚拟服务器，用户访问静态文件不需要任何权限。2023 年 11 月 12 日，有人进入公司服务器内将文件改写成赌博网站信息。经查，该网站联网使用后，系统没有在公安机关进行网络安全等级保护备案，对系统的漏洞扫描已是半年前。该公司网站系统未落实网络安全保护义务，未采取防范计算机病毒和网络侵入等技术措施。北京市公安局东城分局根据《网络安全法》第二十一条、第五十九条之规定，责令该公司整改并给予警告的行政处罚。

案例二：北京某科技有限责任公司未落实网络安全保护责任，无内部网络安全管理制度以及操作规程，其内部的网站存在被植入不法链接、跳转赌博网站的漏洞，属于不履行网络安全保护义务的行为。北京市公安局门头沟分局根据《网络安全法》第二十一条第一项、第二项、第五十九条第一款之规定，责令该公司整改并给予警告的行政处罚。

案例三：北京某科贸有限公司网站发现存在SQL注入漏洞。经查，该公司网站没有制定管理制度，没有定期开展网络漏洞扫描工作，未依法采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。北京市公安局密云分局根据《网络安全法》第二十一条、第五十九条第一款，责令该公司整改并给予警告的行政处罚。

案例四：北京某装饰工程有限公司网站存有违法信息，该网站未对其发布的信息进行有效审核及管理，导致该违法信息在网络上发布，造成不良影响，属于不履行网络信息安全管理义务的行为。北京市公安局大兴分局根据《网络安全法》第六十八条第一款之规定，责令该公司整改并给予警告的行政处罚。

案例五：北京某科技有限公司所使用的一款寄快递微信小程序存在安全隐患，经对小程序进行检测，发现该款小程序存在高风险漏洞 5 个，容易造成数据泄漏的风险。北京市公安局通州分局依据《网络安全法》第二十一条第二项、第五十九条第一款的规定，责令该公司整改并给予警告的行政处罚。（来源：公安部网安局）

3. 陕西西安、香港警方破获两起“AI 换脸”诈骗案

2 月 26 日消息，陕西西安警方近期破获一起“AI换脸”诈骗案。该案中，陕西西安财务人员张女士与老板视频通话，老板要求她转账 186 万元到一个指定账号。转账之后，张女士按照规定将电子凭证发到公司财务内部群里，老板称未要求转账。张女士意识到被骗遂报警求助，警方对接反诈中心、联系相关银行进行紧急止付，最终保住大部分被骗资金 156 万元。

香港警方近期也披露了一起AI“多人换脸”诈骗案，涉案金额高达 2 亿港元。在该起案件中，一家跨国公司香港分部的职员，受邀参加总部首席财务官发起的多人视频会议，并按照要求前后转账多次，将 2 亿港元转账到 5 个本地银行账户内，其后向总部查询方知受骗。警方调查得知，这起案件中，所谓的视频会议中，只有受害者一人为“真人”，其余所谓参会人员，全部是经过AI换脸后的诈骗人员。（来源：西安公安）

（二）网信部门治理实践

1. 浙江省网信办公布 2023 年执法工作成效

2 月 1 日，浙江省网信办公布 2023 年执法工作成效。2023 年，浙江省网信系统坚决把依法治网作为基础性手段，坚持“依法依规、有力有效、宽严相济、精准执法”原则，聚焦人民群众反映强烈的网上违法违规问题，全面系统推进严格规范公正文明执法，营造清朗有序的网络空间。

一是出重拳，依法严处网上违法违规行为，确保互联网在法治轨道上健康运行。全省网信部门持续加大执法力度、强化执法震慑，重点查处发布虚假不实信息、扰乱网络传播秩序、传播淫秽色情信息、危害网络安全、数据安全、侵害公民个人信息等典型网络违法违规案件。约谈“ChatYuan”等网站平台账号 700 余次，责令整改“好范文网”等网站平台 1000 余家次，下架“蓝莓直播”等APP和小程序 180 余个，对“天天好书网”等账号主体采取禁言、关闭等措施 500 余次。

二是强服务，探索打造服务型网络执法监管模式，持续提升网络空间法治健全度。全年累计对重点平台企业开展行政指导 300 余次、行政检查 160 余次。聚焦杭州亚运会亚残运会等重要时间节点，针对仿冒亚运网站、泄露志愿者个人信息等违法违规行为采取行政处置处罚措施560 余家(次)，对于初次违法、情节轻微且无主观过错、及时改正的新生企业，分类采取行政约谈、行政告诫等柔性执法方式。

三是提效能，聚焦重点领域开展执法专项行动，不断优化营商网络环境。浙江网信部门聚焦省委营商环境优化提升“一号改革工程”，集中开展“浙E执法”专项行动，全年巡查综合生活信息门户、新闻信息、电商、直播等类别 320 余家网站平台 3000 余万个页面，依法依规处置网站平台 30

余家（次），查处违法违规信息 130 余条，助力企业规范健康发展。（来源：网信浙江）

2. 上海市网信办公布 2023 年执法工作成效

2 月 1 日，上海市网信办公布 2023 年执法工作成效。据统计，市区两级网信部门共办理各类网络执法案件 842 件，关闭违规账号 504 个，会同本市通信管理部门关停网站 164 家。

依法打击违反网络信息安全的违法违规行为。依法从严从快查处发布传播涉政涉意识形态有害信息的网站平台，相关案件在行政处罚类案件中占比 52.2%，对多家企业依据《网络安全法》顶格罚款 50 万元。结合开展“清朗”系列专项行动，针对严重扰乱网络传播秩序、未经许可开展新闻信息服务的违法违规行为，对“上海网”、“七叔东山再起”等一批“自媒体”予以立案处罚。针对发布破坏网络生态、危害未成年人身心健康信息内容的违法违规行为，依法关闭“天天吉历”、“小蜜蜂”、“幽谷”等一批网站平台，对平台传播诱导未成年人接触医疗美容、诱导自杀自残等有害信息案件进行查处，指导属地短视频、生活服务类、社交类、电商类网站平台持续提高对生态不良信息的审核把关能力，为未成年人提供安全、健康的网络环境。上海网信办会同市检察院、市文旅局执法总队制定发布了《侵害未成年人身心健康的网络信息执法指南》《未成年人网络保护风险识别清单》，并联合公布一批行政执法、法律监督警示案例，为互联网企业合规发展提出明确的指导意见，督促属地各平台结合实际采取有效工作举措，建立长效治理机制。要求本地应用商店下架各类违法违规移动应用程序 234 个，包括存在色情低俗信息的“星火直播”“桃花直播”等APP。

开展“亮剑浦江”专项行动。围绕消费领域个人信息被“过度采、强制要、诱导取、违规用”等问题，聚焦扫码点餐、扫码停车、房产中介等八类重点场景，组织开展为期半年的“亮剑浦江”专项执法行动。期间，会同市场监管部门累计检查企业6043家，约谈企业520余家，查处各类个人信息保护案件50余件。联合市商委等行业主管部门组织8场普法培训，涉及餐饮、少儿培训、大型商超等57000余家连锁门店和机构。

在网络和数据安全、个人信息保护领域持续加大执法力度。依法打击危害网络运行安全、数据安全、侵害公民个人信息权益等新型领域违法违规行为。依据《数据安全法》对数据涉嫌泄露到境外的多家企业进行处罚，对其中擅自删除数据库的一家企业和直接责任人员进行“一案双罚”。依据《个人信息保护法》对一批怠于履行个人信息保护义务的知名企业进行处罚，是地方网信办自主办理的首批系列行政处罚案件。办理一批算法治理类典型案件，针对部分大型平台存在的推送正能量不足、无法删除针对个人特征的用户标签等问题，依法立案处罚，督促企业完善算法治理机制。（来源：网信上海）

3. 因误导消费者“入会”索要手机号，上海市网信办约谈餐饮连锁企业“半天妖烤鱼”

2月2日，上海市网信办依法约谈“半天妖烤鱼”运营企业上海半天妖餐饮管理有限公司负责人。

根据网民举报并经核实，“半天妖烤鱼”在消费者扫码点餐过程中，微信小程序存在误导消费者认为必须先注册会员才能点餐、索取非必要的手机号且首次使用未主动弹窗告知消费者收集使用个人信息规则等违法违规行为。上海市网信办要求企业立即整改，对照问题举一反三自查自纠，

切实把个人信息保护置于企业运营的重要位置。企业负责人表示，将认真落实网信部门要求，开展全面自查整改，以实际行动维护消费者个人信息权益。

上海网信办表示，2023 年“亮剑浦江”消费领域个人信息权益保护专项行动中，其会同市场监管部门围绕“扫码点餐”场景下企业过度收集消费者个人信息问题开展集中整治。55000 余家全国连锁餐饮门店已完成自查整改，但仍有个别企业置若罔闻、心存侥幸，怠于履行个人信息保护义务。

上海市网信办相关负责人指出，“扫码点餐”等小微消费场景不能成为个人信息保护死角，消费者在到店点餐非注册会员情况下无需提供任何个人消息。部分餐饮企业在点餐小程序中设置强制或诱导消费者关注公众号、注册会员，以及收集消费者非必要个人信息等行为，违反《个人信息保护法》规定的“合法、正当、必要和诚信原则”，侵犯消费者的知情权与自主选择权。上海市餐饮经营者要按照网信部门指导市消保委会同市餐饮烹饪行业协会制定发布的《上海市网络点餐服务消费者个人信息保护合规指引》要求，在收集、使用、保管消费者个人信息的各个环节提高合规意识和保护水平。全国连锁门店超过 100 家的大型餐饮企业尤其要做出行业表率。（来源：网信上海）

4. 因存在系统漏洞和弱口令，重庆市涪陵区网信办依法约谈某区级行业主管部门及行业相关单位

2 月 3 日消息，因 2023 年以来某行业领域多家单位被通报存在系统漏洞和弱口令问题，重庆市涪陵区网信办依据《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，对某区级行业主管部门及行业相关单位进行集中约谈。

涪陵区网信办通报该行业网络安全风险漏洞情况，要求该部门和相关单位严格落实网络安全指导监管责任和主体责任，健全完善领导责任体系，全面普查行业领域网络资产，加强网络安全防护，开展风险漏洞自查整改，主动上报发现问题。该部门表示，将认真履行行业监管责任，加强对本单位本行业网络安全督导，全面排查弱口令、未授权访问及其他高危系统漏洞，限期整改到位。（来源：网信重庆）

5. 因存在弱口令漏洞，重庆市高新区网信办联合多部门约谈属地某公司负责人

2 月 4 日消息，重庆市高新区网信办联合改革发展局、综合执法局、高新区公安分局依法对属地某公司负责人进行约谈。

接市网信办移交线索，该公司的选料台系统及其子公司的后台管理系统在短期内连续被通报弱口令漏洞。根据《网络安全法》等法律法规，重庆高新区网信办责成该公司严格落实网络安全主体责任，切实抓好自查，定期开展安全培训，持续加大安全投入。高新区公安分局现场出具限期整改通知书，要求该公司从问题产生原因、处置过程、整改情况、验证通过情况、涉及业务系统情况、全网排查情况、网络安全防护情况等 7 方面做好排查整改并按时反馈。（来源：网信重庆）

6. 因连续出现网站网页被篡改等网络安全问题，重庆市北碚区网信办依法约谈某区级部门

2 月 6 日消息，重庆市北碚区网信办工作发现北碚某区级部门连续出现网站网页被篡改等网络安全问题。北碚区网信办依据《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，对相关负责同志

进行约谈。北碚区网信办通报网站被篡改网页的情况，要求相关单位提高网络安全意识，严格落实网络安全主体责任，切实加强网络安全防护。被约谈部门负责人表示，将吸取教训、举一反三，全面开展自查排查，网络安全问题在限期内整改到位。（来源：网信重庆）

7. 因多家单位存在弱口令漏洞问题，重庆市秀山县网信办依法约谈某行业单位

2月7日消息，重庆市秀山县网信办接市网信办移交线索以及秀山网信办日常排查发现，秀山县图书馆、县禹通公司、西街旅游景区等单位存在弱口令漏洞问题。秀山县网信办依据《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，对该行业主管部门及行业相关单位进行集中约谈。

秀山县网信办通报该行业网络安全风险漏洞情况，下发整改通知书，要求该部门和相关单位严格落实网络安全指导监管责任和主体责任，从问题产生的原因、处置过程、整改情况、验证通过情况、涉及业务系统情况、全网排查情况、网络安全防护情况等方面做好排查整改并按时反馈。该部门表示，将认真履行行业监管责任，加强对本单位本行业网络安全督导，确保整改到位。（来源：网信重庆）

8. 因未履行网络安全保护义务等，江西省南昌市网信办对属地某连锁超市作出行政处罚

2月28日消息，江西省南昌市网信办近日在日常网络安全监测中发现，属地某连锁超市所属IP疑似被黑客远控，频繁对外发起网络爆破攻击。

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：（一）该连锁超市未履行网络安全保护义务，未对运营的网络及信息系统开展网络安全等级保护测评等相关工作，所属的服务器和多台终端感染木马病毒；（二）该连锁超市未及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，所属网络持续对内对外发起大规模网络攻击，导致产生危害网络安全的后果。相关行为违反《网络安全法》第二十一条、第二十五条的规定。

2 月 19 日，南昌市网信办依据《网络安全法》第五十九条的规定，对该连锁超市作出罚款 5 万元、对直接负责的主管人员作出罚款 1 万元的行政处罚。（来源：网信南昌）

（三）通信管理部门治理实践

1. 多地通信管理局提示：4 月 1 日起未备案 App 将下架关停

2 月，湖北、内蒙古、河北、广东、陕西通信管理局相继发布通知，明确自 4 月 1 日起，对逾期未履行备案手续的境内存量移动互联网应用程序（含 APP、小程序、快应用等），将按照《反电信网络诈骗法》《互联网信息服务管理办法》等法律法规要求，依法采取下架、关停等处理措施，网络接入服务提供者、应用分发平台、智能终端生产企业应全面落实“先备案后服务”要求，不得为未备案 APP 提供网络接入、分发、预置等服务，保障互联网行业规范健康发展，维护网络安全和公众利益。

根据 2023 年 8 月 4 日工信部印发的《工业和信息化部关于开展移动互联网应用程序备案工作的通知》，2023 年 9 月至 2024 年 3 月为存量 App 备案阶段，已开展业务的 App 应按照通知要求，通过其网络接入服务提供者、

分发平台向其住所所在地省级通信管理局履行备案手续。（来源：湖北、内蒙古、河北等省通管局）

2. 多地通信管理局通报问题 App

（1）湖北省通信管理局

2 月 21 日，湖北省通信管理局发布侵害用户权益行为 App 的通报（2024 年第一批）。

湖北省通信管理局近期组织第三方检测机构对本省 APP 应用侵害用户权益行为开展检查。经检测发现 35 款 APP 存在违规收集个人信息、超范围收集个人信息、强制用户使用定向推送功能等相关问题，湖北省通信管理局对相关违规单位发出《整改通知》，责令 APP 运营者限期完成整改。截至目前，尚有 4 款 APP 未按期完成整改。涉及被通报的 APP 运营者，可在 2 月 27 日前就有关问题向湖北省通信管理局提交书面说明；逾期未提交或理由不充分的，湖北省通信管理局将依法依规组织开展相关处置工作。

（2）浙江省通信管理局

2 月 26 日，浙江省通信管理局通报 12 款侵害用户权益行为的 APP（2024 年第 1 批）。

近期，浙江省通信管理局组织第三方检测机构对群众关注的即时通信、实用工具、学习教育等类型 APP 进行检查，发现部分 APP 存在违规收集个人信息、超范围收集个人信息、强制频繁过度索取权限等问题，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 12 款 APP 未按要求完成整改，现予以通报。相关 APP 开发运营者应在 3 月 6 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。

（3）北京市通信管理局

2 月 29 日，北京市通信管理局通报问题 APP（2024 年第二期）。近期，北京市通信管理局通过抽测发现北京市部分 APP 存在违反必要原则收集个人信息、未明示收集使用个人信息的目的、方式和范围等侵害用户权益和安全隐患类问题。截至目前，尚有 10 款 APP 未整改或整改不到位，予以公开通报。

此外，通报指出，2024 年 1 月 29 日，北京市通信管理局通报了存在侵害用户权益行为的 APP 并要求整改。截至目前，仍有 9 款 APP 未整改或整改不到位，现予以全网下架处置。

（4）重庆市通信管理局

2 月 29 日，重庆市通信管理局官网通报川渝两地侵害用户权益 APP 名单（2024 年第二期）。

近期，重庆市通信管理局和四川省通信管理局组织第三方检测机构对川渝两地主流应用商店移动互联网应用程序(APP)进行检查。发现部分 APP 存在违规收集个人信息，违反必要原则收集与其提供的服务无关的个人信息，未明示个人信息处理规则，隐私政策中未对处理的个人信息保存期限加以说明，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。截至目前，仍有 14 款 APP 未按要求完成整改。相关 APP 应在 2024 年 3 月 8 日前完成整改落实工作。逾期不整改的，将依法依规进行处置。（来源：湖北、浙江、北京、重庆市通管局）

3. 上海市通信管理局：已建立本市首批电信领域重要数据目录

2 月 1 日，上海市通信管理局组织召开“浦江护航”数据安全专项行动落实情况专题通报会，就专项行动中发现的主要问题以及相关企业的数据安全风险评估责任落实情况，对 14 家企业进行约谈通报。

自 2023 年 3 月“浦江护航”数据安全专项行动启动以来，上海市通信管理局以试点实施首席数据官制度、开展重要数据和核心数据识别认定及备案、开展数据安全评估管理、开展数据安全监测预警与通报处置、加强数据全生命周期安全管理、加强数据安全能力建设和能力培养等六项重点任务为牵引，组织本市头部电信和互联网企业加快落实数据安全保护义务，提升数据安全防护水平。截至 2024 年 2 月 1 日，上海市通信管理局已审核公示 97 家电信和互联网企业的首席数据官备案信息，组织 102 家企业开展重要数据认定和数据安全风险评估工作，建立本市首批电信领域重要数据目录，并指导企业按照工业和信息化部“数安护航”专项和属地“浦江护航”专项要求，积极落实数据保护责任，有效防范数据安全风险。（来源：上海通信圈）

（四）其他部门治理实践

1. 国家数据局等四部门联合开展全国数据资源调查

2 月 7 日，国家数据局、中央网络安全和信息化委员会办公室、工信部、公安部联合发布通知，开展全国数据资源情况调查，调研各单位数据资源生产存储、流通交易、开发利用、安全等情况，为相关政策制定、试点示范等工作提供数据支持。

通知明确调查对象包括：（1）省级数据管理机构、工业和信息化主管部门、公安厅（局）；（2）各省重点数据采集和存储设备商、消费互联网平台和工业互联网平台企业、大数据和人工智能技术企业、应用企业、数据交易所、国家实验室等单位；（3）中央企业；（4）行业协会商会；（5）国家信息中心。调查对象需通过全国数据资源调查管理平台，填写相关调查表。（来源：国家数据局）

2. 多地成立省级数据局

（1）陕西省

2 月 3 日，陕西省人民政府决定，任命刘晓军为陕西省数据和政务服务局局长。

（2）新疆生产建设兵团

2 月 3 日，新疆生产建设兵团数据局揭牌成立。揭牌仪式上有关领导要求，各级各部门要提高政治站位，从政治和全局的高度认识加快数字化发展在推进中国式现代化兵团实践中的重大战略意义。深入贯彻落实习近平总书记、党中央关于数字化改革工作决策部署，加快数字政府改革建设，大力发展数字经济，努力建设数字兵团，坚定不移把兵团党委、兵团的决策部署落地见效。要强化顶层设计，着力开创新时代兵团数字化发展工作新局面；要统筹发展和安全，加强网络和数据监管，构建数字兵团全方位安全保障体系；要加强组织领导，坚持整体谋划、统筹推进，确保形成一体推进的工作合力；要加快思想融合、职能融合、业务融合，不断提升运

用数字化手段赋能各项工作的能力，推动兵团数字化改革工作取得实实在在成效。

（3）西藏自治区

2月6日,西藏自治区数据管理局在拉萨正式挂牌。自治区管理局表示，将深入贯彻党中央、国务院关于数字化改革重大决策，全面落实区党委、政府关于数据管理工作要求，立足西藏实际，进一步理顺数据发展管理体制和运行机制，建立健全数据基础制度和标准，深化数智融合应用，推动数字西藏、数字经济、绿色算力等高质量发展，加快发展新质生产力，充分发挥数据管理局统筹协调和组织实施作用，抓顶层设计协同，抓战略落实协同，抓政策效果协同，在政策制定上相互配合，在实施过程上相互促进，在工作成效上相得益彰，朝着不断做强做优做大自治区数字经济聚焦发力。

（4）江西省

2月8日，江西省数据局揭牌仪式在南昌举行。揭牌仪式上有关领导要求，要自觉把思想和认识统一到党中央、国务院决策部署上来，认真落实省委和省政府工作要求，全力抢抓“数据”机遇，以“数据”赋能经济高质量发展、社会高效能治理、人民高品质生活；要知责尽责，充分发挥宏观统筹和综合协调能力，全面推进数据资源整合共享和开发利用，协调推动数字江西、数字经济、数字社会的规划和建设，持续提升数字江西建设的整体性、系统性、协同性。（来源：陕西省人民政府、人民网、西藏自治区经济和信息化厅、江西省发展和改革委员会）

3. 最高检：当前网络犯罪呈多发高发态势

2 月 23 日，最高人民检察院召开“依法惩治网络犯罪 助力网络空间综合治理”发布会，通报工作情况。

通报指出，网络犯罪不断滋生蔓延，网络诈骗、网络暴力、侵犯公民个人信息等犯罪升级演变。总的看，当前网络犯罪呈多发高发态势。2023 年 1 至 11 月，检察机关共起诉各类网络犯罪 28 万人，同比上升 35.5%，占全部刑事犯罪的 18.8%。

网络犯罪呈现如下趋势特点：一是电信网络诈骗及其关联犯罪大幅增多；二是与新技术新业态相伴生，黑灰产业加速迭代升级；三是传统犯罪向网络空间迁移，网络犯罪样态日趋复杂；四是威胁数据信息安全类犯罪常见多发，危害数字经济健康发展。

发布会同步发布八起典型案例，包括黄某某侵犯公民个人信息案——利用网络非法买卖他人实名微信号；吕某某非法控制计算机信息系统案——离职人员远程登录科技公司服务器删除数据等案件。（来源：最高人民检察院）

4. 最高检印发第五十批指导性案例，含一起利用网络侵犯公民个人信息案

2 月 22 日，最高人民检察院印发第五十批指导性案例，其中包括一起康某某利用网络侵犯公民个人信息案。

本案中，被告人康某某系某网络科技公司法定代表人。2022 年 12 月至 2023 年 2 月，康某某以网络科技公司兼职为名招聘刘某某等人（另案处理）帮助其收购电话卡。刘某某系某学院学生，通过微信朋友圈发布兼职招聘信息，招募到 40 多名在校学生，其中未成年人 21 人。在康某某安排下，

刘某某等人到指定网点办理电话卡577张，人均办卡14张。康某某将电话卡出售给上游犯罪行为人，用于注册各类社交APP账号，提供有偿引流、点赞服务。部分电话卡在康某某不知情的情况下，被上游犯罪行为人用于实施电信网络诈骗犯罪。

2023年2月10日，内蒙古自治区某市公安局某区分局以侵犯公民个人信息罪对康某某立案侦查。2023年8月3日，内蒙古自治区某市某区人民检察院对康某某提起公诉。康某某被人民法院以侵犯公民个人信息罪判处刑罚。（来源：最高人民检察院）

5. 财政部：推动数据资产开发利用，鼓励依法依规推进公共数据资产有效供给

2月1日，国家新闻办公室就2023年全年财政收支情况举行发布会。财政部资产管理司司长表示，在加强数据资产管理、推动数字经济发展方面，下一步，财政部将重点推进三方面工作：

一是加强数据资产全流程管理。规范数据资产的登记、存储、使用、披露、处置等环节，构建起清晰、完整的数据资产管理路径，有序推进数据资产化，更好发挥数据资产的经济价值和社会价值。

二是推动数据资产开发利用。鼓励依法依规推进公共数据资产有效供给，加大数据资产信息的公开和披露力度，提高数据资产流转透明度。支持在金融、交通、医疗、能源等数据富集行业，探索多样化的开发利用模式。建立合理的收益分配机制，充分调动各参与方的积极性。

三是确保数据资产合规安全使用。推动加强对数据资产的监测监督，用好先进技术，严格防范数据资产泄露、损毁、丢失等管理风险。同时，

在数据资产评估、交易等环节，设置合理的程序，严防虚增数据资产价值。（来源：央视网）

境外前沿观察：月度速览十则

导读：2 月，美国总统拜登签署《关于防止受关注国家访问美国公民的大量敏感个人数据和美国政府数据的行政令》，限制向中国、俄罗斯、伊朗、朝鲜、古巴和委内瑞拉等受关注国家传输美国公民的敏感个人数据，包括基因组数据、生物识别数据、个人健康数据、地理位置数据、财务数据和特定类型的个人身份识别信息。美国白宫发布公告《总统关于解决美国汽车行业国家安全风险的声明》，以存在潜在国家安全风险为由指示商务部调查来自包括中国在内的受关注国家的联网车辆。克罗地亚《网络安全法》施行，明确“网络安全关键和重要实体”的认定条件，并要求采取与所识别的风险相称的网络安全风险管理措施。日本公布《负责任的人工智能促进基本法案（暂定）》，聚焦于具有特别重大社会影响的类 GPT 先进人工智能模型，要求开发者履行第三方漏洞检测和报告、模型基本信息披露、社会风险研究等安全义务。

马拉维移民局因网络攻击暂停护照服务，政府拒绝“安抚犯罪分子”或“与攻击政府的人进行谈判”。加拿大皇家骑警网站遭受网络攻击，在 2 月 25 日关闭，并显示 HTTP 404 错误消息。

关键词：数据获取出口管制、海事网络安全、智能网联汽车国家安全审查、网络安全关键和重要实体风险管控、政务网络攻击

1. 美国白宫发布行政令，加强港口、船舶、海滨设施网络安全保护

2 月 21 日，美国总统拜登签署《关于修订保护美国船舶、港口和海滨设施相关法规的行政令》，强化海事领域网络安全防御。

行政令赋予海岸警卫队应对网络安全事件的 7 项权限，包括：（1）在必要时阻止任何人员、物品或事物（包括数据、信息、网络、程序、系统或其他数字基础设施）登上、被带上或放置在船只上，或进入、被带入或放置在海滨设施之上或其中；（2）建立安全区并限制人员或船舶进入安全区，限制人员在安全区内的任何船舶、海滨设施上登上、取走或放置任何物品；（3）在美国管辖范围内检查和搜查任何船舶、海滨设施或安全区；（4）必要时在管辖下的美国领海内监督和控制任何船只的移动，并完全或部分占有或控制任何船只或其任何部分；（5）签发或撤销海岸警卫队港口安全卡；（6）规定与海滨设施和港口船舶安全有关的条件和限制，相关条件和限制可扩大，且不限于此类船舶和海滨设施的检查、操作、维护、守卫、配备以及防火措施；（7）必要时阻止任何船舶停泊在码头、船坞、桥墩或其他海滨设施上，或强制该船舶从任何此类码头、船坞、桥墩或其他海滨设施上转移。（来源：美国白宫）

2. 美国白宫发布行政令，限制向中国传输特定类型数据

2 月 28 日，美国总统拜登签署《关于防止受关注国家访问美国公民的大量敏感个人数据和美国政府数据的行政令》，限制向中国、俄罗斯、伊朗、朝鲜、古巴和委内瑞拉等受关注国家传输美国公民的敏感个人数据，

包括基因组数据、生物识别数据、个人健康数据、地理位置数据、财务数据和特定类型的个人身份识别信息。

行政令要求：（1）司法部发布新规，限制受关注国家对于美国公民敏感个人数据的访问和利用，阻止敏感个人数据大规模转移到这些国家；（2）司法部发布新规，加强对敏感政府数据的保护，包括敏感政府场所的地理位置信息和军事人员的信息；（3）司法部和国土安全部共同制定高安全标准，防止受关注国家通过其他商业手段获取美国公民的信息，如通过投资、供应商和雇佣关系；（4）卫生与公共服务部、国防部和退伍军人事务部确保联邦拨款、合同、奖励不被用于帮助受关注国家（包括通过位于美国的公司）获取美国公民的敏感健康数据；（5）美国电信服务行业外国参与评估委员会在审查海底电缆许可证时考虑对美国公民敏感个人数据的威胁等。（来源：美国白宫）

3. 美国拟对内嵌中国信息通信技术或服务的智能网联汽车启动国家安全审查

2 月 29 日，美国白宫发布公告《拜登总统关于解决美国汽车行业国家安全风险的声明》，以存在潜在的国家安全风险为由指示商务部调查来自包括中国在内的受关注国家的联网车辆，并采取行动应对此等风险。

同日，美国商务部工业与安全局（BIS）发布拟议规则预通知《确保信息和通信技术与服务供应链安全：联网车辆》，旨在就联网车辆涉及的信息通信技术和服务交易问题征求公众意见。通知内容包括：（1）关键术语定义；（2）联网车辆相关交易如何对美国国家安全构成不适当或不可接受的风险；（3）通过发布禁令或采取可行的缓解措施应对相关风险的实施机

制；（4）考虑是否需要为公众建立一项程序，通过证明特定交易中对美国国家安全构成的风险是否已得到充分缓解，从而申请批准参与原本被禁止的交易。（来源：美国白宫、美国BIS）

4. 克罗地亚《网络安全法》施行，强化网络安全关键和重要实体风险管控

2月15日，克罗地亚《网络安全法》施行，该法将欧盟NIS 2指令转化为国家法律，推动落实网络安全保护措施，明确“网络安全关键和重要实体”认定条件。

认定条件包括：（1）实体是维持关键社会活动或经济活动所必需的网络服务提供商；（2）实体提供的网络服务中断或实体活动运转中断可能对公共安全、公共利益或公共健康产生重大影响；（3）实体提供的网络服务中断或实体活动运转中断可能对特定行业造成重大系统性风险；（4）实体在国家、地区或地方层面对特定行业、服务或其他相互依存的行业具有特殊重要性。该法规定，网络安全关键和重要实体应当采取网络安全风险管理措施，确保网络和信息系统安全水平与所识别的风险相称。（来源：克罗地亚议会）

5. 日本公布《负责任的人工智能促进基本法案（暂定）》

2月16日，日本公布《负责任的人工智能促进基本法案（暂定）》，聚焦于具有特别重大社会影响的类GPT先进人工智能模型，要求开发者遵守一系列安全开发义务，包括对系统进行内外部安全验证、风险信息共享、网络安全投资、第三方漏洞检测和报告、模型基本信息披露、社会风险研

究等。其中，第三方漏洞验证、模型基本信息披露等义务的内容与2023年白宫宣布的七家头部生成式人工智能公司的自愿承诺基本一致。法案要求先进人工智能模型开发者定期向政府或第三方（如人工智能安全研究所）报告系统开发合规状况，政府应定期审查并在必要时公开，提供指导和监督。（来源：日本众议院）

6. 欧盟就《选举过程中超大型在线平台和超大型在线搜索引擎提供者应遵循的系统性风险缓解指南（草案）》公开征求意见

2月9日，欧盟就《选举过程中超大型在线平台和超大型在线搜索引擎提供者应遵循的系统性风险缓解指南（草案）》公开征求意见。指南是《数字服务法》（DSA）第35条规定下首个指导性文件，针对Facebook、谷歌、TikTok和X等超大型在线平台和超大型在线搜索引擎的服务提供者提供最佳实践指引，以减轻选举安全风险，要点包括：（1）通过横幅、弹出窗口、搜索干预、选举网站链接等方式向用户提供有关选举进程的官方信息，包括有关选举进程、如何投票的信息，显示的信息应当始终来自成员国选举当局；（2）共同推动、投资并参与以选举为重点的公众媒体素养提升措施和活动，培养公众的批判性思维并帮助改进所需的技能，如分析复杂的现实、认识到社交媒体观点与事实之间的差异以及生成人工智能相关风险；（3）提供事实核查标签、提示并敦促用户在分享内容前评估信息的准确性和来源、提供清晰可见的已验证账户等。（来源：欧盟委员会）

7. 全球多家科技企业签署协议，承诺打击滥用人工智能干扰 2024 年选举

2 月 16 日,Adobe、Meta、IBM、OpenAI、Microsoft、TikTok、X、LinkedIn、亚马逊、谷歌等全球多家科技企业在第 60 届慕尼黑安全会议上签署《打击在 2024 年选举中欺骗性使用人工智能技术的协议》，承诺在 2024 年打击干扰选举的人工智能滥用行为，通过技术部署减少利用人工智能生成和分发欺骗性内容干扰选举的风险。与会企业同意 8 项具体承诺：（1）开发和实施技术以降低与欺骗性人工智能选举内容相关的风险；（2）评估协议范围内的模型，了解它们可能带来的有关欺骗性人工智能选举内容的风险；（3）检测欺骗性人工智能选举内容在其平台上的发布情况；（4）寻求适当解决在其平台上检测到的欺骗性人工智能选举内容；（5）培养跨行业对欺骗性人工智能选举内容的韧性；（6）向公众提供有关公司如何解决欺骗性人工智能选举内容风险的透明度；（7）继续与各种全球民间社会组织、学术界接触；（8）增强公众意识，加强媒体素养和全社会复原力。（来源：Microsoft 官网）

8. 因网络攻击，马拉维移民局暂停护照服务

2 月 24 日消息，由于移民局计算机网络遭到勒索软件攻击，马拉维政府在过去两周暂停发放护照。马拉维总统表示，黑客索要赎金，但马拉维政府无意支付赎金，政府拒绝“安抚犯罪分子”或“与攻击政府的人进行谈判”；预计移民部门将在三周期限内找到临时解决方案，以恢复护照签发活动；国家计划制定一项长期解决方案，通过额外安全措施强化重要系

统防护。目前马拉维政府尚未披露攻击的幕后黑手以及数据是否被盗等信息。（来源：Dark Reading Logo）

9. 2024 年以来已有约 5 亿条俄罗斯人记录被泄露

2 月 24 日消息，据俄罗斯联邦通信、信息技术和大众媒体监督局（Roskomnadzor）记录，自 2024 年初以来，已有 19 起个人数据泄露事件发生，导致超过 5.1 亿条有关俄罗斯人的记录被泄露到网络中。Roskomnadzor 表示，有一起泄露事件尤其突出，5 亿用户数据被泄露，目前此案正在调查中。相比之下，2023 年登记的泄露记录约为 3 亿；2022 年特别军事行动开始后，登记的泄露记录为 6 亿。（来源：Roskomnadzor 官网）

10. 加拿大皇家骑警遭受网络攻击

2 月 25 日，加拿大皇家骑警网站关闭，并显示 HTTP 404 错误消息，对 www.rcmp-grc.gc.ca 的请求被重定向到一个不存在的 install.php 页面。警方已对这起网络攻击事件展开调查，并敦促工作人员保持警惕。加拿大皇家骑警已将本次网络攻击事件通知加拿大隐私专员办公室。（来源：BleepingComputer）

行业前沿观察一：中央网信办部署开展 2024 年“清朗”系列专项行动、中央网信办等 11 部门联合印发《关于开展第二批国家数字乡村试点工作的通知》、国安部解读网络安全法亮点、2023“安满周”4 月中旬全国线上线下同步举办

近日，中央网信办部署开展 2024 年“清朗”系列专项行动。2024 年“清朗”系列专项行动将紧紧围绕人民群众的新期待新要求，全面覆盖网上重点领域环节，着力研究破解网络生态新问题新风险，重点开展 10 项整治任务。

为贯彻落实党中央、国务院关于推进乡村全面振兴的决策部署，深入实施数字乡村发展行动，中央网信办、农业农村部、国家发展改革委、工业和信息化部、民政部、生态环境部、商务部、文化和旅游部、中国人民银行、市场监管总局、国家数据局印发《关于开展第二批国家数字乡村试点工作的通知》，部署开展第二批国家数字乡村试点工作。《通知》指出，要按照推进乡村全面振兴、加快建设农业强国的部署要求，以学习运用“千万工程”经验为引领，以信息化驱动农业农村现代化为主线，探索形成数字乡村可持续发展模式，不断增强乡村振兴内生动力。

《中华人民共和国网络安全法》于 2016 年 11 月 7 日发布，自 2017 年

6 月 1 日起施行，是我国第一部全面规范网络空间安全管理方面的基础性法律。微信公众号“国家安全部”发文解读《网络安全法》的四大亮点。

为深入学习贯彻 2024 全国两会精神，落实习近平总书记关于网络强国的重要思想和一系列讲话精神，不断汇聚社会各方力量，加快发展新质生产力，助力推进高质量发展。 2023 网民网络安全感满意度调查报告发布周（简称“安满周”）将于 4 月中旬全国线上线下同步举办。本届安满周以“网络安全为人民，网络安全靠人民”为主题。

1. 中央网信办部署开展 2024 年“清朗”系列专项行动

近年来，中央网信办坚持以清朗网络空间为目标，以人民根本利益为出发点和落脚点，持续开展“清朗”系列专项行动，集中整治网上突出问题乱象，推动网络生态持续向好。2024 年“清朗”系列专项行动将紧紧围绕人民群众的新期待新要求，全面覆盖网上重点领域环节，着力研究破解网络生态新问题新风险，重点开展 10 项整治任务。

（1）.“清朗• 2024 年春节网络环境整治”专项行动。春节期间，集中整治 6 方面问题乱象：发布误导性旅游攻略、自导自演有违公序良俗的离奇剧情视频；借热点话题挑起互撕谩骂、煽动群体对立；利用年终盘点、返乡见闻等形式编造不实内容；发布涉色情、赌博、网络水军等违法引流信息；鼓吹炫富拜金、诱导粉丝无底线追星；危害未成年人身心健康等，为广大网民营造积极向上、文明健康的春节网上氛围。

（2）.“清朗• 优化营商网络环境—整治涉企侵权信息乱象”专项行动。重点整治散布传播涉企虚假不实信息，蓄意造谣抹黑企业、企业家，以“舆论监督”名义对企业进行敲诈勒索等问题。督促网站平台加强涉企信息审核管理，及时提醒有关账号主体严格遵守落实法律法规、社区规则和专项行动要求。依法处置问题突出、情节严重的网站平台和账号。

（3）.“清朗• 打击违法信息外链”专项行动。坚决打击利用各种“暗号”“套路”发布非法外链，严防通过将用户引流到隐蔽环节或境外网站等形式，发布传输色情、赌博、网络水军等违法信息。督促网站平台持续加大对图形化、符号化等各类引流变形体的识别打击力度，开展跨平台联动，排查处置引流信息指向的黑灰产群组、账号、APP，违法犯罪线索及时移交公安机关。

（4）.“清朗• 整治‘自媒体’无底线博流量”专项行动。集中整治“自媒体”造热点蹭热点制造“信息陷阱”、无底线吸粉引流牟利等问题。督促网站平台做好涉国内外时事、公共政策、社会事件等领域信息来源标注，AI 生成信息标注以及虚构摆拍内容标注。严格营利权限开通条件，明确审核、认定及处置标准。优化流量分发机制，有效扩大优质信息内容触达范围。

（5）.“清朗• 网络直播领域虚假和低俗乱象整治”专项行动。重点整治 7 方面突出问题：通过摆拍场景等方式，制作“扮穷”“卖惨”内容博眼球；通过渲染商品“功效”等方式，在直播带货中进行虚假宣传；虚构直播“相亲”嘉宾身份，炒作婚恋话题；主播刻意展示发布“软色情”内容；通过深夜付费直播躲避监管，隐蔽传播低俗色情信息；直播低俗搭讪，实施恶俗 PK 行为，无底线挑战公众审美；在直播时传播虚假科普信息，混淆视听。

（6）.“清朗• 规范生成合成内容标识”专项行动。落实《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》相关要求，督促生成合成服务提供者、网络信息内容服务平台落实主体责任，规范开展生成合成内容标识，清理未有效标识、易造成公众混淆误认的生成合成信息内容，处置利用生成合成技术制造谣言、营销炒作的违规账号。

（7）.“清朗• 2024 年暑期未成年人网络环境整治”专项行动。贯彻落实《未成年人网络保护条例》相关要求，从人民群众反映强烈的突出问题入手，集中整治在首页首屏、弹窗、热搜等醒目位置呈现涉未成年人不良内容，以手办文具、动漫二创等方式变相发布低俗色情内容，利用密聊软件、加密照片等方式实施网络欺凌、隔空猥亵等突出问题，严管儿童智

能设备信息内容安全，防范未成年人网络沉迷，对问题突出平台、机构和账号从严采取处置处罚措施。

（8）.“清朗• 规范网络语言文字使用”专项行动。重点整治通过故意使用错字、滥用谐音指代词、编造黑话烂梗、恶意曲解文字含义等方式，传播低俗色情、攻击恶搞、煽动对立等违法不良信息问题。督促短视频、智能编辑工具等平台，优化错别字提示功能，协助用户规范使用语言文字。督促网站平台进一步畅通举报受理渠道，鼓励网民广泛参与，及时处置不规范使用语言文字的违法不良信息。

（9）.“清朗• 整治违规开展互联网新闻信息服务”专项行动。集中整治未经批准或超范围提供互联网新闻信息服务，倒卖、出租、出借互联网新闻信息服务许可证，发布传播虚假不实新闻信息等问题。指导督促互联网新闻信息服务单位加强内部管理，提高服务质量，依法依规提供互联网新闻信息服务。压实重点网站平台和应用程序分发平台主体责任，加强对使用“新闻”“报道”等具有新闻属性表述的账号、应用程序的资质审核，从严处置违法违规主体。

（10）.“清朗• 同城版块信息内容问题整治”专项行动。重点整治低俗不良营销、网络水军、网络谣言和虚假信息、网络戾气等同城版块多发易发问题。督促网站平台强化日常巡查管理，及时处置违规账号主体，优化信息内容推荐机制，严防根据用户地理位置和兴趣爱好扎堆推送违法不良信息，切实净化同城版块网络生态环境。

中央网信办相关部门负责人表示，将按照工作计划安排，有力有序推进2024年“清朗”系列专项行动，确保整治工作取得扎实成效，为广大网民营造文明健康的网络环境。

（来源：中国网信网）

2. 中央网信办等 11 部门联合印发《关于开展第二批国家数字乡村试点工作的通知》

近日，为贯彻落实党中央、国务院关于推进乡村全面振兴的决策部署，深入实施数字乡村发展行动，中央网信办、农业农村部、国家发展改革委、工业和信息化部、民政部、生态环境部、商务部、文化和旅游部、中国人民银行、市场监管总局、国家数据局印发《关于开展第二批国家数字乡村试点工作的通知》，部署开展第二批国家数字乡村试点工作。

《通知》指出，要按照推进乡村全面振兴、加快建设农业强国的部署要求，以学习运用“千万工程”经验为引领，以信息化驱动农业农村现代化为主线，探索形成数字乡村可持续发展模式，不断增强乡村振兴内生动力。

《通知》要求，要加强领导、统筹推进，建立健全跨部门协调机制和跨层级联动机制，做好数字乡村建设整体规划设计，整合用好相关支持政策和现有资源，以责任落实推动工作落实、政策落实。要政府引导、多方参与，充分发挥市场机制作用，更好发挥政府作用，培育数字乡村发展良好生态，以信息流带动技术流、资金流、人才流，探索形成社会多元共建新局面。要问题导向、创新驱动，围绕农民最关心最直接最现实的利益问题，加快制度、机制、模式和技术创新，积极拓展数字化应用场景，不断增强广大农民的获得感、幸福感、安全感。要因地制宜、循序渐进，立足本地发展实际，探索具有区域特色的模式做法，不搞一刀切、齐步走，杜绝“形象工程”，久久为功、有力有序推进数字乡村建设。

《通知》明确了工作目标，到 2026 年底，试点地区数字乡村建设取得显著成效，乡村信息化发展基础更加夯实，城乡“数字鸿沟”加快弥合，

涉农数据资源实现共享互通，乡村数字化应用场景持续涌现，数字经济促进共同富裕作用凸显，乡村振兴内生动力不断增强。通过开展第二批试点，探索不同区域条件下数字乡村发展路径和方法，打造一批有特色、有亮点的发展样板，挖掘一批可复制、可推广的典型模式，为推进乡村全面振兴、加快建设农业强国提供有力支撑。

《通知》提出，试点工作以市或县为单位、按照不同试点类型方向分类开展。一是领域特色型，包括智慧农业、乡村数字富民产业、乡村数字治理、乡村数字文化、乡村数字惠民服务、智慧美丽乡村 6 个方向。建设一批智慧农（林、牧、渔）场，推动智能感知、智能分析、智能控制技术与装备在农业生产经营中的集成应用。深入实施“互联网+”农产品出村进城工程和“数商兴农”，推动生产、加工、流通、销售各环节数字化转型。构建农文旅融合的现代产业体系，培育依托互联网的农文旅新业态新模式。坚持和发展新时代“枫桥经验”，推进数字技术与乡村治理深度融合，打造一批集约、高效、精准的数字化应用场景。深入实施国家文化数字化战略，运用数字技术加强对传统村落、农耕文化、非物质文化遗产等文化资源的挖掘活化和保护利用。构建线上线下相结合的农村信息服务体系，提升乡村公共服务数字化智能化水平。践行“绿水青山就是金山银山”理念，运用数字技术推进农业绿色发展，创新塑造乡村绿色生活。试点地区结合自身需求和特色优势，聚焦某一领域方向开展试点，集中力量打造一批典型样板。二是区域综合型，分东部、中部、西部、东北 4 个片区开展综合性试点。试点地区立足区位特点、资源禀赋、经济水平等基础条件，从智慧农业、乡村数字富民产业、乡村数字治理、乡村数字文化、乡村数字惠民服务、智慧美丽乡村等领域中，选择至少 3 个作为试点主攻方向，探索具有区域特色的路径模式。三是机制共建型，包括城乡融合发展、东西部

协作 2 个方向。城乡融合发展方向，以县域为基本单元，以畅通城乡要素双向流动为关键，统筹推进智慧城市与数字乡村建设，推动城乡数字基础设施互联互通、数据资源整合共享、产业生态相互促进、数字治理一体推进、公共服务共建共享，有效释放数字化发展红利、弥合城乡“数字鸿沟”。东西部协作方向，围绕数字乡村建设重点领域，探索东西部以信息流带动技术流、资金流、人才流、物资流的协作模式，促进资源优化配置，助力区域协调发展。

下一步，中央网信办将会同有关部门组织开展试点地区遴选工作，加强对试点地区的政策支持和业务指导，及时总结提炼试点地区优秀案例和创新做法，强化经验交流与示范推广，整体带动数字乡村建设迈上新台阶。

（来源：中国网信网）

3. 明确对关键信息基础设施重点保护，国安部解读网络安全法亮点

《中华人民共和国网络安全法》于 2016 年 11 月 7 日发布，自 2017 年 6 月 1 日起施行，是我国第一部全面规范网络空间安全管理方面的基础性法律。这部法律是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定，对提高我国网络安全保障水平和全民网络安全意识具有重要意义。

近日，微信公众号“国家安全部”发文解读《网络安全法》的四大亮点。

亮点一：明确网络空间主权原则

《网络安全法》第一条开宗明义，明确要维护我国网络空间主权。同时，第二条规定，在我国境内建设、运营、维护和使用网络，以及网络安全的监督管理适用本法。

网络空间主权是指国家主权在网络空间的自然延伸，是一国基于国家主权对本国境内的网络设施、网络主体、网络行为及相关网络数据和信息等所享有的对内最高权和对外独立权。

亮点二：明确实施网络实名制度

《网络安全法》第二十四条规定，网络运营者为用户办理入网手续，或者为用户提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

网络实名制的实施有利于构建良好的网络秩序。一个安全稳定繁荣的网络空间，对经济发展和社会稳定具有重要意义。网络空间是虚拟的，但参与网络活动的人是真实的，一些别有用心的人披着“马甲”，以虚拟的身份捏造歪曲事实、恶意引导舆论、肆意造谣抹黑，网络实名制就是一面让他们无所遁形的“照妖镜”。

亮点三：明确对关键信息基础设施实行重点保护

《网络安全法》第五条和第七十五条规定，对关键信息基础设施实行重点保护，境外的个人或组织机构从事攻击、侵入、干扰、破坏等危害我国关键信息基础设施的活动，造成严重后果的，依法追究法律责任；有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

同时，《网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境

内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等基础设施。近年来，境外势力加大对我关键信息基础设施数据的刺探和搜集力度，对我国国家安全造成现实威胁。明确相关重要数据跨境传输规则，才能为我国关键信息基础设施安全提供有效保障。

亮点四：明确共同治理原则

《网络安全法》第十四条赋予了个人和组织向有关部门举报危害网络安全行为的权利；第二十八条和第六十九条规定了个人和组织有维护国家安全的责任义务。网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助，拒不提供者，由有关主管部门责令改正；拒不改正或情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接负责人员，处一万元以上十万元以下罚款。

维护网络空间安全需要多主体的共同参与，《网络安全法》鼓励政府部门、网络建设者、网络运营者、网络服务提供者、网络行业相关组织、公民等根据各自角色参与网络空间安全治理工作。

国家安全机关提示

网络安全为人民，网络安全靠人民。任何个人和组织在使用网络时应当遵守宪法法律，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益的活动。公民和组织应依法协助配合国家安全机关维护国家安全和侦查犯罪活动。

让我们共同遵守网络安全法律，增强网络安全意识，携手筑牢国家网络安全屏障。

（来源：观察者网）

4. 2023“安满周”4 月中旬全国线上线下同步举办 亮点纷呈

为深入学习贯彻 2024 全国两会精神，落实习近平总书记关于网络强国的重要思想和一系列讲话精神，不断汇聚社会各方力量，加快发展新质生产力，助力推进高质量发展。在网民网络安全感满意度调查活动组委会统筹下， 2023 网民网络安全感满意度调查报告发布周（简称“安满周”）将于 4 月中旬全国线上线下同步举办。

本届安满周以“你我携手——构筑数字时代网络安全新防线”为主题，邀请全国网安联成员单位、调查活动发起单位，以及各地各级相关政府主管部门、高校科研院所、企事业单位、志愿服务团队、网民代表等，共聚京城香山，出席全国总报告、部分专题报告和区域报告的发布和解读，携手共筑数字时代网络安全新防线，与亿万网民同心而行，与国家网络安全同向而进。

亮点一：连接第二个五年规划，探索未来发展新方向

从 2023 年开始，网民网络安全感满意度调查活动步入第二个五年，在国家有关新政策、新部署、新指示的指引下，更加注重数字经济发展带给民生的改变，并充分运用互联网、大数据等现代信息技术，在问卷调查、抽样调查、统计分析中进行全面升级，对活动官网（网络安全共建网）、“网安联”小程序、调查问卷系统等平台进行改版/升级，更好地支持服务各项活动的宣传推广、组织协调、样本采集等工作的开展。坚持不遗余力

开展调查研究，倾听网民心声，分析网民意见，发现社会网络综合治理中的主要情况和重点问题，通过全面的调查和权威的发布，向国家和有关部门开展网络社会治理与监管提供详实的网情民意支撑。

2023“全国总报告发布会”是本届安满周最重要的活动，将邀请全国各地政府主管部门、企业机构和院校组织一起为网民呈现2023广大网民最关注哪些网络安全问题，新一代信息技术和数字化又将怎么样影响百姓生活。

亮点二：线下发布全面放开，多城市点亮发布盛况

2021 安满周作为首届调查报告专属发布周，创新性地将全国总报告、系列专题报告、以及部分区域报告的发布安排在一个自然周期内，全国十数个城市举办相应的发布会和专家解读专场，全国各界相关人士、数十万网友齐聚云端，共话网安。

2022 安满周，又创造性的将“安满周”作为发布周品牌名字确定下来，并完成更为全面的“总报告发布”“网安共建”“网民满意”三个发布版块架构，启动多论坛形式共话网安新生态。

2023 安满周，将承上启下，在延续安满周发布报告的“百名专家学者参与报告发布、报告解读、主题演讲和讨论”的特色上，还将加大报告发布和论坛权重，增加创新亮点，多城市线下发布，创新接力“点亮城市之光”，充分弥补前两届因疫情影响不能密集举办线下发布的遗憾，并将在全面放开的基础上，以“线下+线上”相结合的发布形式，壮大全网宣传势能，进一步提升活动影响力。

亮点三：网安联年会同期举办，19 年峥嵘回顾齐聚首

2024 网安联工作年会将在安满周期间同步在北京举办。

这是一场由来自各地的网络安全行业协会及相关社会组织、互联网行业专家学者共同参与的盛会，来自北京、上海、重庆、广东、安徽、广西、贵州、甘肃、湖北、湖南、海南、黑龙江、江苏、辽宁、陕西、新疆、广州、揭阳、南宁、贵阳、郑州、武汉、徐州、苏州、南昌、榆林、成都、昆明、曲靖、金华、宁波等省市的网安联成员单位代表以及各省市的志愿服务团队代表共赴“网安联之约”，回首网安联19年历程，进一步深化各成员单位之间协作交流，协同服务高质量发展，构建网络志愿服务共同体，创新开展“网民网络安全感满意度调查活动”和“安满周”，为网络强国建设作出新贡献。

亮点四：超重磅嘉宾阵容发布报告，多家流量平台直播盛况，活动规模进一步扩大

本届安满周，将邀请中国工程院院士出席，他们将带着最新的视角，分享关于报告的研究和解读。与此同时，还将邀请来自公安部、工信部、教育部等多家国家部委及直属机构领导、专家，以及清华大学、复旦大学、浙江大学、北京师范大学等全国数十家知名高校及科研院所的百位教授学者进行多个专题的解读。

今年安满周期间将剖析网络谣言案例；聚焦个人信息保护和互联网平台监管；助力数字政府服务建设，关注移动新科技对百姓生活影响和网民新诉求；分析热点话题——数字经济发展和网络安全挑战等。今年的专题除了关注网情民意外，还将更多专业技术型板块拓宽深挖，发布《网络安全法治社会建设专题报告》《行业治理与企业合规专题报告》《算力网络安全专题报告》《新技术挑战与网络安全专题报告》及解读，同步腾讯集团、虎牙等多平台直播，与广大网民在线互动，让专家与网民线上零距离接触，打造一个民意触达互动的多元平台。

亮点五：全国100+志愿团队线上线下齐关注，搭建群众心意沟通桥梁

2023调查活动开展期间，全国100+志愿团队助力参与网络诚信建设专题调查活动，逐步形成了一股踊跃参与调查的基层力量，各地协会携手基层志愿者团队，共建网络安全，共享网络文明，深入农村、社区、企业、医院、学校、新经济组织，全面开展提升广大网民数字素养和技能的调查研究，一批批网络志愿服务站/队加入进来，成为耀眼的存在。

本届安满周也成为各志愿服务机构展现自我的舞台，“网安联全国网络志愿服务大会”将对全国“网安联• 2023 网络志愿服务调查活动”优秀组织单位与优秀支持单位、先进个人进行表彰颁奖，进一步助力数字时代我国网络强国和人才强国建设，搭建各团队交流的平台与群众心意沟通桥梁，共同探讨志愿服务与调查活动延伸的未来发展趋向。

（来源：网安联）

行业前沿观察二：各地协会动态

导读：伴随春天的脚步，全国人民喜庆迎来了“两会”的召开，各地协会开展了精彩纷呈的活动。多家网安联成员单位协会参与了黑猫投诉联合各地公检法特别策划“法制赋能 315”普法活动；湖北省信息网络安全协会组织 2024 年网络安全管理员第一期考试；江苏省信息网络安全协会走访江苏省国信数字科技有限公司，探索会企共建新机制；上海市信息安全行业协会成功举办 2024 上海网络安全产业创新大会数据安全产业创新论坛；携手奋进，共赢未来，“第三届广东信创大赛”融企对接会（第一场）召开，共同探讨信创产业的发展；徐州网络公共安防技术协会召开工业互联网信息安全工作贯标与分级分类战略分析座谈会。

关键词：协会，网络安全，法治，315，互联网

1. 多家网安联成员单位协会参与——黑猫投诉联合各地公检法特别策划“法制赋能 315”普法活动

2024 年 315 期间，新浪旗下消费者服务平台黑猫投诉将在北京、上海、广东等地方法院、检察院的指导下，联合北京网络行业协会、上海市信息网络安全管理协会、广东省计算机信息网络安全协会、陕西省信息网络安全协会、湖北信息网络安全协会、成都信息网络安全协会等地方网安单位举办系列普法活动。

活动旨在推动消费者权益保护知识的普及、提高公众对于法律法规的认知，促进构建公平、透明、诚信的消费市场环境。将以“法制赋能 315”为主旨，邀请黑猫投诉旗下律师团队黑猫帮帮团律师共 30 位参与此次公益活动，包括最高检民事行政诉讼监督案件咨询专家、最高法、司法部指定法律援助律师王杰律师、央视《法律讲堂》栏目律师主讲人李娜律师、中央人民广播电台《华夏之声》节目嘉宾律师张党伟律师、北京网络行业协会法律委员会副主任王琮玮律师等。

活动期间，黑猫投诉将聚焦于消费者所关注的社会热点事件，通过各大媒体、社交平台等多元化渠道，分享真实消费陷阱案例以及避坑指南。同时，针对 315 期间以及 2023 年全年的热门话题精心安排一系列直播连麦活动，邀请行业大 V、旗下帮帮团律师以及地方媒体代表共同参与，并通过互动讨论的形式，深入剖析消费者所关心的法律问题，分享实用的法律知识和维权经验。（来源：北京网络行业协会）

2. 湖北省信息网络安全协会组织 2024 年网络安全管理员第一期考试

3 月 13 日，湖北省信息网络安全协会发布 2024 年网络安全管理员第一期考试公告，就相关事项进行公告通知。

全面落实终身职业技能培训制度，深入实施国家职业技能提升行动，大力推进技能强国建设，建立科学的技能人才评价制度，对于加强职业技能培训，提高劳动者素质，促进劳动者就业创业，激励引导技能人才成长成才具有重要作用。

湖北省信息网络安全协会作为湖北省人力资源和社会保障厅备案批准的省级社会培训评价组织，特此按照国家职业技能标准开展网络安全管理员，信息安全管理员职业技能等级认定评价工作。

公告就认定工种及等级、认定条件、认定程序、认定要求、注意事项等内容进行了详细说明。其中，此次职业技能认定职业（工种）为：网络安全管理员（四级、三级）、信息安全管理员（四级、三级）。考试（认定）地点在湖北省信息网络安全协会。（来源：湖北省信息网络安全协会）

3. 江苏省信息网络安全协会走访江苏省国信数字科技有限公司，探索会企共建新机制

3 月 8 日，江苏省信息网络安全协会常务副理事长尤文杰、副理事长赵和平率队前往协会理事单位——江苏省国信数字科技有限公司考察交流，并就会企共建工作进行探讨。国信数科董事长陈晓东及业务骨干出席了会议。

交流期间，国信数科董事长陈晓东对协会领导深入企业走访考察表示热烈欢迎，随后对公司的经营情况、业务板块、运营模式等方面做了介绍。并希望通过协会这一平台能够获得更多资源和更大的发展空间，促成项目合作，为江苏的网络强省建设贡献力量。

协会领导在听取情况介绍后，对国信数科的信息安全和数字化转型工作表示高度赞赏，并对会企共建工作提出了总体建议。强调协会将进一步强化质量意识、创新意识和责任意识，坚持政治引领，探索会企共建新机制，与会员单位建立联系点制度，开展党员联建，活动联办，业务联动，为会员单位提供更加精准高效的服务，为助推江苏高质量发展贡献力量。（来源：共创网安）

4. 上海市信息安全行业协会成功举办 2024 上海网络安全产业创新大会数据安全产业创新论坛

日前，2024 上海网络安全产业创新大会数据安全产业创新论坛在上海成功举办。此次论坛是在上海市经济和信息化委员会和普陀区人民政府的指导下，由上海市信息安全行业协会等 3 家行业社会组织主办，上海市信息安全行业协会数据安全与隐私计算专业委员会承办。上海市普陀区科学技术委员会主任李文波和中国信息通信研究院泰尔系统实验室副总工程师张治兵出席论坛并致辞。

论坛上举行了“2023 年度数据安全优秀案例评选”入选单位颁奖仪式。该评选活动围绕标准化安全产品、车联网场景、工业互联网场景、政务场景、数据安全治理、金融场景、互联网场景 7 个方向评选出优秀案例，旨在提升公众和行业对数据安全的重视程度，促进相关技术和产品的创新与

应用，树立行业标杆，扩大产业影响，激发市场主体活力，对于保障数据安全、推动数字经济健康发展具有重要意义。

论坛还以“数据资产管理与金融化”为主题进行了精彩的圆桌讨论，展开多方位、多角度的深入解析。（来源：上海市信息安全行业协会）

5. 携手奋进 共赢未来 “第三届广东信创大赛”融企对接会（第一场）召开

2 月 29 日，“第三届广东信创大赛”融企对接会（第一场）在广东省网络空间安全协会 19 楼报告厅召开，广东省网络空间安全协会长黄丽玲、副会长黄志豪，中信银行广州流花路支行负责人高帅等相关负责人出席会议。协会会长助理黄丽佳主持会议。来自全国各地的会员单位和企业代表 20 余人通过线上加线下的方式参加会议，共同探讨信创产业的发展。

协会党支部专职副书记黄汝锡致欢迎辞，代表主办方向出席“第三届广东信创大赛”融企对接会的来宾表示诚挚欢迎。他提到，此次“第三届广东信创大赛”融企对接会第一会，旨在践行服务企业健康快速发展、推动广东信创产业高质量发展，是加强融企对接交流互动，推进交流合作的体现，是推动大赛工作有效开展的实际行动，希望大家多出金点子、建真言、谋良策、出实招，共同努力把此次对接会开好开出成效。今后会有更多金融机构参与进来对接各类活动，为企业服务，为大家服务。

中信银行广州流花路支行负责人高帅致辞，从中信概况、业务概览、中信银行简介三方面详细介绍了中信集团的实力与业务领域 。中信集团深耕五大板块，构建五大平台，突出整合协同拓展三大抓手。中信银行成立于 1987 年，是国内全牌照平台背景的国有股份制商业银行，目前在全国 153

个城市设有1432家营业网点，是中信集团的秘书处，提供金融综合、智能制造、先进材料等一体化综合服务。

在参会代表进行了交流互动，针对广东在网络安全领域的现状和发展、如何提高广东企业在网络安全领域的影响力、企业如何异地融资、网络安全行业融资困难、利用银行资源进行合作和分忧的可能性等问题进行了详细探讨。

协会会长黄丽玲做总结讲话，她表示，通过金融的手段来促进协会企业会员的健康发展，邀请优质金融机构为有需求企业和项目团队提供资金支持，使广东的信创企业更加快速的发展是协会此次举办融企对接会的主要目的，希望在场的企业在这里能够有所收获，通过此次活动，促进银企关系，助力协会的会员单位和信创企业的健康发展，合作共创美好未来。

她提到，网络安全是国家安全战略非常重要的板块，长时间以来，协会面对民营企业关注的主要是技术、管理、合规，对企业融资方面关注比较少，在服务会员这一块思路要拓宽。协会在网络空间安全领域深耕了20多年，拥有丰富的行业经验和平台资源，可以为企业提供网络安全专业服务，帮助企业发展。其次，由协会主办的广东信创大赛将信创产品、技术、方案与业务需求融合更加紧密，为企业发展提供赋能。大赛连续举办了两届，吸引了全省21个地市人员积极参与，每年报名人数超过2600 多人次，已经成为全省的一个品牌赛事。今年即将举行的“第三届广东信创大赛”更是受到了省政数局、省国资委、省教育厅、省科协等跟信创、网络安全相关的政府部门的大力支持，如何依托广东信创大赛平台反哺会员单位和信创企业、为信创企业做出更大的实质性服务还需要详细规划。希望接下来中信能够更多的支持，也希望在座的各位企业跟协会多交流，把大家的

需求诉求多跟协会反映，共同携手，为广东省信创产业高质量发展添砖加瓦。（来源：广东省网络空间安全协会）

6. 徐州网络公共安防技术协会召开工业互联网信息安全工作贯标与分级分类战略分析座谈会

3 月 3 日上午，徐州网络公共安防技术协会召开了一场题为“锚定安全目标•共绘发展蓝图”的工业互联网信息安全工作贯标与分级分类战略分析座谈会。会议围绕如何加快安全贯标进程、细化分类分级管理以及提升行业安全防护水平等展开了全面而深入的研究探讨。

会议详尽介绍了目前徐州市工业互联网信息安全工作推进的总体情况与方案思路，梳理了安全贯标与分类分级工作组的具体任务，广泛征求了与会人员的意见与建议。会议倡导协会要联手市公安信息安全通报中心、工信局等部门，建立一套完整的工业互联网信息安全通报协同响应发布机制。与会人员就协会如何凭借自身的学术权威及技术实力系统开展区域性工业互联网信息安全维护工作进行了探讨。

协会理事长卜庆亚做会议发言，并提出了“全力推动协会数字化服务平台搭建”“精心筹备年度中期（年中）理事会”“加快开展网络安全行业职称评定工作”这三大协会近期的核心工作任务。（来源：徐州网络公共安防技术协会）

7. 佛山市信息协会承办“2024年佛山市中小企业服务机构宣贯服务活动（第一期）

近日，由佛山市工业和信息化局指导、佛山市中小企业服务中心主办、佛山市信息协会承办的“2024年佛山市中小企业服务机构宣贯服务活动（第一期）顺利举行。

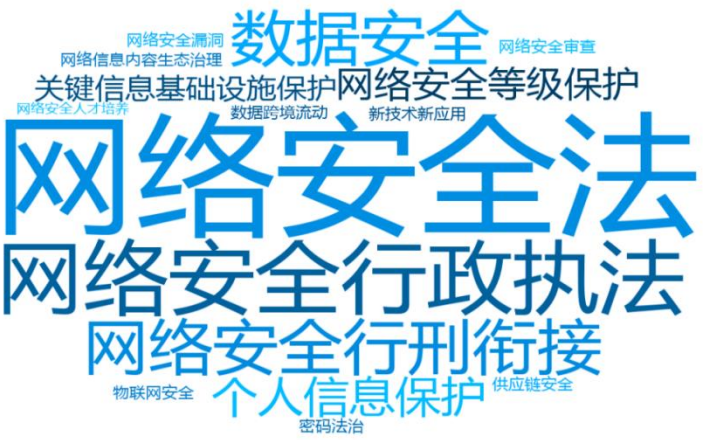
来自产业集群、示范平台、示范基地、产业园区、商协会、涉企服务机构的70名代表参加了第一期研修班。

此次研修班邀请到了多位业界精英和行业专家担任讲师，围绕佛山工业互联网产业发展探索和破局的思考、产业集群培育经验分享、细分行业中小企业数字化转型产业集群模式的实践与探索、佛山市产业集群政策及广东省中小企业数字化转型城市试点政策、“专精特新”“小巨人”政策解读及申报实务技巧交流企业培育辅导实务、金融赋能中小企业高质量发展等，他们分别从自己的实践经验和研究成果出发，分享了大量实用性的案例和经验，并就参训人员的问题进行了细致的解答和指导。（来源：佛山市信息协会）

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

……