网安联
Wang An Lian

网络与数据安全治理

FRONTIERS OF REGULATORY OVERSIGHT IN CYBERSECURITY AND DATA GOVERNANCE

前沿洞察（月刊）

2024年4月第4期（总第9期）

2024年4月30日

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：聚焦两会

导读：3 月 5 日至 11 日，2024 年全国两会在北京召开。期间，国务院、全国人大常委会、最高人民法院、最高人民检察院作工作报告。报告内容涉及数字经济发展、网络安全相关立法推进、网络违法犯罪打击整治等。

政府工作报告统筹安全与发展，表示 2024 年政府将深入推进数字经济创新发展。健全数据基础制度，大力推动数据开发开放和流通使用。推动解决数据跨境流动等问题。保障安全方面，2024 年政府将加强重点领域安全能力建设，提高网络、数据等安全保障能力。完善网络综合治理，培育积极健康、向上向善的网络文化。

全国人大常委会工作报告 2023 年工作和 2024 年任务中，均涉及网络安全相关立法推进。2023 年，初次审议治安管理处罚法修订草案，将违法出售或提供公民个人信息等行为纳入处罚范围。2024 年将修改网络安全法。

作为我国网络安全领域首部基础性、综合性法律，《网络安全法》自 2017 年 6 月 1 日正式施行以来，已六年有余。2022 年 9 月，国家互联网信息办公室发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》，意在对《网络安全法》法律责任部分进行调整优化。全国人大常委会表示 2024 年将修改网络安全法，该项立法工作有望取得新的进展。

最高人民法院、最高人民检察院工作报告聚焦电信网络诈骗、网络暴力、个人信息保护方面。2023 年，各级法院、检察院围绕惩治电信网络诈骗、网络暴力“按键伤人”“按键杀人”等开展大量工作。检察院还针对

互联网领域侵犯个人信息、虚假宣传、消费欺诈等乱象，办理公益诉讼 6766 件。2024 年，各级法院将严厉打击整治电信网络诈骗、跨境赌博等犯罪。从源头加强数据权利和个人信息保护，完善数字权益保护规则。各级检察院将协同开展“净网”行动，专项打击整治网络谣言，依法惩治网络犯罪，促进依法管网治网。深入打击整治电信网络诈骗犯罪。加强个人信息保护等民生领域司法保障。

关键词：数字经济创新发展、网络综合治理、网络安全法修改、电信网络诈骗、网络暴力、个人信息保护

1. 2024 年《政府工作报告》：将提高网络、数据安全保障能力

3 月 5 日，国务院总理李强在第十四届全国人民代表大会第二次会议上作政府工作报告。

报告指出，2024 年政府将深入推进数字经济创新发展。制定支持数字经济高质量发展政策，积极推进数字产业化、产业数字化，促进数字技术和实体经济深度融合。深化大数据、人工智能等研发应用，开展“人工智能+”行动，打造具有国际竞争力的数字产业集群。健全数据基础制度，大力推动数据开发开放和流通使用。集成国家战略科技力量、社会创新资源，推进关键核心技术协同攻关，加强颠覆性技术和前沿技术研究。推动解决数据跨境流动等问题。推进中国一东盟自贸区 3.0 版谈判，推动加入《数字经济伙伴关系协定》、《全面与进步跨太平洋伙伴关系协定》。

报告强调，2024 年将加强重点领域安全能力建设，提高网络、数据等安全保障能力。有效维护产业链供应链安全稳定，支撑国民经济循环畅通。完善网络综合治理，培育积极健康、向上向善的网络文化。维护国家安全和社会稳定。贯彻总体国家安全观，加强国家安全体系和能力建设。提高公共安全治理水平，推动治理模式向事前预防转型。（来源：中国政府网）

2. 2024 年《全国人大常委会工作报告》：将修改网络安全法

3 月 8 日，全国人民代表大会常务委员会委员长赵乐际在第十四届全国人民代表大会第二次会议上作全国人民代表大会常务委员会工作报告。

报告指出，2023 年，全国人大常委会修订反间谍法，将防范化解风险的关口前移，丰富反渗透、反颠覆、反窃密斗争的法律工具箱。修订保守国家秘密法，健全保密管理制度和监管措施。初次审议治安管理处罚法修订草案，将违法出售或提供公民个人信息等行为纳入处罚范围。

报告指出，2024 年，将围绕推进国家安全体系和能力现代化，修改网络安全法。（来源：中国政府网）

3. 2024 年《最高人民法院工作报告》：将从源头加强数据权利和个人信息保护

3 月 8 日，最高人民法院院长张军在第十四届全国人民代表大会第二次会议上作最高人民法院工作报告。

报告指出，2023 年，各级法院严厉惩治境内外电信网络诈骗犯罪，审结电信网络诈骗案件 3.1 万件 6.4 万人，同比增长 48.4%。依法惩治网络暴力。针对网络暴力“按键伤人”、“按键杀人”，严重扰乱社会秩序，会同最高人民检察院、公安部出台司法政策，严惩网暴恶意发起者、组织者及屡教不改者。明确网络侮辱诽谤，造成被害人或其近亲属身心严重损害后果，或者随意以普通公众为侵害对象等，以公诉案件追究刑事责任。审结网络诽谤公诉案件 32 件，判决有罪人数 85 人，同比分别增长 10.3%、102.4%。

报告强调，2024 年将贯彻总体国家安全观，依法严惩危害国家安全、公共安全等犯罪，严厉打击整治电信网络诈骗、跨境赌博等犯罪。从源头

加强数据权利和个人信息保护，完善数字权益保护规则。（来源：中国政府网）

4. 2024 年《最高人民检察院工作报告》：推动网络空间依法治理

3 月 8 日，最高人民检察院检察长应勇在第十四届全国人民代表大会第二次会议上作最高人民检察院工作报告。

报告指出，2023 年全国检察机关推动网络空间依法治理。制定检察机关网络法治工作 21 条意见，起诉利用网络实施的犯罪 32.3 万人，同比上升 36.2%。坚决惩治网络暴力“按键伤人”，会同最高人民法院、公安部制定指导意见，对在网上肆意造谣诽谤、谩骂侮辱、“人肉搜索”等涉嫌犯罪的，依法提起公诉，追究刑事责任，维护公民人格权益和网络秩序。严厉打击“网络水军”造谣引流、舆情敲诈等违法犯罪，净化网络舆论环境。依法严惩电诈网赌，积极参与打击涉缅北电信网络诈骗专项行动，深挖严打组织者、领导者及幕后“金主”，起诉电信网络诈骗犯罪 5.1 万人、帮助信息网络犯罪 14.7 万人、网络赌博犯罪 1.9 万人，同比分别上升 66.9%、13%和 5.3%。针对互联网领域侵犯个人信息、虚假宣传、消费欺诈等乱象，办理公益诉讼 6766 件，督促落实监管责任和平台责任，用法治力量维护网络清朗。发布未成年人网络保护指导性案例，严惩“隔空猥亵”、线上联系线下侵害等犯罪，协同防治网络沉迷，引导安全用网上网。

报告强调，2024 年，全国检察机关将协同开展“净网”行动，专项打击整治网络谣言，依法惩治网络犯罪，促进依法管网治网。深入打击整治

电信网络诈骗犯罪。以专门立法为契机，进一步加强公益诉讼检察工作。深入实施数字检察战略。加强个人信息保护等民生领域司法保障。（来源：中国政府网）

境内前沿观察二：政策立法

导读：3 月，数据跨境流动管理模式发生重要调整。自《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》等法律法规正式确定并细化数据出境安全评估要求以来，数据出境安全评估成为组织在面临数据出境相关业务场景时需要考虑的重要合规义务之一。为进一步统筹安全与发展，探索更加灵活便利的数据出境管理模式，国家网信办正式公布《促进和规范数据跨境流动规定》，适当放宽数据跨境流动条件，适度收窄数据出境安全评估范围，在保障国家数据安全的前提下，便利数据跨境流动，降低企业合规成本，充分释放数据要素价值。国家网信办发布《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》。指南结合《促进和规范数据跨境流动规定》进行调整，为组织申报数据出境安全评估、备案个人信息出境标准合同提供指导，对数据处理者需要提交的相关材料进行优化简化。

在政策文件和地方探索方面，国务院办公厅印发《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》，支持外商投资企业与总部数据流动，将制定粤港澳大湾区跨境数据转移标准，建立港澳企业数据跨境流动机制，探索建立跨境数据流动“白名单”制度。上海市人民政府办公厅印发《上海外资研发中心提升计划》，支持外资研发中心研发数据依法跨境流动。甘肃省人民政府办公厅印发《甘肃省“数据要素×”三年行动实施方案（2024—2026 年）》，提出将探索推进数据跨境流动，在兰州新

区建设以数据跨境为特色的数字贸易示范区，打响“一带一路”向西开放平台特色牌。

数据分类分级和重要数据识别认定是数据安全保障中一项重要的基础性工作。3 月，国家标准《数据安全技术 数据分类分级规则》正式通过，给出数据分类分级的通用规则，为数据分类分级管理工作的落地执行提供重要指导。标准明确数据分类分级应当遵守科学实用、边界清晰、就高从严、点面结合、动态更新原则。行业领域方面，自然资源部印发《自然资源领域数据安全管理办法》，给出重要数据判定标准。

关键词：数据跨境流动、数据出境安全评估、数据分类分级、重要数据认定

（一）国家层面动向

1. 国务院办公厅印发《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》，将支持外商投资企业与总部数据流动

2 月 28 日，国务院办公厅印发《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》。

行动方案指出，将支持外商投资企业与总部数据流动。规范数据跨境安全管理，组织开展数据出境安全评估、规范个人信息出境标准合同备案等相关工作，促进外商投资企业研发、生产、销售等数据跨境安全有序流动。制定粤港澳大湾区跨境数据转移标准，依托横琴粤澳深度合作区、前海深港现代服务业合作区等重大合作平台，建立港澳企业数据跨境流动机制，探索建立跨境数据流动“白名单”制度，稳步推动实现粤港澳大湾区内数据便捷流动。

行动方案强调，将健全数据跨境流动规则。科学界定重要数据的范围。全面深入参与世界贸易组织电子商务谈判，推动加快构建全球数字贸易规则。探索与《数字经济伙伴关系协定》成员方开展数据跨境流动试点，加快与主要经贸伙伴国家和地区建立数据跨境流动合作机制，推动构建多层次全球数字合作伙伴关系网络。（来源：中国政府网）

2. 国务院发布《消费者权益保护法实施条例》，细化消费者个人信息保护规则

3 月 15 日，国务院发布《消费者权益保护法实施条例》，强调加大消费者合法权益保护力度。

实施条例规定，经营者应当依法保护消费者的个人信息。经营者在提供商品或者服务时，不得过度收集消费者个人信息，不得采用一次概括授权、默认授权等方式，强制或者变相强制消费者同意收集、使用与经营活动无直接关系的个人信息。经营者处理包含消费者的生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息以及不满十四周岁未成年人的个人信息等敏感个人信息的，应当符合有关法律、行政法规的规定。（来源：中国政府网）

（二）部委层面动向

1. 国家网信办公布《促进和规范数据跨境流动规定》

3 月 22 日，国家网信办公布《促进和规范数据跨境流动规定》，对现有数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的实施和衔接作出进一步明确，适当放宽数据跨境流动条件，适度收窄数据出境安全评估范围，在保障国家数据安全的前提下，便利数据跨境流动，降低企业合规成本，充分释放数据要素价值，扩大高水平对外开放，为数字经济高质量发展提供法律保障。

规定主要对下列内容进行规定：一是明确重要数据出境安全评估申报标准；二是明确免予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数据出境活动条件；三是设立自由贸易试验区负面清单制度；四是调整应当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数据出境活动条件；五是延长数据出境安全评估结果有效期，增加数据处理者可以申请延长评估结果有效期的规定。（来源：中国网信网）

2. 国家网信办发布《数据出境安全评估申报指南（第二版）》《个人信息出境标准合同备案指南（第二版）》

3 月 22 日，国家网信办发布《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》，对申报数据出境安全评估、备案个人信息出境标准合同的方式、流程和材料等具体要求作出说明，对数据处理者需要提交的相关材料进行优化简化。

数据处理者因业务需要向境外提供重要数据和个人信息，应当遵守《数据出境安全评估办法》、《个人信息出境标准合同办法》和《促进和规范数据跨境流动规定》有关规定。符合数据出境安全评估适用情形的，按照申报指南申报数据出境安全评估；通过与境外接收方订立个人信息出境标准合同的方式向境外提供个人信息的，按照备案指南向所在地省级网信部门备案。

国家网信办开通“数据出境申报系统”（https://sjcj.cac.gov.cn）。数据处理者可以通过该系统申报数据出境安全评估、备案个人信息出境标准合同。（来源：中国网信网）

3. 自然资源部印发《自然资源领域数据安全管理办法》

3 月 22 日，自然资源部印发《自然资源领域数据安全管理办法》，对数据分类分级管理、数据全生命周期安全管理、数据安全监测预警与应急管理、监督检查等内容进行规定。

办法结合自然资源领域数据特点，指出满足以下两项（含）以上参考指标的数据是重要数据：（一）支撑党中央和国务院赋予的“两统一”职责产生的具有不可替代性和行业唯一性的，一旦发生数据篡改、泄露或服务中断等安全事故，将影响自然资源部门履行职责，对全国范围内服务对象产生重要影响的数据；（二）涉及国民经济和重要民生的，为其他行业、领域提供自然资源基础数据支撑的，一旦发生数据安全事故会对其他行业、领域造成重要影响的数据；（三）覆盖多个省份甚至全国，规模大、精度高，且极具敏感性、重要性的数据；（四）直接影响国家关键信息基础设施正常运行服务的数据；（五）危害国家安全、国家经济竞争力、危害公众接受公共服务、危害公民生存条件和安定工作生活环境、危害公民的生命财产安全和其他合法利益、导致社会恐慌等的数据；（六）我国法律法规及规范性文件规定的其他自然资源重要数据。（来源：自然资源部）

4. 中国民用航空局发布《民航数据管理办法（征求意见稿）》《民航数据共享管理办法（征求意见稿）》

3 月 11 日，中国民用航空局发布《民航数据管理办法（征求意见稿）》《民航数据共享管理办法（征求意见稿）》。

《民航数据管理办法（征求意见稿）》就民航数据管理的职责分工、数据资源目录、数据采集与治理、数据共享、数据应用、数据安全、监督保障等作出规定。征求意见稿将民航数据分为公共数据、企业数据、个人信息数据三类；根据数据全生命周期处理活动场景，将民航数据处理主体分为数据提供方、数据使用方、数据管理方和数据平台方。

《民航数据共享管理办法（征求意见稿）》就民航数据共享类型、目录管理、数据归集、数据的获取与使用、保障监督等做出规定。征求意见稿要求，民航局数据统筹管理部门应当组织民航局各业务领域数据管理方，按照应归尽归的原则，监督本业务领域无条件共享类和有条件共享类的数据归集至行业数据共享与服务平台，并形成基础数据库、主题数据库等。（来源：中国民用航空局）

5. 国家金融监督管理总局发布《银行保险机构数据安全管理办法（征求意见稿）》

3 月 22 日，国家金融监督管理总局发布《银行保险机构数据安全管理办法（征求意见稿）》。征求意见稿主要内容如下：

一是落实数据安全责任制。明确银行保险机构党委（党组）、董（理）事会对本单位数据安全工作负主体责任，机构主要负责人为数据安全第一责任人，分管数据安全的领导为直接责任人。

二是明确数据安全归口管理部门。要求银行保险机构指定数据安全归口管理部门，作为本机构负责数据安全工作的主责部门，承担制定数据安全管理制度标准、建立维护数据目录、推动数据分类分级保护、组织开展风险监测、预警及处置等职责。

三是将数据安全风险纳入全面风险管理体系。要求银行保险机构明确管理流程，主动评估风险，对数据安全风险进行有效监测，防止数据破坏、泄露、非法利用等安全事件发生。风险管理、内控合规和审计部门定期对数据安全开展审计、监督检查与评价。

四是强化数据安全评估。要求银行保险机构开展相关数据处理活动时，应事先开展安全评估。根据数据处理目的、性质和范围，分析数据安全风险和对数据主体权益影响，评估数据处理的必要性、合规性及防控措施的有效性。

五是建立数据安全保护基线。将数据纳入网络安全等级保护，对存放或传输敏感级及以上数据的机房、网络实施重点防护，在数据全生命周期内采取有效访问控制管理措施，采用安全有效的传输方式保障数据完整性、保密性、可用性。（来源：国家金融监督管理总局）

6. 全国网安标委发布《生成式人工智能服务安全基本要求》

2 月 29 日，全国网安标委发布《生成式人工智能服务安全基本要求》，给出生成式人工智能服务在安全方面的基本要求，包括语料安全、模型安全、安全措施等。文件适用于服务提供者开展安全评估、提高安全水平，也可为相关主管部门评判生成式人工智能服务安全水平提供参考。

本文件支撑《生成式人工智能服务管理暂行办法》，提出服务提供者需遵循的安全基本要求。服务提供者在按照有关要求履行备案手续时，按照本文件要求进行安全评估，并提交评估报告。

除本文件提出的基本要求外，服务提供者应自行按照我国法律法规以及国家标准相关要求做好网络安全、数据安全、个人信息保护等方面的其他安全工作。服务提供者应紧密注意生成式人工智能可能带来的长期风险，谨慎对待可能具备欺骗人类、自我复制、自我改造能力的人工智能，并重点关注生成式人工智能可能被用于编写恶意软件、制造生物武器或化学武器等安全风险。（来源：全国网络安全标准化技术委员会）

7. 全国网安标委发布《数据安全技术 数据分类分级规则》

3 月 21 日，全国网安标委发布 GB/T 43697-2024《数据安全技术 数据分类分级规则》，给出数据分类分级的通用规则，为数据分类分级管理工作的落地执行提供重要指导。该标准自 2024 年 10 月 1 日起施行。

标准指出，重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济

运行、社会稳定、公共健康和安全的数据。仅影响组织自身或公民个体的数据一般不作为重要数据。

核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

标准明确数据分类分级应当遵守科学实用、边界清晰、就高从严、点面结合、动态更新原则。（来源：全国网络安全标准化技术委员会）

（三）地方层面动向

1. 上海市人民政府办公厅印发《上海外资研发中心提升计划》，支持外资研发中心研发数据依法跨境流动

3 月 1 日，上海市人民政府办公厅印发《上海外资研发中心提升计划》，支持外资研发中心研发数据依法跨境流动。

提升计划强调，要加快建立健全数据资源交易流通、跨境传输、安全保护等制度和标准规范。鼓励外资研发中心通过数据安全管理认证，提高数据安全管理能力和水平，形成符合数据安全要求的标准或最佳实践，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。在中国（上海）自由贸易试验区（含临港新片区）按照数据分类分级保护制度，依法制定需要纳入管理范围的数据清单和重要数据目录，清单和目录以外

的数据出境，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。（来源：上海市人民政府办公厅）

2. 上海市财政局发布《关于进一步加强本市数据资产管理的通知》

3 月 21 日，上海市财政局发布《关于进一步加强本市数据资产管理的通知》。通知要求本市各级部门、行政事业单位和有关单位提高站位，充分认识加强数据资产管理的重要性；因地制宜，积极探索数据资产全过程管理路径；夯实责任，严格防控数据资产管理风险。

防控安全风险方面，通知要求上海市各级部门、行政事业单位和有关单位应当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；特别是针对数据资产确权、配置、使用、处置、收益、安全、保密等重点管理环节，明确管理责任，确保数据资产全过程管理安全，严格防控数据资产管理风险，切实筑牢数据资产安全保障防线。同时，本市各级部门、行政事业单位和有关单位也应依法依规保护各类主体在依法收集、生成、存储、管理数据资产过程中的相关权益。（来源：上海市人民政府）

3. 内蒙古自治区人民政府印发《内蒙古自治区数字政府建设实施方案》

3 月 5 日，内蒙古自治区人民政府印发《内蒙古自治区数字政府建设实施方案》。实施方案围绕提高政府数字化履职能力、完善数字政府建设制

度规则、促进数据资源共享开放、强化平台支撑能力、加强数字政府安全保障提出53项主要任务。同时，围绕引领驱动数字化发展提出10项要求。

其中，加强数字政府安全保障方面，实施方案要求加强安全管理。建立数字政府安全评估、责任落实和重大事件处置机制，强化网络安全、数据安全监管，切实防范公共数据被篡改、泄露和滥用。落实国家《规范企业参与政府信息化建设加强政务数据安全管理办法》，加强对参与政府信息化建设运维企业的规范管理，确保政务系统和数据安全管理边界清晰、职责明确、责任落实。

实施方案还要求构筑数据安全防护体系。强化数据全生命周期安全管理和技术防护，加强数据安全防护体系建设，推进数据加密、数据脱敏、数据水印、数据备份、数据溯源、隐私计算的技术能力全面应用。加强重要数据出境安全管理。加快自治区密码云建设，提升密码应用水平。加强数据安全业务培训和应急演练。落实数据安全分类分级保护制度，加大个人信息保护力度，制定重要数据具体目录，出台网络数据安全应急预案，落实数据安全和个人信息保护评估要求，加强网络数据安全风险和事件监督预警、通报、应急处置工作。（来源：内蒙古自治区人民政府）

4. 甘肃省人民政府办公厅印发《甘肃省“数据要素×”三年行动实施方案（2024—2026年）》

3月15日，甘肃省人民政府办公厅印发《甘肃省“数据要素×”三年行动实施方案（2024—2026年）》，旨在充分发挥数据要素乘数效应，赋能经济社会高质量发展。

优化数据流通环境方面，实施方案提出，提高交易流通效率，探索完善数据要素产权体系的相关政策，积极推动数据资产管理有关规定贯彻落实，建立健全数据登记确权、成本核算、价格形成、资产入表、收益分配等机制，完善全社会层面数据价格形成机制，推动数据要素市场化配置改革重大任务和事项落实。探索推进数据跨境流动，在兰州新区建设以数据跨境为特色的数字贸易示范区，打响“一带一路”向西开放平台特色牌。

加强数据安全保障方面，实施方案强调，强化数据安全防护责任落实，贯彻落实国家网络安全法、数据安全法、个人信息保护法及关键信息基础设施安全保护条例等法律法规，加强数据分类分级保护、个人信息保护和全生命周期安全管理。制定重要数据和核心数据保护工作指南，对重要数据和核心数据进行有效保护。丰富数据安全产品，多部门协同加强数据安全合作，鼓励基础电信企业、数据安全企业、服务机构研发推广多层次、专业化、定制化数据安全产品，促进各行业各领域深度应用，推动数据安全产业高质量发展。培育数据安全服务，鼓励数据安全企业开展基于云端的安全服务，有效提升数据安全水平。（来源：甘肃省人民政府办公厅）

5. 江苏省南京市数据局发布《南京市公共数据授权运营管理暂行办法 （征求意见稿）》《南京市数据资产登记暂行办法（征求意见稿）》

3 月 21 日，江苏省南京市数据局发布《南京市公共数据授权运营管理暂行办法（征求意见稿）》《南京市数据资产登记暂行办法(征求意见稿)》。

《南京市公共数据授权运营管理暂行办法 （征求意见稿）》规定职责分工、被授权运营单位申请和退出流程、授权运营要求、安全和监督等内容。征求意见稿规定，被授权运营单位应当满足运营安全要求和技术安全要求两个基本条件，包括落实数据安全负责人和管理部门，建立公共数据授权运营内部管理和安全保障制度;具有符合网络安全等级保护三级标准和商用密码应用安全性评估要求的系统开发和运维实践经验;具备成熟的数据管理能力和数据安全保障能力;以及近3年未发生网络安全或数据安全事件等。

征求意见稿规定，市数据主管部门联合网信、公安等监管部门加强各专区数据安全的监督检查，将专区检查纳入全市安全检查计划，每年开展监督检查。专区监管部门和被授权运营单位应当配合检查，及时整改检查中发现的问题，防范数据安全风险。被授权运营单位是公共数据专区的管理责任主体，承担专区数据安全主体责任。

《南京市数据资产登记暂行办法（征求意见稿）》对数据资产登记的内容和条件、登记申请人及登记主体、登记机构、登记行为等作出规定，旨在规范数据资产登记行为，保护数据要素市场参与主体的合法权益，促进数据的高效流动和开发利用。（来源：南京市数据局）

境内前沿观察三：治理实践

导读：3 月，部委和地方层面多项专项行动接连开展。中央网信办发布通知，部署开展 2024 年“清朗”系列专项行动，具体将围绕涉企侵权信息、违法信息外链、“自媒体”无底线博流量、生成合成内容标识等方面开展 10 项整治任务。3 月底，中央网信办部署开展“清朗·优化营商网络环境—整治涉企侵权信息乱象”专项行动。

地方层面，上海市和广东省通管局、广东佛山市委网信办针对车联网、电信和互联网行业、公共服务领域开展专项行动。其中，上海市通信管理局开展的是“铸盾车联”2024 年车联网网络和数据安全专项行动。聚焦车联网相关企业，检查网络和数据安全主体责任、车联网网络设施和系统安全、智能网联汽车产品安全、车联网平台和应用服务安全、车联网数据安全、自动驾驶功能安全六方面内容。广东省通信管理局开展的是 2024 年广东省电信和互联网行业网络数据安全和应用合规行政检查。检查对象较为广泛，包括相关企业建设运营的网络、系统、平台、应用、业务，重点是电信和互联网行业关键信息基础设施和重要网络单元及承载的信息系统；检查内容除网络与数据安全相关制度和防护措施外，还将对市场秩序和用户权益保护、互联网基础资源合规、反诈义务落实情况进行检查。中共佛山市委网信办开展的是公共服务领域网络和数据安全专项行动，针对全市党政部门、社会组织或国有企业通过信息化手段以满足群众各项公共服务活动需求所自行或委托建设的信息系统，将开展自查、远程技术检测、数据泄露监测、现场检查、意识培训、隐患整改、实战攻防演练复盘等工作。

3月公布的行政执法个案方面，涉及的违法行为均较为常见，即网络长期不使用不管理/未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施/未按要求留存网络日志等，导致网络存在漏洞或被侵入篡改，这在一定程度上反映出《网络安全法》实施至今，在中小型或微型组织的合规义务落地方面仍需持续加强。此外，中消协、上海市市场监管局公布多起保护个人网络权益相关的执法、司法案例，围绕线上点餐、公共场所安装具有人脸识别功能的摄像头、非法收集使用消费者个人信息拨打推销电话或发送商业性信息等场景，通过行政处罚或司法判决处置相关违法行为，保护个人合法权益。

关键词：清朗系列专项行动、车联网专项行动、电信和互联网行业合规检查、个人权益保护

（一）公安机关治理实践

1. 上海市公安局：将严厉打击网络直播诈骗犯罪

3 月 19 日，上海市公安局召开“砺剑 2024”上海公安新闻发布会，通报上海警方打击网络直播诈骗措施成效和典型案例。

通报指出，今年以来，上海警方深入开展“砺剑 2024”系列专项行动，持续严厉打击、严密防范电信网络诈骗。全市电诈案件既遂数和立案数在去年实现“五年连降”的基础上，继续保持“双下降”，同比分别下降 15.5%和 20.8%。依托前端预警和资金防阻体系，已上门提醒劝阻 7.3 万余人次，拦阻涉诈转账 2.9 万余笔，直接避免损失 5.1 亿余元。

通报提到，本市电诈发案以冒充客服、虚假购物、刷单返利三个类型为主，占比近 70%，随着直播经济的发展，利用网络直播进行的诈骗主要表现为以下五类手法：恋爱交友类、虚假网络购物类、直播售课类、投资认购类和直播引流类。

对此，上海警方坚持问题导向，紧盯新动向、新手法、新变化，依托“砺剑 2024”系列专项行动，全链条打击利用网络直播实施诈骗犯罪活动，不断挤压此类犯罪生存空间，全力维护人民群众财产安全。会同相关平台启动专项治理行动，强化事前风险防控，在提升部门监管、企业自治的同时，通过定时巡查、集中整治等方式，针对直播黑灰产等问题进行重点打击，不断营造良好的网络直播环境。（来源：警民直通车上海）

2. 四川网警查处两起不履行网络安全保护义务案

3 月 2 日消息，四川省攀枝花市公安局仁和区分局近日查处两起不履行网络安全保护义务案。

案例一：攀枝花市仁和区某经营部不履行网络安全保护义务案

攀枝花市仁和区某经营部自行开发建设名为“科岩 岩板”的网站用于公司产品的宣传。但由于该公司对网站长时间不使用不管理，导致网站被黑客攻击，造成网页被挂载赌博网站链接的严重后果。2024 年 2 月，攀枝花市公安局仁和区分局按照《网络安全法》第五十九条规定，依法给予攀枝花市仁和区某经营部警告处罚，并要求其立即整改。

案例二：攀枝花某旅游投资有限公司不履行网络安全保护义务案

攀枝花某旅游投资有限公司缺乏网络安全保护意识，相关系统日志未按国家要求保存六个月，存在相关风险隐患。2024 年 2 月，攀枝花市公安局仁和区分局按照《网络安全法》第五十九条规定，依法给予攀枝花某旅游投资有限公司警告处罚，并要求其立即整改。（来源：攀枝花平安仁和）

3. 湖南网警查处四起不履行网络安全保护义务案

3 月 5 日消息，湖南省永州市公安局冷水滩分局网安部门近期大力加强网络秩序清理整顿，积极开展网络安全检查，对四家不履行网络安全保护义务的单位依法予以处罚。

案例一：永州市某协会不履行网络安全保护义务案

1 月 10 日，永州市某协会的网站被他人侵入，在网站首页发布涉赌博网站类违法有害信息，该协会未采取防范计算机病毒和网络攻击、网络侵

入等危害网络安全行为的技术措施，属于不履行网络安全保护义务的行为。2024 年 1 月，永州市公安局冷水滩分局根据《网络安全法》第二十一条、第五十九条，责令该协会整改并给予警告的行政处罚。

案例二：永州某科技有限公司不履行网络安全保护义务案

永州某科技有限公司网站由于长时间无人管理，遭到他人的劫持篡改，成为通往非法网站的“跳板”。其内部的网站存在被植入不法链接、跳转赌博类网站的漏洞，属于不履行网络安全保护义务的行为。2024 年 2 月，永州市公安局冷水滩分局根据《网络安全法》第二十一条、第五十九条，责令该公司整改并给予警告的行政处罚。

案例三：湖南某技术有限公司不履行网络安全保护义务案

湖南某技术有限公司网站发现存在系统漏洞。经查，该公司网站没有制定建立管理制度，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，导致公司网站被植入后台程序，属于不履行网络安全保护义务的行为。2024 年 2 月，永州市公安局冷水滩分局根据《网络安全法》第二十一条、第五十九条，责令该公司整改并给予警告的行政处罚。

案例四：湖南某农业有限公司不履行网络安全保护义务案

湖南某农业有限公司网站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，导致公司网站被植入后台程序，网站首页存有违法信息，造成不良影响，属于不履行网络安全保护义务的行为。2024 年 2 月，永州市公安局冷水滩分局根据《网络安全法》第二十一条、第五十九条，责令该公司整改并给予警告的行政处罚。（来源：冷水滩公安）

4. 广西网警依法处置两起利用人工智能生成网络谣言的案例

3 月 4 日，公安部网安局公布两起广西警方处置的利用人工智能技术编“伪消息”博眼球，造“假通报”蹭热度的案例。

案例一：制作假地震消息误导社会公众

2024 年 1 月 23 日，东兴市骆某某（男，32 岁）为博取流量吸引粉丝，将其他地区的抗洪、救灾视频，利用 AI 软件自动编辑功能，嫁接新疆乌什县发生地震的虚假视频信息。视频被大量播放，并引发许多不明真相网民评论和转发，严重干扰社会秩序。目前，东兴市公安机关已依法对骆某某进行处罚。

案例二：编造假官方通报扰乱公共秩序

贺州市公安局平桂分局网警发现有人冒用贺州市平桂区人民政府办公室的名义，在网上发布一条“关于贺州市第五高级中学小卖部经营权调查情况的通报”。经查，该通报内容与政府发布通报实际情况严重不符，该发布人是山东青岛人于某某，其在网上看到关于贺州市第五高级中学小卖部经营权调查情况的通报后为蹭热度为自己账号涨粉，使用 AI 工具将该报道重新生成了一篇内容与政府发布通报实际情况严重不相符的文章，并发布到网上。目前，公安机关已依法对其处以行政处罚。（来源：公安部网安局）

5. 陕西西安网警依法处置一起利用人工智能生成网络谣言的案例

3 月 27 日消息，公安部网安局公布一起西安网警依法处置利用人工智能洗稿，生成网络谣言的案例。

2023 年 12 月以来，一条“西安市鄠邑区地下涌出热水”的信息频繁在网络上传播。伴随该条信息，互联网涌现出各式各样的谣言，如“地下出热水是因为发生了地震”、“是因为地下热管道破裂”.....部分谣言信息将事发于外地的照片与不实文字内容拼接起来，致使不明真相的网民信以为真，造成严重不良社会影响。发现此类信息后，民警积极开展调查取证工作。同时，多家主流媒体通过官方账号进行互联网辟谣。

经查，该类谣言均通过 AI 洗稿的方式生成。首先，违法行为人柳某等人利用一款可以洗稿的 AI 生成软件，将网络上海量的文章通过 AI 洗稿变成新的主题文章。然后，柳某把生成的文章草稿件推送给王某、伍某、范某等人，再由他们通过各自的社交平台账号将 AI 洗稿生成的不实内容发布于互联网，利用平台的创作模块获取收益，并将收益按一定比例与前期“洗稿”的柳某分成。西安市公安局鄠邑分局网安大队组织警力，分别赴四川、甘肃等地，协同当地公安机关，依据《治安管理处罚法》对违法行为人柳某、王某、范某给予行政处罚，对伍某进行批评教育，并责令 4 人删除相关谣言信息。现案件仍在进一步办理中。（来源：公安部网安局）

6. 陕西西安网警成功打掉一出售公民个人信息团伙

3 月 11 日消息，陕西西安未央网警近日成功打掉一个非法出售公民个人信息团伙，抓获犯罪嫌疑人 124 人，依法刑事拘留 19 人，冻结涉案银行卡账户 13 个。

2023 年 10 月，有群众向公安机关举报自己在网上咨询法律业务时，某法律咨询公司声称可查询各种包括银行卡、手机号等在内的公民个人身

份信息。西安未央网警初步查明该公司老板为李某，其上线为刘某，下线为 4 部 12 组的运营管理体系。该公司通过抖音、快手等网络社交平台发布广告引流，身披法律咨询业务外衣，以为客户提供诉讼代理为由，行“有偿查询、提供公民个人敏感信息”之实。经统计，该公司所提供的查询内容包括身份证号查地址、身份证查手机等个人敏感信息，索要价格在 600 元至 2000 元不等，通过查询买卖他人信息非法获利 270 余万。

目前，案件正在进一步侦办当中。（来源：西安网警）

（二）网信部门治理实践

1. 中央网信办部署开展 2024 年“清朗”系列专项行动

3 月 15 日，中央网信办发布通知，部署开展 2024 年“清朗”系列专项行动。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。

10 项专项行动分别是：（1）“清朗·2024 年春节网络环境整治”专项行动；（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；（3）“清朗·打击违法信息外链”专项行动；（4）“清朗·整治‘自媒体’无底线博流量”专项行动；（5）“清朗·网络直播领域虚假和低俗乱象整治”专项行动；（6）“清朗·规范生成合成内容标识”专项行动；（7）“清朗·2024 年暑期未成年人网络环境整治”专项行动；（8）“清朗·规范网络语言文字使用”专项行动；（9）“清朗·整治违规开展

互联网新闻信息服务”专项行动；（10）“清朗·同城版块信息内容问题整治”专项行动。

其中“清朗·打击违法信息外链”专项行动将坚决打击利用各种“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。

“清朗·规范生成合成内容标识”专项行动将聚焦落实《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。（来源：网信中国）

2. 中央网信办部署开展“清朗·优化营商网络环境—整治涉企侵权信息乱象”专项行动

3 月 30 日消息，中央网信办部署开展“清朗·优化营商网络环境—整治涉企侵权信息乱象”专项行动。

专项行动聚焦侵犯企业和企业家合法权益的网络信息内容乱象，通过压实网站平台主体责任，规范网站平台受理处置涉企信息举报工作，重点整治无事实依据凭空抹黑诋毁企业和企业家形象声誉、炮制传播虚假不实

信息、敲诈勒索谋取非法利益、干扰企业正常生产经营秩序和恶意炒作涉企公开信息等问题。

各地网信办要指导督促属地网站平台对照专项行动目标任务，加强信息管理，深入清理存量涉企侵权信息，强化热搜榜单等重点环节管理，严格要求相关账号、MCN机构不得炒作营销涉企侵权信息。中央网信办鼓励支持企业和企业家依法维护自身权益，对“顶风作案”、情节严重的网站平台和账号严格依法处罚，对各类典型案例予以公开曝光，切实营造良好的营商网络环境。（来源：网信中国）

3. 广东佛山市委网信办启动公共服务领域网络和数据安全专项行动

3月18日消息，中共佛山市委网信办于近日印发《佛山市公共服务领域网络和数据安全专项行动工作方案》。从即日起，全市将开展七大网络安全风险隐患排查工作，进一步完善佛山市公共服务领域网络和数据安全保障体系建设。

专项行动检查范围为全市党政部门、社会组织或国有企业通过信息化手段以满足群众各项公共服务活动需求所自行或委托建设的信息系统，包括但不限于公共教育、医疗卫生、劳动就业、养老托育、社会保险、社会救助、社会福利、文化旅游、体育健身、住房保障和物业服务等方面。其中，对具有运行不间断要求的、群众个人可直接进行在线业务登记或办理的、存储50万以上个人信息或1万以上个人敏感信息的系统进行重点检查。

专项行动将重点开展七大工作，包括网络和数据安全自查、远程技术检测、数据泄露监测、现场安全检查、网络安全意识培训、隐患全面整改、实战攻防演练复盘等，通过“自查自纠+专项检查+复盘整治+宣传培训”等多项措施，织牢织密数据安全保障制度，全面防控数据安全风险隐患。

其中，网络和数据安全自查清单对照行业规范进行制定，包括责任落实、日常管理、安全防护、应急工作、教育培训、技术产品使用、技术检测、信息技术外包等八大方面80多个安全控制点，相关单位可通过对照清单查漏补缺，进一步落实公共数据分类分级、脱敏、风险评估、监测预警、应急处置、安全审查等安全管理制度。

此外，市委网信办还将组织技术支持单位，对重要信息系统进行远程检测，集中排查各单位网络安全漏洞、隐患、问题和风险。对部分重点公共服务单位，还将开展安全保护现场检查，以督促相关单位提升网络安全防护、监测预警和应急处置能力。（来源：网信佛山）

4. 上海市网信办发布数据出境安全评估申报及个人信息出境标准合同备案工作实务问答（三）

3月27日，上海市网信办结合国家网信办发布的《促进和规范数据跨境流动规定》《数据出境安全评估申报指南（第二版）》《个人信息出境标准合同备案指南（第二版）》，发布数据出境安全评估申报及个人信息出境标准合同备案工作实务问答（三），对如何提交材料、申报材料变化、申报情形确认、免于申报情形、材料查验时限、咨询方式等九个问题进行解答。

其中，对于数据处理者如何提交评估或备案材料，问答指出应通过数据出境申报系统提交材料，系统网址为 https://sjcj.cac.gov.cn。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的，可以采用线下方式申报。已经通过线下方式提交安全评估申报、标准合同备案材料的，不需要通过数据出境申报系统进行重新提交。

对于申报材料要求的变化，问答指出《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》对需要提交的数据出境安全评估申报表、数据出境风险自评估报告及个人信息保护影响评估报告等材料进行了优化。请数据处理者特别注意对于申报表、评估报告的格式要求，包括字体、段落、页面设置等。

5. 重庆市江北区网信办就网络安全问题约谈属地某公司负责人

3 月 11 日消息，重庆市江北区网信办近日接市网信办移交线索，辖区内某公司数据库存在未授权高危安全漏洞，有数据泄露现象。江北区网信办联合区公安分局依法对该公司开展调查和技术取证，并于日前对该公司负责人进行执法约谈，作出行政警告处罚。

根据《网络安全法》等法律法规，江北区网信办在约谈中深刻剖析问题根源，阐明可能导致的危害和后果，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。目前，该高危漏洞已修复。（来源：网信重庆）

6. 重庆市荣昌区网信办就网络安全问题约谈属地某公司负责人

3 月 18 日消息，重庆市荣昌区网信办联合区公安局、荣昌高新区管委会依法对属地某公司负责人进行约谈。接市网信办移交线索，该公司的工控系统、OA 系统在短期内连续被通报弱口令漏洞。荣昌区网信办高度重视，迅速开展相关处置工作。

根据《网络安全法》等法律法规，荣昌区网信办在约谈中深刻剖析问题根源，阐明可能导致的危害和后果，责成该公司严格落实网络安全主体责任，切实抓好整改落实，定期开展安全培训，提升网络安全意识，加大网络安全投入，提升网络安全防护能力。荣昌区公安局现场出具限期整改通知书，要求该公司限期整改，并按时反馈整改情况。（来源：网信重庆）

（三）通信管理部门治理实践

1. 工信部、多地通管局通报侵害用户权益行为的 APP

（1）工信部

3 月 14 日，工信部通报 2024 年第 2 批，总第 37 批侵害用户权益行为的 APP（SDK）。通报指出，工信部组织第三方检测机构对用户反映突出的“摇一摇”乱跳转、信息窗口“关不掉”以及违规收集使用个人信息等焦点问题进行检查，共发现怪兽充电、途虎养车等 62 款 APP 及 SDK 存在上述侵害用户权益行为，予以通报。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）安徽省通信管理局

3月14日,安徽省通信管理局通报2024年第2批侵害用户权益的APP。通报指出，安徽省通信管理局近日对省内APP进行拨测检查，检测发现27款APP存在违法违规收集使用个人信息的问题，并已于2月22日对上述违规APP企业下达责令改正通知书,要求限期完成整改工作。截至3月14日，尚有8款APP未完成问题整改，涉及违规收集个人信息，超范围收集个人信息，强制、频繁、过度索取权限，频繁自启动和关联启动等多类问题。相关APP企业应在2024年3月20日前落实整改要求，逾期不整改的，安徽省通信管理局将依法依规组织开展相关处置工作。

（3）浙江省通信管理局

3月27日，浙江省通信管理局通报2024年第2批27款侵害用户权益行为的APP。通报指出，浙江省通信管理局前期组织第三方检测机构对群众关注的实用工具、用车服务、网络社区等类型APP进行检查，并书面要求违规APP开发运营者限期整改。截止3月27日，尚有今日速运司机端、卡帕奇体温等27款APP未按要求完成整改。上述APP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、APP强制频繁过度索取权限等问题。上述APP开发运营者应在4月4日前完成整改落实工作，整改落实不到位的，该局将视情采取下架、关停、行政处罚等措施。

（4）江西省通信管理局

3月27日,江西省通信管理局通报2024年第一批侵害用户权益行为的APP。通报指出，江西省通信管理局前期对省内部分APP进行拨测检查，共检测到7款APP存在违法违规收集使用个人信息的问题,并对上述违规APP下达《违法违规APP处置通知》,要求限期完成整改工作。截至3月27日，

尚有珍汇淘、咕鸽运动等 5 款 APP 未按要求完成整改。上述 APP 涉及违规使用个人信息、强制频繁过度索取权限等问题。上述 APP 企业应在 4 月 7 日前落实整改。逾期不整改的，该局将依法依规组织开展相关处置工作。

(5)广东省通信管理局

3 月 29 日，广东省通信管理局发布通报，下架 3 款侵害用户权益 APP。广东省通信管理局持续开展 APP 隐私合规和数据安全专项整治行动，截至规定时限，经核查复检，尚有 3 款 APP 未完成问题整改，分别是 e 路相伴、叮叮抓娃娃、芭乐视频，涉及违规收集个人信息、APP 频繁自启动和关联启动等多类问题。

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。相关应用商店应立即组织对名单中的 APP 进行下架处理，并举一反三，排查反复出现问题的 APP 开发运营者，严格落实分发平台主体责任，把好上架审核关。广东省通信管理局将对通报 APP 持续跟踪，视情况进一步采取断开网络、行政处罚、纳入电信业务经营不良名单等后续处理措施。（来源：安徽省、浙江省、江西省、广东省通信管理局、工信部）

2. 上海市通信管理局开展“铸盾车联”2024 年车联网网络和数据安全专项行动

3 月 6 日，上海市通信管理局印发通知，决定开展“铸盾车联”2024 年车联网网络和数据安全专项行动。

专项行动重点对象为在本市生产、销售智能网联汽车产品的生产企业（含智能网联汽车生产企业、具有智能网联功能的车载终端软硬件生产企

业，不含代理销售企业），在本市运营车联网相关平台的服务企业（含车联网服务平台运营商、车载应用平台运营商、OTA 升级服务提供商、导航系统服务提供商、电子地图服务提供商、车载信息应用服务提供商、车联网卡服务提供商等），本市车联网网络设施和车路协同设施运营企业以及自动驾驶功能产品和解决方案服务企业。

专项行动包括六项重点任务，分别是网络和数据安全主体责任、车联网网络设施和系统安全、智能网联汽车产品安全、车联网平台和应用服务安全、车联网数据安全、自动驾驶功能安全。其中，通知指出企业需跨主体共享车联网相关数据的，应对数据合作方的数据安全保护能力进行审核评估，并将拟共享数据的类型、规模、用途、提供方式、提供周期、合作方主体等情况以及内部审核评估记录向市通信管理局报备，报备内容不包含数据本身。

专项行动包括五项保障措施，分别是强化政策宣贯、强化责任落实、强化技术保障、强化实战检验以及强化标准创新。（来源：上海通信圈）

3. 广东省通信管理局开展 2024 年广东省电信和互联网行业网络数据安全和应用合规行政检查

3 月 25 日，广东省通信管理局印发通知，决定开展 2024 年广东省电信和互联网行业网络数据安全和应用合规行政检查。

通知指出，检查对象是相关企业建设运营的网络、系统、平台、应用、业务，重点是电信和互联网行业关键信息基础设施和重要网络单元及承载的信息系统。将主要开展以下六方面检查：安全合规管理制度机制、网络

安全防护检查、数据安全和个人信息保护检查、市场秩序和用户权益保护工作检查、互联网基础资源合规检查、反诈义务落实情况检查。

通知强调,广东省通信管理局将结合监管重点和2024年相关“双随机”检查工作,并委托支撑单位和专业技术机构进行远程监测/检测、现场检查。对检查过程中发现的问题，各单位要高度重视，认真及时整改并向广东省通信管理局报告整改情况。发现存在违反法律法规行为、问题逾期不改正或导致危害网络与数据安全等严重后果的，广东省通信管理局将依法依规给予行政处罚并纳入不良名单和失信名单。（来源：广东信息通信业）

（四）其他部门治理实践

1. 最高检发布《公益诉讼检察工作白皮书（2023）》

3月9日，最高检发布《公益诉讼检察工作白皮书（2023）》，聚焦网络时代公民个人信息保护更高需求，扎实开展个人信息保护和反电信网络诈骗领域公益诉讼。

白皮书指出，2023年检察机关加强个人信息保护。最高检与工信、网信部门建立个人信息保护工作联系、协作机制。上海市检察院立案办理的督促整治手机APP侵害公民个人信息案，督促相关职能部门积极整改并开展专项检查，取得良好监督效果。山东省青岛市市北区检察院对跨境“裸聊”恶势力非法获取公民个人信息1600余万条违法行为提起刑事附带民事公益诉讼，在有效保护个人信息的同时推动青岛市反诈平台建设。内蒙古自治区乌兰浩特市检察院运用公益诉讼大数据应用平台筛查和实地走访等

方式，累计排查涉及不当公开的个人敏感信息 7 万余条，督促 14 个乡镇街道及 2 家机关单位规范政务信息公开。

白皮书强调，2023 年检察机关着力协同防治电信网络诈骗。最高检与公安、工信部门就电信网络诈骗领域开展密切协作配合，针对源头风险防范充分发挥公益诉讼独特职能作用，督促相关行政主管部门依法履职，促进诉源治理。江苏省南通市检察院针对“空壳公司”批量申请固话诈骗问题，制发检察建议，督促行政机关加强入网审核，及时清退状态异常的市场主体。贵州省贵阳市南明区检察院针对涉电信网络诈骗“空壳公司”营业执照和对公账户监管不到位公益损害问题，督促市场主体登记机关落实监管责任，依法对涉案企业撤销登记，减少涉电信网络诈骗犯罪滋生土壤。（来源：最高人民检察院）

2. 中消协发布 2023 年“全国消费维权十大典型司法案例”，涉个人信息保护纠纷案

3 月 15 日，中消协发布 2023 年“全国消费维权十大典型司法案例”，涉及一例个人信息保护纠纷案件，即孔某诉北京南锣肥猫餐饮有限公司个人信息保护纠纷案——“变相强制”消费者扫码点餐获取其个人信息构成侵权。

本案中，北京南锣肥猫餐饮有限公司（以下简称被告）推出手机扫码点餐服务，要求消费者使用微信扫描二维码并关注公众号进行线上点餐。若不同意授权获取个人信息，则无法使用该服务。2021 年 7 月，孔某在被告门店用餐时选择了手机扫码点餐，并在此过程中成为公司会员。后来孔

某取消关注公众号，发现个人信息仍被保留在被告处，无法自行删除。孔某因此将被告告上法庭，要求停止侵害个人信息权益、告知信息处理情况、赔礼道歉并赔偿相关损失。

2023 年 10 月 20 日，北京市第三中级人民法院作出终审，依据《民法典》《消费者权益保护法》《个人信息保护法》相关条款，判决被告向原告书面告知处理孔某个人信息的范围、方式，向原告进行书面赔礼道歉，赔偿原告公证费五千元。

中消协表示，在点餐方式上，消费者享有自主选择权，经营者不得误导和变相强制消费者使用扫码点餐。餐饮经营者收集个人信息应与当前餐饮消费场景密切相关，不得在消费者登录、点餐、取号、加菜、结账等环节设置不必要程序或环节，诱导索取与餐饮服务无关的个人信息。消费者对其个人信息处理享有知情权，有权要求经营者公示扫码点餐收集消费者个人信息的目的、方式和范围。消费者发现经营者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权要求信息处理者及时删除。（来源：中国消费者协会）

3. 国家计算机病毒应急处理中心公开监测发现 14 款违规移动应用

3 月 21 日消息，国家计算机病毒应急处理中心近日通过联网监测发现“晁藤”“天津农商银行”等 14 款移动 App 存在隐私不合规行为。

具体的违规行为包括但不限于：（1）无隐私政策；（2）隐私政策未逐一列出 App 收集使用个人信息的目的、方式、范围等；（3）App 客户端向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式

向第三方提供个人信息，未经过用户同意，未做匿名化处理；个人信息处理者向其他个人信息处理者提供其处理的个人信息，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，未取得个人的单独同意；（4）未提供有效的更正、删除个人信息及注销用户账号功能，或为更正、删除个人信息或注销用户账号设置不必要或不合理条件；（5）未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内受理并处理。个人信息处理者未建立便捷的个人行使权利的申请受理和处理机制；（6）App 频繁自启动和关联启动。（来源：国家计算机病毒应急处理中心）

4. 金融监管总局办公厅下发《关于银行保险机构侵害个人信息权益乱象专项整治发现主要问题的通报》

3 月 26 日消息，金融监管总局办公厅近日下发《关于银行保险机构侵害个人信息权益乱象专项整治发现主要问题的通报》。通报称：“全行业个人信息保护工作水平得到有效提升”，但“从目前投诉督查、举报调查、监管评价等工作中反映的问题来看，银行保险机构侵害个人信息权益的行为仍时有发生，内部管控还存在短板弱项和风险隐患”。

2022 年 8 月，监管部门组织开展银行保险机构侵害个人信息权益乱象专项整治，以银行保险机构自查为主，监管部门适时开展抽查和督导，确保全面覆盖与消费者个人信息处理相关的业务环节、员工行为和管理流程。

通报指出，专项整治全面深入检视银行保险机构个人信息处理工作各类流程，在个人信息处理具体执行层面发现大量问题或隐患。机构自查共

发现问题15.42万个，涉及合同协议、声明等2.63万份。监管部门开展监管抽查共发现问题5561个，涉及机构1985家次、员工3566人，影响消费者1556万人次。

根据通报，金融机构在个人信息保护方面主要存在五大问题，分别是：（1）个人信息收集方面存在强制同意、扩大授权、笼统授权等问题；（2）个人信息存储和传输方面存在电子数据管理混乱、纸质材料管理不严、传输方式不安全等问题；（3）个人信息查询和使用方面存在违规查询账户信息、不当使用客户信息等问题；（4）个人信息提供和删除方面存在未经授权对外提供、未及时删除等问题；（5）个人信息第三方合作方面存在对外合作机构管控失效等问题。

针对专项整治发现的主要问题，金融监管总局要求从提高思想认识，落实主体责任；聚焦风险短板，健全长效机制；层层压实责任，强化内控管理；加强教育培训，树牢消保理念四方面加强工作。（来源：中国消费网、北京商报）

5. 上海市市场监管局公布四起个人信息保护违法典型案例

3月14日，上海市市场监管局公布四起个人信息保护违法典型案例。

案例一：上海洳娟实业有限公司未经消费者同意擅用人脸识别设备收集个人信息案

2023年3月24日，普陀区市场监督管理局根据相关线索对当事人未经消费者同意擅用人脸识别设备收集个人信息进行立案调查。经查，当事人出于防范盗窃等目的，于2021年4月委托某信息科技公司在超市大门位置

安装了一台具有人脸识别功能的摄像头，对进入超市人员进行拍照、人脸识别分析比对，相关数据存储于超市监控系统硬盘内，定期自动覆盖。该公司在经营过程中使用具有人脸识别功能的摄像头收集人脸数据图片未经消费者同意，且经营现场无明示收集脸部信息的目的、方式、范围和收集规则等，侵害了消费者个人信息依法得到保护的权利。

当事人未经消费者同意擅用人脸识别设备收集个人信息的行为，违反《消费者权益保护法》第二十九条第一款的规定，根据《消费者权益保护法》第五十六条第一款第(九)项之规定，普陀区市场监督管理局对当事人作出警告并罚款 3000 元的行政处罚。

案例二：上海中原物业顾问有限公司侵害消费者个人信息依法得到保护的权利案

杨浦区市场监督管理局执法人员根据相关线索对上海中原物业顾问有限公司的下属分公司进行执法检查。经查，当事人办公电脑系统内存在被泄露的房源信息且未取得房主授权委托，上述信息系当事人从其他房产中介（已另案查处）处获得，当事人未经被侵犯信息的房源信息主同意，非法收集、使用消费者个人信息，并拨打滋扰电话，严重影响房源信息主的日常工作和生活。

当事人上述行为违反《上海市消费者权益保护条例》第二十一条第一款的规定，杨浦区市场监督管理局依据《上海市消费者权益保护条例》第七十四条和《消费者权益保护法》第五十六条第一款第（九）项的规定，作出罚款 60000 元的行政处罚。

案例三：上海秦汉胡同教育培训有限公司青浦第一分公司侵害消费者个人信息依法得到保护的权利案

2023 年 7 月 24 日，青浦区市场监督管理局执法人员在对当事人经营场所检查时发现，当事人电脑中存储个人信息内含姓名、年龄、电话以及联系记录若干条，当事人无法提供上述个人信息的合法来源。在当事人的业务操作系统中还发现有多条挂断、拒接、打不通但仍多次拨打消费者电话的记录，以及部分消费者明确表示拒绝，当事人员工仍向其联系业务的记录。

当事人在未取得消费者同意，同时也未向消费者明示收集信息的目的、方式和范围的情况下，通过与同行交换等途径收集大量消费者个人信息，以及消费者明确表示拒绝，仍向其发送商业性信息的行为违反《消费者权益保护法》第二十九条第一款、第三款的规定，青浦区市场监督管理局依据《消费者权益保护法》第五十六条第一款第（九）项的规定，对当事人作出罚款 10000 元的行政处罚。

案例四：上海那嘎的餐饮管理有限公司闵行分公司非法处理个人信息案

闵行区市场监督管理局接消费者举报，反映其在当事人处就餐后，莫名接受到电话和短信骚扰，怀疑就餐时被商家违法收集消费者数据信息。经调查发现，当事人通过设置桌面二维码扫码点单的方式为来店消费者提供点餐服务。顾客扫描桌面二维码后跳转到当事人企业公众号授权服务页面，通过点击页面中《隐私权政策》，页面无法弹出个人信息隐私权收集详细内容，相关跳转页面中个人信息收集种类、处理目的均未告知消费者。

当事人通过上述功能，收集消费者手机号的个人信息，当事人为来店顾客提供扫码点餐的方式，本意为方便来店顾客提供点餐服务，但顾客个人手机号作为个人信息，与点餐服务并不直接相关，不应在使用上述服务过程中被收集、使用。

当事人的上述行为违反《个人信息保护法》第六条第一款、第二款以及第十七条第一款第（二）项的规定，构成非法处理个人信息的行为。闵行区市场监督管理局依据《个人信息保护法》第六十六条第一款的规定，依法对当事人处以警告的处罚。（来源：上海市场监管）

6. 广东省政务服务和数据管理局发布《2023 广东省数字政府网络安全指数评估报告》

3 月 16 日，广东省政务服务和数据管理局发布《2023 广东省数字政府网络安全指数评估报告》，报告显示，2023 年广东省数字政府网络安全指数为 73.63，比 2022 年提高了 14.71%，比 2020 年提高了 36.83%；网络安全能力等级达到受控级（C）及以上的地市增加至 20 个，全省绝大多数地市数字政府建立了安全制度规范及配套技术措施。

在各地市的表现中，深圳市连续 4 年评估保持着领先，初步具备了网络安全综合防御能力；中山市进步显著，从启动级（D）跃升至完善级（A），网络安全综合防御能力达到第一梯队水平。此外，广州、珠海、佛山、江门、茂名、惠州、东莞等地市也排名靠前，初步具备了网络安全主动防御能力；茂名、惠州、揭阳、梅州、湛江等 5 个地市进步明显。

基于2023年广东省数字政府网络安全指数，报告强调要全面落实网络安全工作责任制，大力加强数字政府本质安全保障体系建设，进一步强化重要数据和个人信息保护，建设良好的网络安全生态环境，有效防范网络安全威胁，有力处置网络安全事件，为数字经济保驾护航。（来源：网信广东）

境外前沿观察：月度速览十则

导读：3 月，澳大利亚网络与基础设施安全中心发布两份针对国家重要系统的网络安全指南《强化网络安全义务：事件响应计划》《强化网络安全义务：网络安全演习》。美国 CISA 就拟议规则《<关键基础设施网络事件报告法>报告要求》公开征求意见，拟细化 2022 年《关键基础设施网络事件报告法》提出的关键基础设施运营组织 72 小时报告重大网络安全事件，以及 24 小时报告勒索攻击赎金支付情况的要求。该法授权 CISA 制定具体的细化落实规则。爱尔兰加尔达国家网络犯罪局发布《网络犯罪风险和防治建议》，就如何防范恶意软件、网络钓鱼和数据泄露提出建议。

英国信息专员办公室发布谴责，指控英国多佛、肯特警察局多名警务人员利用 WhatsApp、Telegram 等向国内外警务人员共享犯罪车辆信息，且这些信息在没有适当安全保障措施的情况下被转发给不同人员。意大利数据保护机构宣布对 OpenAI 公司新模型 Sora 展开调查，重点关注算法训练方式、训练数据范围、是否收集敏感个人数据、训练数据来源等方面。法国劳动局发生大规模数据泄露，约 4300 万公民个人数据被窃取。

关键词：重要系统网络安全保护、关键基础设施网络事件报告、人工智能执法、数据泄露

1. 澳大利亚 CISC 发布两份针对国家重要系统的网络安全指南

3 月 11 日，澳大利亚网络与基础设施安全中心（CISC）发布两份针对国家重要系统的网络安全指南。一是《强化网络安全义务：事件响应计划》概述事件响应计划要点，包括：（1）与网络安全态势和风险管理政策保持一致，确保考虑到最可能的网络攻击场景和要保护的最关键业务资产；（2）具备足够的网络安全事件识别能力，可在必要时触发事件响应计划；（3）网络安全事件响应的关键是确保决策者及时作出关键决策，事件响应计划应描述事件关键升级点及其触发因素。二是《强化网络安全义务：网络安全演习》指出，演习可通过不同形式进行，包括：（1）讨论和桌面演习，团队或个人讨论拟如何应对网络安全事件并探讨事件期间的相关安全问题；（2）操作、功能练习，团队或个人模拟实施风险管理计划、流程和程序，预演网络安全事件发生时的各自角色和职责。（来源：澳大利亚 CISC）

2. 爱尔兰加尔达国家网络犯罪局发布《网络犯罪风险和防治建议》

3 月 13 日，爱尔兰加尔达国家网络犯罪局（GNCCB）发布《网络犯罪风险和防治建议》，提供网络犯罪风险信息和网络犯罪预防措施。要点包括：（1）恶意软件。恶意软件可通过多种方式感染计算机网络，共同点是都在一定程度上涉及人的因素，包括访问感染的电子邮件附件、点击导致网站感染的链接、从未知来源处下载文件到外部设备后将其连接到工作系统等，系统所有者和用户可通过防病毒软件、防火墙、备份等方式进行防范；（2）网络钓鱼。网络钓鱼通常涉及看似来自银行、政府或供应商等受信任来源

的伪造电子邮件，实际上这些机构不会要求通过点击链接提供登录凭据。若收到此类邮件或消息，系统所有者和用户应对内容和发件人提出质疑；（3）数据泄露。未定期更新系统、用户访问控制政策执行不力等因素都可能导致数据泄漏，公司应制定并定期测试数据安全政策，更新系统使用程序和指南，及时修补、备份并更新系统，对所有员工进行数据安全风险和治理培训，定期测试培训效果。（来源：爱尔兰加尔达国家网络犯罪局）

3. 美国 CISA 就拟议规则《<关键基础设施网络事件报告法>报告要求》公开征求意见

3 月 27 日，美国网络安全和基础设施安全局（CISA）就拟议规则《<关键基础设施网络事件报告法>报告要求》公开征求意见。拟议规则基于美国总统拜登 2022 年 3 月签署的《关键基础设施网络事件报告法》，是美国联邦政府首次提出的一套跨关键基础设施部门的全面性网络安全要求。拟议规则要点包括：（1）72 小时报告义务。拥有和运营关键基础设施的组织应在 72 小时内报告重大网络安全事件，在 24 小时内报告勒索攻击赎金支付情况；（2）适用范围。适用于任何拥有或运营美国政府认定为关键基础设施的所有者，以及不运营关键基础设施，但系统可能对特定行业关键基础设施造成影响的组织，如服务提供商；（3）重大网络安全事件认定。涉及非法入侵系统并导致停机、运营严重受损等影响的攻击活动将触发报告要求的门槛，但并非所有网络安全事件都会触发报告义务，如由第三方服务提供商在服务器配置中出现的一些错误，若未造成严重停机，则无需报告，渗透测试等也不在监管范围内。（来源：美国 CISA）

4. 美国 FBI 互联网犯罪投诉中心发布《2023 年网络犯罪报告》

3 月 6 日，美国 FBI 互联网犯罪投诉中心（IC3）发布《2023 年网络犯罪报告》。报告显示，2023 年 IC3 接到来自美国公众的 880418 起网络犯罪投诉，潜在损失超过 125 亿美元。与 2022 年相比，投诉数量增加近 10%，损失增加 22%。据统计，2023 年，投资诈骗再次成为 IC3 追踪的犯罪中损失最高的类型。投资诈骗造成的损失从 2022 年的 33.1 亿美元增至 2023 年的45.7亿美元,增长38%;第二高损失的犯罪类型是电子邮件业务诈骗(BEC),共有 21489 宗投诉，损失额达 29 亿美元；技术诈骗是 IC3 追踪的第三大损失犯罪类型。此外，勒索软件攻击影响力凸显，比 2022 年增长 18%，造成的损失增长 74%，从 3430 万美元增至 5960 万美元。网络犯罪分子继续调整战术，FBI 已经观察到新的勒索攻击趋势，如对同一受害者部署多种勒索软件变种、使用数据销毁战术提升谈判压力等。（来源：美国 FBI）

5. 意大利数据保护局对 OpenAI 新模型 Sora 展开调查

3 月 8 日，意大利数据保护机构（Garante）宣布对 OpenAI 公司新模型 Sora 展开调查。Sora 是一款可根据文本指令生成动态、现实和富有想象力的视频的人工智能模型。Garante 指出，Sora 可能对欧盟和意大利用户个人数据处理产生影响，要求 OpenAI 在 20 日内说明用户现在是否可以访问 Sora，以及是否会向欧盟和意大利的用户提供 Sora 服务。OpenAI 还需提供的信息包括：（1）算法训练方式；（2）训练数据范围，是否涉及个人数据；（3）公司是否收集敏感个人数据，包括宗教信仰、政治观点、遗传数据、健康和性生活数据等；（4）训练数据来源。（来源：意大利 Garante）

6. 因有害内容检查不力，意大利对 TikTok 处以 1000 万欧元罚款

3 月 15 日消息，意大利竞争监管机构表示，由于社交媒体巨头 TikTok 可能存在对年轻或弱势用户有害内容检查不力的情况，将对 TikTok 的三个部门处以总计 1000 万欧元的罚款。最近欧洲未成年人在 TikTok 掀起“疤痕挑战”热潮，用力捏或拧自己脸颊，创造一些明显的红色疤痕并拍摄下来。意大利竞争监管机构表示这些具备潜在安全危害的视频是通过分析算法传播的，TikTok 没有采取足够的措施防范此类内容传播，也没有完全遵守相关指导方针，无法向用户确保该平台是一个安全空间。（来源：意大利竞争监管机构）

7. 英国信息专员办公室抨击警务人员使用 WhatsApp、Telegram 共享犯罪车辆信息

3 月 15 日，英国信息专员办公室（ICO）发布谴责，指控英国多佛、肯特警察局多名警务人员利用 WhatsApp、Telegram 等向国内外警务人员共享犯罪车辆信息，且这些信息在没有适当安全保障措施的情况下被转发给不同人员。ICO 就警务人员使用社交媒体提出建议，要求地方警察总监采取以下措施：（1）定期审查警察局的信息和通信技术使用政策，将个人设备使用与审批程序纳入考量，指导警务人员数据保护合规使用；（2）定期审查并发布更新政策、指南、程序，确保所有警务人员阅读并理解相关要求；（3）定期审查数据保护培训内容，以案释法；（4）为警务人员社交媒体使用提供指导和培训。（来源：英国 ICO）

8. 美国国防部通过赏金计划在系统中发现 5 万多个漏洞

3 月 18 日消息，美国国防部表示自 2016 年 11 月在 HackerOne 推出首个白帽子漏洞赏金计划“黑进五角大楼”以来，已通过漏洞披露项目收到 5 万多个安全漏洞的相关信息。国防部将继续与 HackerOne、Bugcrowd 和 Synack 合作运行独立的漏洞赏金计划，涵盖空军、海军陆战队、陆军等系统资产。（来源：美国国防部）

9. 法国劳动局泄露 4300 万公民个人数据

3 月 13 日，法国劳动局发表声明，承认发生大规模数据泄露，预计 4300 万公民的个人数据被窃取。目前在法国劳动局注册的求职者、过去 20 年内注册的求职者以及未在求职者名单上注册但在候选名单上的人员的个人数据可能会被非法披露和利用。被非法窃取的数据类型包括姓名、出生日期、社会保障号码、劳动局标识符、电子邮件地址、邮政地址和电话号码。根据 GDPR 规定，法国劳动局已向法国数据保护监管机构报告本次数据泄露。（来源：法国劳动局）

10. 微软旗下 GitHub 平台遭遇严重供应链投毒攻击

3 月 27 日消息，有黑客近日针对 Discord Top.gg 的 GitHub 账户发起供应链攻击，导致用户账户密码、登录凭证等敏感数据被窃取，也影响到大量开发人员。GitHub 是一个在线软件源代码托管服务平台，使用 Git 作为版本控制软件，2018 年 GitHub 被微软公司收购。据悉，此次攻击黑客使用多种策略、技术和程序，包括窃取浏览器 cookie 接管账户、通过验证提

交恶意代码、建立自定义 Python 镜像、向 PyPI 注册表发布恶意软件包等。

（来源：The Hacker News）

行业前沿观察一：2023“安满周”在京开幕 公布 2023 年度网民网络安全感满意度指数及十大主要发现、网信办开展“清朗·整治‘自媒体’无底线博流量”专项行动、中央网信办等三部门印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》

导读：2023“安满周”以习近平总书记关于“网络安全为人民、网络安全靠人民”的重要讲话精神为指引，以“你我携手——构筑数字时代网络安全新防线”为主题，于 2024 年 4 月 15-19 日在全国线上线下同步举办，于 4 月 16 日在北京正式举行开幕式，集中发布 2023 年调查成果（全国总报告、各大专题报告、部分省市区域报告等系列调查报告），聚焦于“发现问题，指出问题，给出解决方案”，向国家和有关部门开展互联网治理与监管提供详实的网情民意数据，助力提升网民群众获得感、幸福感、安全感和满意度，服务国家网络安全和信息化事业高质量发展。4 月 16 日上午，2023 网民网络安全感满意度报告发布周（简称 2023“安满周”）开幕式暨《2023 年全国网民网络安全感满意度调查统计总报告》发布会在北京成功举行。

中央网信办日前印发通知，在全国范围内开展为期两个月的“清朗·整治‘自媒体’无底线博流量”专项行动，聚焦“自媒体”无底线造热点蹭热点，制造以假乱真、虚实混杂的“信息陷阱”等突出问题，从严整治漠视公共利益、违背公序良俗、扰乱公共秩序，为了流量不择手段、丧失底线的“自媒体”。

日前，中央网信办、国家发展改革委、工业和信息化部联合印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》（以下简称《工作安排》）。通知要求，坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大精神，完整、准确、全面贯彻新发展理念，以全面推进 IPv6 技术创新与融合应用为主线，着力破解瓶颈短板，完善技术产业生态，打造创新引领、高效协同的自驱性发展态势，为建设网络强国、数字中国提供有力支撑。

关键词：安满周、2023 年全国网民网络安全感满意度调查统计总报告、中央网信办、数据泄露、IPv6、网络强国

1. 2023“安满周”在京开幕 公布 2023 年度网民网络安全感满意度指数及十大主要发现

4 月 16 日上午，2023 网民网络安全感满意度报告发布周（简称 2023“安满周”）开幕式暨《2023 年全国网民网络安全感满意度调查统计总报告》发布会在北京成功举行。

大会上，由中国工程院院士孔志印作为总报告发布人，中国工程院院士沈昌祥作总结演讲，面向全社会线上线下同步公布 2023 年度我国网民网络安全感满意度指数、10 大主要发现、7 个主要结论，以及 2023 年我国网络空间安全治理主要成效和存在的主要问题等重要内容。北京市人力资源和社会保障局发布《关于增设网络空间安全职称评审专业的通告》，北京人社局处长刘洪朗为北京网络空间安全协会颁发“北京市职称评审服务机构”牌匾，为沈昌祥、方滨兴、孔志印三位中国工程院院士颁发职称评审委员会主任委员证书。方滨兴院士作主任委员讲话。

2023“安满周”以习近平总书记关于“网络安全为人民、网络安全靠人民”的重要讲话精神为指引，以“你我携手——构筑数字时代网络安全新防线”为主题，于 2024 年 4 月 15-19 日在全国线上线下同步举办，于 4 月 16 日在北京正式举行开幕式，集中发布 2023 年调查成果（全国总报告、各大专题报告、部分省市区域报告等系列调查报告），聚焦于“发现问题，指出问题，给出解决方案”，向国家和有关部门开展互联网治理与监管提

供详实的网情民意数据，助力提升网民群众获得感、幸福感、安全感和满意度，服务国家网络安全和信息化事业高质量发展。

2023“安满周”以北京为主会场，于 4 月 16 日至 18 日线上线下举办“2023 安满周·北京香山会议”，期间举行开幕式、全国总报告发布会、6 场专题报告发布会、10 多场区域报告发布会以及第三届网络志愿服务大会、商用密码创新发展研讨会、网络诚信建设研讨会、北京信创大赛筹备会、网安联年会等系列活动。同时在上海、广州、郑州、嘉兴乌镇设置线上线下分会场，于 15 日至 19 日期间共发布 5 份专题报告。此外，还将分别在深圳和厦门由相关部委分别举办的国家级大会上，重磅发布 2 份专题报告。2023“安满周”由网安联全国 135 家网络社会组织及相关机构发起，网安联秘书处牵头组织，网民网络安全感满意度调查活动组委会主办，广东新兴国家网络安全和信息化发展研究院承办，中国网络空间安全协会特别支持，中国计算机学会计算机安全专业委员会、中国教育技术协会网络安全专委会担任战略合作单位。中国工程院院士沈昌祥、方滨兴、孔志印出席活动并发表内容。

基于 2023 年全国各调查活动发起单位、支持单位及志愿服务站（队）采集到的 224.7269 万份样本数据，调查活动组委会联合公安部第三研究所网络安全法律研究中心、复旦大学网络空间国际治理研究基地、上海交通大学信息内容分析技术国家工程研究中心、公安部网络安全等级保护评估中心、乌镇数字文明研究院、浙江大学国际传播研究中心、互联网实验室、广州大学网络空间安全学院、郑州大学网络空间安全学院、广州华南检验

检测中心、奇安信集团、腾讯企鹅有调、粤港澳网络空间治理创新研究院等十多所专业机构和院校及部分网安联成员单位等学术合作单位，密集发布2023年调查活动各类型成果报告。

大会由公安部网络安全保卫局原二级巡视员唐前临主持。中国工程院院士沈昌祥出席大会并作总结演讲。中国工程院院士方滨兴出席大会并作职称评审主任委员讲话。北京市人社局党组成员、副局长荀连忠因公委托本单位副处长黄凯替代出席大会，并发布增设北京网安职称通告。调查活动组委会主任、公安部第一、三研究所原所长严明作组委会领导致辞，调查活动组委会副主任、公安部网络安全保卫局原常务副局长、北京网络行业协会会长袁旭阳及调查活动组委会副主任兼秘书长、北京网络空间安全协会理事长黄丽玲，代表主办单位致辞。教育部教育管理信息中心副主任、中国教育技术协会副会长曾德华，中国网络空间安全协会秘书长郝晓伟作为合作单位领导出席大会并致辞。

公安部科技信息化局原副局长、一级巡视员赵林，密码科技国家工程研究中心副主任封涛，中国科学院信息工程研究所教授级高工、博士生导师查达仁，北京市人力资源和社会保障局处长刘洪朗，北京市民政局处长唐植辉等领导出席大会。全国各地2023调查活动发起单位、部分省市网安协会的领导代表和志愿服务团队代表共400余人线下参会。

据《总报告》显示，2023年参与调查网民的网络安全感满意度指数为75.537，跨上75分台阶，为较好偏好的水平。2023年度网民网络安全感满意度评价明显上升，反映了前一年我国在网络空间安全治理成效显著。和

2022 年比较上升了 2.115，提升明显。从走势来看，2023 年网民满意度指数已经连续 5 年上升，指数走势良好，显示近年来网络空间治理总体状况持续好转，受到网民的肯定。

《总报告》经过对主问卷和各专题问卷调查数据的统计、汇总分析后，得出以下 10 大主要发现：一是网络安全治理成效显著，安全感满意度明显提升；二是网络法治建设稳步推进，社会参与共治持续加强；三是违法犯罪整治成效凸显，网民防范意识持续加强；第四大发现为网络诚信建设相关内容，将于相关大会详细公布；五是个人信息保护效果良好，政策法规普及任重道远；六是网购交易保障仍需加强，维权痛点变化应予重视；七是权益保护状况逐步提升，网络素质教育任重道远；八是平台监管力度仍需加强，企业自律推进效果提升；九是数字政务服务期望提质，网上办理体验有待改善；十是数字经济和 AI 应用浪潮，行业发展面临机遇挑战。

《总报告》通过对广大网民的上网行为、安全认知、网络安全态势、网络安全治理、治理成效评价、网络安全感受进行统计分析，得出以下 7 个主要结论：一是满意评价明显上升，网络安全治理成效显著；二是法治建设上新台阶，人民至上引领协同共治；三是精准打击措施有力，违法痛点治理取得突破；四是综合治理体系保障，权益保护落实质量提升；五是合规自律略有改善，平台监管力度期望提升；六是数字经济机遇涌现，创新赋能推动行业发展；七是人工智能风险挑战，扬长避短统筹安全发展。

同时，《总报告》数据显示各类网络违法犯罪的关注度都有所下降，反映了打击违法犯罪的工作取得成效，不法活动的总体遇见率降低，网民的警惕性与关注度也随之降低。

《总报告》由广东新兴国家网络安全和信息化发展研究院，基于全国224.7269万份调查样本编写而成。大会上，调查活动组委会副秘书长、广东新兴国家网络安全和信息化发展研究院总工程师高宁作报告解读。

结合《总报告》呈现的内容，沈昌祥院士作《按法律、战略、制度 营造清朗网络空间》总结演讲主旨报告，围绕“按法律构筑安全可信的清朗网络安全保障体系”“按战略打造可信计算 3.0 产业生态体系”“落实等保制度2.0 筑牢网络强国防线”三大点内容，向参会人员进行分析分享。

大会期间，同期举办《关于增设网络空间安全职称评审专业的通告》发布会。据现场了解，结合2023调查活动受访从业人员的人才培养等相关情况，为推进网络空间安全产业高质量发展，拓展北京网络空间安全领域专业技术人才职业发展通道，北京市人力资源和社会保障局批准增设“北京网络空间安全职称评审专业”，并授权北京网络空间安全协会成立“北京市工程技术系列(网络空间安全)专业职称评审委员会”。由北京市人社局聘请沈昌祥、方滨兴、孔志印三位中国工程院院士担任委员会主任委员，刘欣然研究员、查达仁教授级高工担任委员。

方滨兴院士作评审专家主任委员讲话，分享委员会专家的履职情况以及对申请职称的业内人士的要求等。

大会上还为调查活动专家委员会的专家颁发聘书、为2023调查活动专题报告撰写和发布承办单位颁发纪念牌匾，为2023年度调查活动优秀发起单位颁发表扬信等；同时进行了网安联·志愿服务队授权仪式，助力推进全国志愿服务事业向数字化、信息化转型升级。

与亿万网民同心而行，与国家网络安全同向而进。2023“安满周”汇聚百余位网络安全领域的主管部门领导、权威专家学者、行业精英、头部企业和社会组织的代表，以及数百位网络安全志愿者和线上参会的各界观众，共同见证系列重磅报告的发布，现场或云端一起对话网络安全，碰撞火花，启迪思想，探索方向。

其中，《互联网平台监管与企业自律专题报告》《网络购物安全权益保护专题报告》于4月15日在广州分会场成功发布；《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》《新技术挑战与网络安全专题报告》《数字经济发展和网络安全挑战专题报告》《特殊人群网络权益保护专题报告》于4月16日下午在“北京香山会议”发布；北京、辽宁、黑龙江、郑州等10多个省市的区域报告于4月17日在北京发布；《个人信息保护和数据安全专题报告》《遏制网络违法犯罪专题报告》于4月18日分别在嘉兴乌镇和郑州发布；《行业发展与科技创新专题报告》《数字政府服务与治理能力提升专题报告》于4月19日在上海线上发布。此外，《网络诚信建设专题报告》《网安联·全国大学生用网安全专题报告》将由相关单位分别于今年在深圳和厦门由相关部委举办的重要大会上发布。

2. 网信办开展“清朗·整治‘自媒体’无底线博流量”专项行动

中央网信办日前印发通知，在全国范围内开展为期两个月的“清朗·整治‘自媒体’无底线博流量”专项行动，聚焦“自媒体”无底线造热点蹭热点，制造以假乱真、虚实混杂的“信息陷阱”等突出问题，从严整治漠视公共利益、违背公序良俗、扰乱公共秩序，为了流量不择手段、丧失底线的“自媒体”。

通知原文：

各省、自治区、直辖市党委网信办，新疆生产建设兵团党委网信办：

按照 2024 年“清朗”系列专项行动计划安排，中央网信办自即日起，在全国范围内开展为期两个月的“清朗·整治‘自媒体’无底线博流量”专项行动。

一、工作目标

贯彻落实习近平总书记关于网络强国的重要思想，深入落实党的二十大精神，通过开展专项行动，遏制“自媒体”摆拍造假风，压缩无底线博流量行为空间，提升“自媒体”发布信息可信度。压紧压实网站平台信息内容管理主体责任，切断“毒流量”吸粉变现利益链，扩大优质信息内容触达范围，营造风清气正网络空间。

二、整治重点

聚焦“自媒体”无底线造热点蹭热点，制造以假乱真、虚实混杂的“信息陷阱”等突出问题，从严整治漠视公共利益、违背公序良俗、扰乱公共秩序，为了流量不择手段、丧失底线的“自媒体”。整治的重点问题如下：

1. 自导自演式造假。摆拍发布涉及国内外时事、社会民生等领域虚假事件信息，弄虚作假欺骗公众，扰乱公共秩序。拼凑剪接网络视频图片，篡改事件发生的时间、地点、人物等要素，以假乱真欺骗公众，侵犯他人合法权益。引用旧闻旧事，未准确完整说明事件全貌，以旧为新欺骗公众，破坏网络生态。

2. 不择手段蹭炒社会热点。假冒热点事件当事人、亲属或者相关人员发布信息，博取网民关注。针对热点事件，以虚构、歪曲等方式炮制事件原因、细节、进展等，发布阴谋论等耸人听闻的信息。操纵矩阵账号散布违法和不良信息，制造虚假热点，浪费公共资源。

3. 以偏概全设置话题。片面选取争议或负面词汇，炮制标题党、震惊体式话题，诱骗公众点击浏览。将极端个例概述为群体现象，以夸张的负面叙事渲染消极情绪。在话题设置上预设狭隘立场，散布偏激言论，挑动群体对立，破坏社会共识。

4. 违背公序良俗制造人设。编造苦情故事制造卖惨人设，打着助农、慈善等旗号，利用公众同情心理骗取关注，牟取利益。迎合低俗需求制造炫富人设，刻意展示金钱堆砌的奢侈生活，借此吸粉引流。挑战公众认知底线制造审丑人设，以装疯卖傻、恶俗行为等进行自我丑化，博取关注。

5. 滥发“新黄色新闻”。运用煽情化表达手法，配以抓人眼球的标题和封面，制作发布要素不全、真假难辨、质量低下、公共价值缺失的信息内容。

三、主要任务

1. 加强重点平台和重点环节管理。短视频和直播平台着重加大对虚假摆拍信息的识别和清理力度，从严处置违背公序良俗制造人设的“自媒体”账号。提供热搜榜单信息服务的平台着重强化拟上榜信息审核，及时处置以偏概全话题。资讯类平台着重清理标题党、要素欠缺、不具公共价值的“新黄色新闻”。搜索引擎平台不得在搜索结果页面、搜索联想词等，呈现“自媒体”无底线博流量信息。

2. 加强“自媒体”账号全流程管理。平台对开通营利权限的账号，应当以身份证件号码等进行真实身份信息认证。加强账号名称等账号信息动态核验，从严审核热点事件发生后新注册及名称变更的账号，发现假冒的一律关闭。严格执行“一人一号、一企两号”账号注册数量规定，对明确告知系小号、实际出镜人为同一人等的，应及时予以处置。

3. 加强信息来源标注展示。平台应要求“自媒体”发布涉国内外时事、公共政策、社会事件等相关信息时，必须准确标注信息来源。使用 AI 等技术生成信息的，必须明确标注系技术生成。发布含有虚构、演绎等内容的，必须明确加注虚构标签。平台需在显著位置展示“自媒体”标注的信息来源或标签。

4. 完善流量管理措施。健全流量管理规则，对“自媒体”应标未标来源的信息，不得在重点环节呈现。对恶意标注的信息，按虚假信息处置。对疑似无底线博流量的信息，应当预先采取流量限制措施，并视情暂停评论、点赞等互动数据增长。

四、工作要求

1. 加强组织领导。各地网信部门要将整治“自媒体”无底线博流量作为一项长期的工作任务，结合本地区实际，指导平台加强对无底线博流量行为的预判、预警、预防，不断完善长效治理措施，加强对“自媒体”教育引导，强化约束和规范。

2. 健全违规“自媒体”发现处置曝光机制。督促平台明确无底线博流量行为处置规则，完善流量、营利权限和粉丝数量一体化处罚机制，充分用好警示教育专栏，针对只要流量罔顾网络秩序的“自媒体”，第一时间发现，从严从重处置，及时公布处置结果。

3. 健全流量分配机制。督促平台将账号评价情况作为流量分配的重要指标，创新工作举措，对导向正确、内容优质的“自媒体”，积极给予扶持。优化算法模型和推荐机制，有效扩大优质内容触达范围，提升高热信息审核标准，阻断无底线博流量信息传播。

中央网信办秘书局

2024 年 4 月 21 日

（来源：中国网信网）

3. 中央网信办等三部门印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》

日前，中央网信办、国家发展改革委、工业和信息化部联合印发《深入推进 IPv6 规模部署和应用 2024 年工作安排》（以下简称《工作安排》）。

通知要求，坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大精神，完整、准确、全面贯彻新发展理念，以全面推进 IPv6 技术创新与融合应用为主线，着力破解瓶颈短板，完善技术产业生态，打造创新引领、高效协同的自驱性发展态势，为建设网络强国、数字中国提供有力支撑。

《工作安排》明确了 2024 年工作目标：到 2024 年末，IPv6 活跃用户数达到 8 亿，物联网 IPv6 连接数达到 6.5 亿，固定网络 IPv6 流量占比达到 23%，移动网络 IPv6 流量占比达到 65%。IPv6 网络性能显著提高，使用体验提升明显。云服务、内容分发网络、数据中心在业务开通时默认启用 IPv6 功能。主要商业网站及移动互联网应用 IPv6 支持率达到 95%，IPv6 行业融合应用更加深入广泛。固定网络 IPv6 贯通水平大幅跃升，新出厂家庭路由器、机顶盒等终端设备默认启用 IPv6，存量家庭路由器 IPv6 开启率明显提升，企业机构互联网专线 IPv6 开通率明显提高。IPv6 单栈支持能力持续增强。“IPv6+”创新技术应用领域进一步拓展。IPv6 标准体系持续完善，立项 IPv6 国家标准达到 50 项。

《工作安排》部署了十个方面重点任务。

一是增强 IPv6 网络性能和服务质量。包括加大 IPv6 网络优化力度、优化 IPv6 业务开通流程、持续提升 IPv6 互联互通水平、持续深入推进广电网络 IPv6 改造。

二是提高应用设施 IPv6 部署水平。包括加强云产品 IPv6 推广应用、提升内容分发网络 IPv6 流量占比、强化数据中心承载业务 IPv6 升级改造、推动算力基础设施同步部署 IPv6。

三是提高终端设备 IPv6 连通水平。包括提升家庭路由器 IPv6 使用水平、扩大家庭智能终端 IPv6 支持范围、加快推进物联网 IPv6 应用。

四是强化先行先试和示范引领。包括开展重点城市 IPv6 专项行动、强化试点示范作用、推动党政机关办公网络率先开通 IPv6、强化推进 IPv6 规模部署和应用专家委平台作用。

五是推进 IPv6 单栈部署演进。包括增强 IPv6 单栈运行能力、拓展 IPv6 单栈试点部署范围。

六是深化行业融合应用。包括深化中央企业行业系统 IPv6 改造、提升金融机构 IPv6 创新应用水平、推进农业农村部系统 IPv6 升级改造、深化教育行业 IPv6 部署应用、推进各级人社部门 IPv6 部署应用、推进民政信息系统 IPv6 部署应用、加强医疗卫生机构 IPv6 升级改造、推进交通数字化设施 IPv6 应用、拓展工业互联网 IPv6 应用、深化水利行业 IPv6 部署应用、加大自然资源与生态环境信息化 IPv6 改造力度、推动应急管理业务系统和终端支持 IPv6。

七是扩大 IPv6 内容源规模。包括深化政务网络和应用服务 IPv6 升级改造、拓展商业应用 IPv6 支持范围。

八是推进创新生态和标准体系建设。包括强化“IPv6+”创新产业生态建设、加强互联网体系结构创新研究、持续推进IPv6国家标准制定与实施、积极参与IPv6技术国际标准制定。

九是强化网络安全保障。包括加快IPv6安全技术产品研发应用、加强IPv6网络安全防护和管理监督。

十是加大宣传推广力度。包括创新宣传形式和内容、丰富行业交流活动。

（来源：中国网信网）

行业前沿观察二：各地协会动态

导读：两会后各地协会开展了精彩纷呈的活动。湖南省网络空间安全协会第五届理事会 2024 年第一次会议顺利召开；西藏自治区互联网协会党支部联合西藏电信客户服务部党支部开展“弘扬劳动精神、争做有为青年”主题党日活动；广东省信息网络安全专家库（揭阳）召开 2024 年度工作座谈会；肇庆市信息协会：跨境电商业务培训及对接交流会顺利举办；南昌市委网信办副主任刘煜一行莅临南昌市网络信息安全协会走访调研；“知识产权转化运用促进高质量发展暨华为鸿蒙生态赋能——应用开发者认证讲座”在广州应用科技学院举行；2024 年宁波市信息网络安全论坛开幕。

1. 湖南省网络空间安全协会第五届理事会2024年第一次会议顺利召开

4月16日，湖南省网络空间安全协会第五届理事会2024年第一次会议在蓉园宾馆顺利召开。协会第五届理事长苏金树、秘书长邓庭波、中南大学电子信息学院施荣华教授及38家理事单位参加会议。

会议由苏金树理事长主持召开。苏理事长首先简单介绍了目前协会的组织架构情况：协会于2005年4月28日正式成立。协会在省民政厅、省公安厅的业务指导和监督管理下，由省内信息网络安全保卫主管机关、重要信息系统运营单位、互联网接入服务单位、互联网内容提供单位、信息网络安全产品生产与服务单位自愿组成的非营利的社会团体，并具备法人资格。协会的最高权力机构是会员大会，下设理事会。理事会负责人由理事长、副理事长、秘书长组成。经过近二十年的发展，湖南省网络空间安全协会基本形成了协会抓总、专家委指导的“1+N”组织体系，目前下设一个专家咨询委员会，六个工作专委会，分别是网络安全等级保护专委会、关键信息基础设施保护专委会、应急处置专委会、网络新媒体专委会、数据安全工作专委会、网络空间安全人才培训专委会，行业组织建设更加专业化、职业化。6个专委会工作正有条不紊的筹备开展中，并将于换届大会结束后正式上报民政厅备案。会议还就《专委会管理办法》进行了讨论，该办法

主要说明了各工作专委会的职责与构成等规则，与会人员一致通过并即刻生效，协会各相关工作专委会将遵守该《办法》相关要求开展工作。

2. 2024 年宁波市信息网络安全论坛开幕

4 月 14 日，宁波市计算机信息网络安全协会和市警察协会联合举办 2024 年宁波市信息网络安全论坛。本次论坛以“信息技术应用创新与数据安全”为主题，深入贯彻落实习近平总书记有关网络强国的系列重要讲话精神，深刻把握网络安全产业发展的新理论、新特点、新模式、新业态，汇聚政产学研各界人士，共同促进信息网络安全理论和技术的创新发展，着力提升数据安全管理和网络安全防护能力。本次活动也是为了提升宁波市民营企业安全防护能力的一次重要活动。

宁波市公安局党委副书记、副局长、市警察协会会长项敏、市公安局党委委员、副局长管海旻、市大数据局党组成员、副局长尤波军、市国资委党委委员、副主任张旭军和市公安局、市卫健委、市教育局、市密码管理局等单位相关领导出席论坛。

论坛吸引了 500 多家单位参与，涵盖政府部门、企事业单位、高等院校、医疗机构等多个领域，与会代表围绕信息技术的理论探索、实践应用、安全保护、技术创新等议题展开了深入广泛的交流和讨论。同时，本次论坛针对警务、国资、医疗、教育等不同行业特点，分门别类地设置了讨论议题，开设了多个分论坛。各分论坛上，与会领导、专家和代表紧密结合不

同行业特点和管理要求，就如何更好地将信息技术应用于行业实践、加强数据安全管理、构建安全可靠的网络环境等问题深入进行探讨，提出了许多富有建设性、指导性和操作性的意见。

3. 广东省信息网络安全专家库（揭阳）召开 2024 年度工作座谈会

3 月 28 日下午，广东省信息网络安全专家库（揭阳）2024 年度工作座谈会在协会会议室召开，会议以线上、线下同步举行的形式进行。来自市电视台、运营商、学校和会员单位等专家代表参加座谈。

首先，座谈会交流了协会发展近况、取得成果及专家库今年主要工作思路；其次，参会专家就当前信息网络安全工作做了分享；最后就第三届广东信创大赛（揭阳赛区）有关赛项和活动的筹备工作、2023 网络安全感满意度调查活动揭阳报告发布、揭阳市学术交流月活动（市科协主办）的主题设计、揭阳市未成年人网络空间权益保护情况调查研究课题（市社科联立项课题）、网安人才培养和成长宣传服务工作等事项进行讨论。

专家们充分肯定协会近年来在网络安全学术活动方面的努力和成果。他们表示，将继续积极参与协会有关技术交流研讨等工作，为我市网络安全和数据安全、数字化转型、以及网络安全科技人才的培养和成长贡献力量。

4. 肇庆市信息协会：跨境电商业务培训及对接交流会顺利举办

为深入贯彻落实市、区“百千万工程”工作部署，推动实施“学校联县行动”工作方案，助力跨境电商产业高质量发展，4 月 18 日下午，由肇庆市商务局指导，端州区工信局、肇庆市工业贸易学校主办，肇庆市计算机学会、肇庆市信息协会协办的2024年政校企合作助力“百千万工程”高质量发展跨境电商业务培训及对接交流会在工业贸易学校举行。肇庆市信息协会执行会长单位副总经理范向文代表出席。

活动聚焦政校企对接、跨境出海布局策略、跨境电商本地服务、跨境电商保效计划和人才供需对接等，为政校企搭建了一个合作交流的平台。

学校副校长彭建新表示，高质量发展是一项系统工程，需要凝聚政府、行业、企业、学校等多方力量。为进一步助力跨境电商产业高质量发展，培养更多高素质的行业人才，学校积极搭建共商共议、互促发展的平台，希望各方能沟通互联、加强合作，共绘肇庆“百千万工程”高质量发展同心圆。

端州区工信局副局长朱江发表了讲话，强调了举办本次活动的重要意义，分析了跨境电商在促进外贸发展方面的作用，提出了两点期望：一是期望参会企业积极开展跨境电商业务，通过优势平台做大海外市场，做强公司产品，为肇庆跨境电商综试区建设作出积极的贡献；二是实现企业人才供需对接，为企业开展跨境电商业务提供人才保障，同时，促进学校有针对性地培养人才。

肇庆市橙优企业服务有限公司总经理李瑞荣结合自身丰富的行业经验，通过中国制造产品的竞争力、海外买家群体的变化、市场变化带来的机遇、海外工程项目等分析了跨境电商的发展情况；以阿里巴巴国际站为例，分享了跨境电商的热卖产品、平台核心优势以及买家卖家精准匹配策略等。

阿里巴巴国际站肇庆渠道负责人聂卫坚从企业的使命与价值观谈起，介绍了跨境电商本土服务网点的功能、服务内容和范围等，同时，还对阿里巴巴国际站出海保效计划进行了说明。

5. 西藏自治区互联网协会党支部联合西藏电信客户服务部党支部开展“弘扬劳动精神、争做有为青年”主题党日活动

为热烈庆祝“五一”劳动节和“五四”青年节，进一步增强协会干部职工的凝聚力、向心力和弘扬艰苦奋斗、勤劳向上的传统美德，树立正确的劳动价值观念，营造浓厚的节日氛围，4 月 25 日下午，西藏自治区互联网协会党支部同协会团指委联合西藏电信客户服务部党支部组织区互联网协会和区通信行业协会党员、发展对象、青年干部职工赴西藏电信公司卫星地面站开展“弘扬劳动精神、争做有为青年”主题党日活动。

一次主题党日活动。全体党员、青年干部职工在党支部书记彭坤的带领下参观了西藏电信史陈列馆、天翼信息体验馆和中国电信应急装备展。参观过程中，讲解员为大家讲述西藏信息通信基础设施建设从“无”到“有”、从“有”到“优”的发展历程，展示了西藏信息通信人传承红色基因，坚

守“人民邮电为人民”的初心使命，克服高寒缺氧，跨越高山峡谷，创造了一个又一个通信建设奇迹，实现西藏通信水平从“能力落后”到“云网融合”的飞跃提升。

通过开展此次主题党日活动，彭坤强调坚持以“双强六好”支部建设行动为抓手，坚持抓创新创特色、抓重点出亮点，持续释放西藏自治区互联网协会党支部党建品牌效应，推动党建和业务深度融合；要必须旗帜鲜明毫不动摇坚持党管互联网，网络发展到哪里党的工作就覆盖到哪里，不断发挥党支部和群团组织在协会决策、提高效益等方面的作用，不断把党的政治优势、组织优势转化为发展优势，以高质量党建助推互联网及信息通信事业高质量发展。

6. 南昌市委网信办副主任刘煜一行莅临南昌市网络信息安全协会走访调研

2024 年 4 月 23 日上午，南昌市委网信办副主任刘煜一行莅临协会走访调研。南昌市网络信息安全协会会长樊建功和协会班子成员参与陪同。

调研组一行参观并了解了协会工作环境后，与协会班子成员在会议室展开了座谈交流。会长樊建功详细介绍了协会的组织架构、发展历程和工作成效。 调研组一行对协会两大委员会和五大中心的职能进行了详细的了解，并对协会利用专家和技术优势支撑服务政府主管部门和广大会员单位的做法予以了充分肯定。

其间，刘煜主任表示，协会作为非盈利性社会组织要做好以下几点：一是要高度重视党建工作。协会要坚定政治方向，发挥党建的引领作用，以党建带动群建、团建；二是要充分发挥专家作用。协会要利用好现有专委会专家团队，为政府主管部门的工作做好支撑，共同保障我市信息网络空间的安全和稳定；三是要积极扩展协会职能。协会要不断吸纳优质会员单位，整合资源，扩展各项职能，作为政府主管部门管理工作的延伸，服务我市网络与信息安全行业的发展。

最后，协会会长樊建功表示，协会将在南昌市委网信办和南昌市互联网行业党委的领导下，不断加强自身宣传，努力提高凝聚力和公信力，树立良好的社会形象；充分发挥平台优势，搭建起会员单位、理事单位以及政府主管部门之间的桥梁纽带；大力协助政府工作，继续做好各项技术支撑和安全保障工作，在行业自律中发挥协会的引领作用，为推动和促进我市网络与信息安全行业健康、有序发展作出贡献。

7. “知识产权转化运用促进高质量发展暨华为鸿蒙生态赋能——应用开发者认证讲座”在广州应用科技学院举行

2024 年 4 月 20 日至 26 日为全国知识产权宣传周，活动主题是“知识产权转化运用促进高质量发展”。肇庆市计算机学会作为知识产权维权援助工作站，一直致力于推广知识产权文化和维权服务工作。

4 月 26 日，在肇庆市市场监督管理局（知识产权局）、端州区工业和信息化局和端州区科学技术协会的指导下，由肇庆市计算机学会主办的 2024 年知识产权进校园系列活动“知识产权转化运用促进高质量发展暨华为鸿蒙生态赋能——应用开发者认证讲座”在广州应用科技学院举行。

广东赛力律师事务所副主任黄杰明围绕“知识产权基础知识”这一个主题，从知识产权战略地位、基本内容、经济贸易协议、前沿发展四大方面系统分析了保护知识产权的重要性 。黄杰明表示，随着人工智能的发展，知识产权保护应充分考虑数据安全与应用，把握产权制度的客观规律，充分尊重原创者的劳动成果和相关投入，积极发挥知识产权转化运用对经济高质量发展的支撑作用。

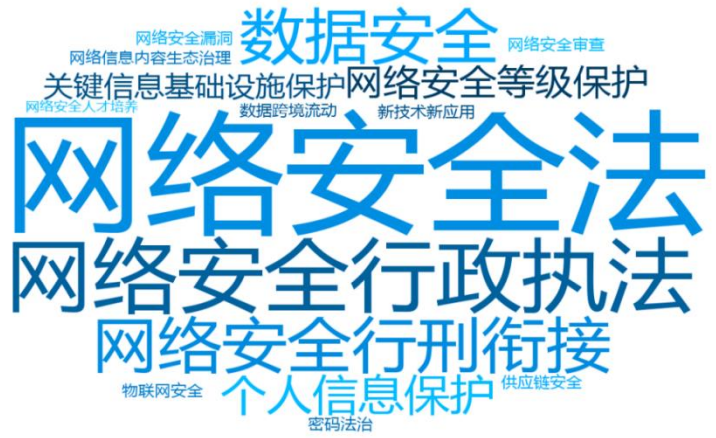
泰克教育张烂老师围绕“华为鸿蒙生态赋能 ”主题，介绍了广东省新一代信息技术产业人才公共实训中心的情况，分享了 HarmonyOS 应用场景、核心技术理念、发展现状以及鸿蒙工程师待遇等问题。在万物互联的时代，鸿蒙应用开发者认证公益项目应运而生，不仅发展潜力巨大，相比 JAVA 等语言更通俗易懂，技术更容易落地，大厂技术+认证，将打造就业双引擎。

通过此次知识产权进校园活动，让在校师生对知识产权发展有了更深入的了解，激发创新创造活力，进一步推动高校科研成果的转化运用。同时，通过加强校企合作，使大学生紧跟时代发展的步伐，掌握前沿技术，不断提升综合素质和就业竞争力。

公安部第三研究所网络安全法律研究中心

2016年2月，公安部第三研究所正式成立“网络安全法律研究中心”。 中心成立以来，聚焦前瞻性研究，切实践行理论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

……