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1月第1期(总第6期)

2024年1月23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：安全事件

导读：12 月，中央经济工作会议举行。会议要求发展数字经济，加快推动人工智能发展。放宽电信、医疗等服务业市场准入，对标国际高标准经贸规则，认真解决数据跨境流动、平等参与政府采购等问题，持续建设市场化、法治化、国际化一流营商环境。

第十三届中国信息安全法律大会在京成功召开，来自政府机构、科研院所、高校、互联网企业的 300 余人出席会议。国家密码管理局相关负责同志在致辞中表示加强密码法治建设和法治实施是一项长期、复杂的系统工程，需要全社会的共同努力，希望社会各界共同参与进来，一起守正创新、持续发力。公安部网络安全保卫局政委孙劲峰在致辞中呼吁，网络空间承载着全人类对美好未来的无限憧憬，也面临着安全和发展方面的问题和挑战，希望大家携起手来共同应对，谱写网络强国建设新篇章。

关键词：中央经济工作会议、中国信息安全法律大会

1. 中央经济工作会议：加快推动人工智能发展，认真解决数据跨境流动等问题

12 月 11 日至 12 日，中央经济工作会议在北京举行。会议强调，以科技创新引领现代化产业体系建设。要大力推进新型工业化，发展数字经济，加快推动人工智能发展。打造生物制造、商业航天、低空经济等若干战略性新兴产业，开辟量子、生命科学等未来产业新赛道，广泛应用数智技术、绿色技术，加快传统产业转型升级。

会议要求，扩大高水平对外开放。放宽电信、医疗等服务业市场准入，对标国际高标准经贸规则，认真解决数据跨境流动、平等参与政府采购等问题，持续建设市场化、法治化、国际化一流营商环境，打造“投资中国”品牌。（来源：新华网）

2. 第十三届中国信息安全法律大会在北京成功召开

12 月 27 日，由国家密码管理局和公安部网络安全保卫局指导，中国信息安全法律大会专家委员会和密码法治实践创新基地主办，公安部第三研究所和西安交通大学苏州研究院承办，北京网络空间安全协会、中国计算机学会计算机安全专业委员会等单位共同协办的第十三届中国信息安全法律大会在北京成功召开。

大会以“敏捷治理 智慧执法 数字安全”为主题，设“新AI时代的数据安全治理与个人信息保护”“密码法治实践与创新发展”“网络安全行政执法：精细化、标准化与智慧化”“网络犯罪生态治理”四个分论坛，

近50位国内政府机构代表、专家学者和企业代表围绕人工智能、密码法治、行政执法和网络犯罪议题作专题发言，并通过圆桌与谈、法治访谈等形式对当前信息技术前沿和法治热点问题进行深入讨论。来自政府机构、科研院所、高校、互联网企业的300余人出席会议。

国家密码管理局相关负责同志致辞。他表示，近年来，密码法治建设成效显著，取得良好的政治效果、社会效果和法律效果。下一步，国家密码管理局将以习近平法治思想为指导，统筹谋划《密码法》和《商用密码管理条例》贯彻实施工作，进一步完善商用密码法律制度体系，全面履行密码行政管理职责，督促相关主体落实密码管理法定义务和责任。他强调，加强密码法治建设和法治实施是一项长期、复杂的系统工程，需要全社会的共同努力，希望社会各界共同参与进来，一起守正创新、持续发力。

公安部网络安全保卫局政委孙劲峰致辞。他指出，公安部党委深入学习贯彻习近平法治思想，高度重视网络安全工作，就维护网络安全、数据安全作出系列部署，着力推进新时代网络法治建设。指导每届中国信息安全法律大会是公安机关推进网络法治建设的重要举措之一，到目前已经形成一批理论结合实际、有广泛而深远影响的研究成果。作为维护国家网络安全的重要职能部门，长期以来，公安机关坚持依法履职、锐意进取，严厉打击人民群众反映强烈的网络犯罪活动，依法强化互联网安全监管，深入推进网络综合治理，切实加强网络安全保护，全力维护网络空间安全、保障人民群众利益。他呼吁，网络空间承载着全人类对美好未来的无限憧

憬，也面临着安全和发展方面的问题和挑战，希望大家携起手来共同应对，谱写网络强国建设新篇章。

大会同步发布《中国后量子密码政策法律蓝皮书（2023）》《国家关键基础设施保护的无人机防御战略倡议》《全球网络安全政策法律发展年度报告（2023）》等五项重要研究成果，对网络安全法治研究和产业方向指引意义重大。

境内前沿观察二：政策立法

导读：12 月，境内立法呈现的显著特点之一是数据的资源价值进一步得到立法认可，充分激发数据要素潜能，发挥数据要素价值将是数字经济发展的核心环节。继国家数据局局长刘烈宏在公开会议表示将围绕发挥数据要素乘数作用，与相关部门一道研究实施“数据要素X”行动后，国家数据局等 17 部门正式印发《“数据要素×”三年行动计划（2024—2026 年）》。行动计划指出，发挥数据要素的放大、叠加、倍增作用，构建以数据为关键要素的数字经济，是推动高质量发展的必然要求。同时，从数据要素×工业制造、交通运输、金融服务、科技创新等十二领域提出重点行动措施。地方层面，海南、重庆、山东青岛围绕培育数据要素市场、数据要素市场化配置改革发布行动计划或行动方案，北京、安徽、贵州、河北石家庄等省市聚焦公共数据，在保障安全的同时探索公共数据开放利用。

事件报告义务的细化落实成为多部门共同关注。国家互联网信息办公室发布《网络安全事件报告管理办法（征求意见稿）》，要求网络运营者发生较大、重大或特别重大网络安全事件时应当于 1 小时内进行报告。工信部发布《工业和信息化领域数据安全事件应急预案（试行）（征求意见稿）》，要求工业和信息化领域数据处理者一旦发生数据安全事件，应当立即先行判断，对自判为较大以上事件的，应当立即向地方行业监管部门报告。可以预见，我国公安、网信及工信等部门已充分意识到强化报告要求的重要性，除了继续通过制度文件要求网络运营者、数据处理者、个人

信息处理者上报安全风险和安全事件外，在行政执法过程中也将进一步提高对于报告义务落实情况的重视程度，将其列为监督检查、专项行动重要检查内容之一。

关键词：数据要素X、培育数据要素市场、公共数据授权运营、网络/数据安全事件报告

（一）国家层面动向

1. 国务院印发《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》，要求全面加强网络安全检查

11 月 26 日，国务院印发《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》。

数据跨境流动方面，方案提出，企业和个人因业务需要确需向境外提供数据，且符合国家数据跨境传输安全管理要求的，可以向境外提供。按照数据分类分级保护制度，支持上海自贸试验区率先制定重要数据目录。指导数据处理者开展数据出境风险自评估，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。商用密码产品管理方面，方案提出，除列入商用密码进口许可清单的外，对不涉及国家安全、社会公共利益的商用密码产品进口，不采取限制措施。加强风险防控体系建设方面，方案要求，全面加强网络安全检查，落实关键信息基础设施防护责任。（来源：中国政府网）

2. 国务院审议通过《非银行支付机构监督管理条例》，不得将涉及信息安全等的核心业务和技术服务委托第三方处理

12 月 9 日，国务院审议通过《非银行支付机构监督管理条例》，自 2024 年 5 月 1 日起施行。

条例规定，非银行支付机构不得将涉及资金安全、信息安全等的核心业务和技术服务委托第三方处理。非银行支付机构应当具备必要和独立的业务系统、设施和技术，按照强制性国家标准以及相关网络、数据安全管理要求，确保支付业务处理的及时性、准确性和支付业务的连续性、安全性、可溯源性。非银行支付机构的业务系统及其备份应当存放在境内。

条例明确，非银行支付机构相关网络设施、信息系统等被依法认定为关键信息基础设施，或者处理个人信息达到国家网信部门规定数量的，其在境内收集和产生的个人信息的处理应当在境内进行。确需向境外提供的，应当符合法律、行政法规和国家有关规定，并取得用户单独同意。非银行支付机构在境内收集和产生的重要数据的出境安全管理，依照法律、行政法规和国家有关规定执行。（来源：中国政府网）

3. 中央网络安全和信息化委员会印发《关于防治“指尖上的形式主义”的若干意见》

12 月 18 日，中央网络安全和信息化委员会印发《关于防治“指尖上的形式主义”的若干意见》。意见主要规范政务移动互联网应用程序、政务公众账号和工作群组管理，从强化建设管理、使用管理、安全管理和组织保障方面提出具体要求。

强化安全管理方面，意见要求，严格落实党委（党组）网络意识形态工作责任制、网络安全工作责任制，建立政务应用程序、政务公众账号和工作群组安全管理制度，健全应急处置机制，配强配齐应急处置力量，制定应急预案，开展应急演练，不断优化应急处置流程，有效防范各类突发

情况。落实网络安全、数据安全、关键信息基础设施安全保护、个人信息保护等相关法律规定，加强全生命周期数据安全管理，依法依规保护数据和个人信息安全。组织做好政务应用程序运行监测，建立健全运维管理规范，严格值班值守和巡查巡检，保障可靠稳定运行。（来源：中国网信网）

（二）部委层面动向

1. 国家互联网信息办公室发布《网络安全事件报告管理办法（征求意见稿）》

12 月 8 日，国家互联网信息办公室发布《网络安全事件报告管理办法（征求意见稿）》。

征求意见稿规定，运营者在发生网络安全事件时，应当及时启动应急预案进行处置。按照《网络安全事件分级指南》，属于较大、重大或特别重大网络安全事件的，应当于 1 小时内进行报告。为运营者提供服务的组织或个人发现运营者发生较大、重大或特别重大网络安全事件时，应当提醒运营者按照本办法规定报告事件，运营者有意隐瞒或拒不报告的，可向属地网信部门或国家网信部门报告。

征求意见稿规定，发生网络安全事件时，运营者已采取合理必要的防护措施，按照本办法规定主动报告，同时按照预案有关程序进行处置、尽最大努力降低事件影响，可视情免除或从轻追究运营者及有关责任人的责任。（来源：中国网信网）

2. 国家互联网信息办公室与香港创新科技及工业局共同发布《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》

12 月 10 日，国家互联网信息办公室与香港创新科技及工业局共同发布《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》。

指引指出，粤港澳大湾区个人信息处理者及接收方可以按照实施指引要求，通过订立标准合同的方式进行粤港澳大湾区内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。

指引要求，个人信息处理者按照实施指引，通过订立标准合同跨境提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：（一）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性；（二）对个人信息主体权益的影响及安全风险；（三）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。（来源：中国网信网）

3. 工信部发布《工业和信息化领域数据安全事件应急预案（试行）（征求意见稿）》

12 月 15 日，工信部发布《工业和信息化领域数据安全事件应急预案（试行）（征求意见稿）》，明确工信领域数据安全事件的管理机构、监测与预警机制、事件应急响应处置流程以及预防措施等内容。

征求意见稿明确，数据安全事件应急响应分为四级：I级、II级、III级、IV级，分别对应发生特别重大、重大、较大、一般数据安全事件的应

急响应。工业和信息化领域数据处理者一旦发生数据安全事件，应当立即先行判断，对自判为较大以上事件的，应当立即向地方行业监管部门报告，不得迟报、谎报、瞒报、漏报。数据安全应急支撑机构应当通过多种途径监测、收集数据安全事件信息，及时向行业监管部门报告。地方行业监管部门初步研判为特别重大、重大数据安全事件的，应当在发现事件后按照“电话 10 分钟、书面 30 分钟”的要求向机制办公室报告。报告事件研判信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议。（来源：工信部）

4. 工信部、国家标准化管理委员会印发《工业领域数据安全标准体系建设指南（2023 版）》

12 月 19 日，工信部、国家标准化管理委员会印发《工业领域数据安全标准体系建设指南（2023 版）》。

指南明确工业领域数据安全标准体系总体框架，以及基础共性、安全管理、技术和产品、安全评估与产业评价、新兴融合领域、工业细分行业六个子体系内容。基础共性、安全管理、技术和产品、安全评估与产业评价子体系聚焦工业领域具有共性的数据安全标准，新兴融合领域、工业细分行业两个子体系重点突出特定业务场景的数据安全标准。指南另发布《工业领域数据安全现行及在研标准明细表》及《工业领域数据安全标准拟研制重点方向》两项附件。（来源：工信部）

5. 国家数据局等 17 部门印发《“数据要素×”三年行动计划（2024—2026 年）》

12 月 31 日，国家数据局、中央网信办、科技部、工信部等 17 部门联合印发《“数据要素×”三年行动计划（2024—2026 年）》，旨在充分发挥数据要素乘数效应，赋能经济社会发展。

行动计划明确总体目标是到 2026 年底，数据要素应用广度和深度大幅拓展，打造 300 个以上示范性强、显示度高、带动性广的典型应用场景，涌现出一批成效明显的数据要素应用示范地区，培育一批创新能力强、成长性好的数据商和第三方专业服务机构，数据产品和服务质量效益明显提升，数据产业年均增速超过 20%，场内交易与场外交易协调发展，数据交易规模倍增。

行动计划明确十二项重点行动，包括数据要素×工业制造、现代农业、商贸流通、交通运输、金融服务、科技创新、文化旅游、医疗健康、应急管理、气象服务、城市治理、绿色低碳等方面。行动计划同时明确三方面保障措施。一是提升数据供给水平，完善数据资源体系，加大公共数据资源供给，健全标准体系，加强供给激励；二是优化数据流通环境，提高交易流通效率，打造安全可信流通环境，培育流通服务主体，促进数据跨境有序流动；三是加强数据安全保障，落实数据安全法规制度，丰富数据安全产品，培育数据安全服务。（来源：国家数据局）

6. 商务部等12部门印发《关于加快生活服务数字化赋能的指导意见》，要求增强数据安全保护与融合应用能力

12月19日，商务部、国家发展改革委、教育部、工信部等12部门联合印发《关于加快生活服务数字化赋能的指导意见》。

指导意见从丰富生活服务数字化应用场景、补齐生活服务数字化发展短板、激发生活服务数字化发展动能、夯实生活服务数字化发展基础以及强化支持保障措施5个方向提出19条具体任务举措。同时，相关部门将强化支持保障措施，加强组织协调，由商务部、国家发展改革委、工信部牵头，会同相关部门建立生活服务数字化发展工作联络机制，协调推进生活服务数字化相关工作，及时解决政策落实过程中的难点、堵点问题。

数据安全方面，指导意见要求严格落实《数据安全法》《个人信息保护法》等相关法规要求，落实数据分类分级保护制度，推进网络身份认证公共服务建设，保护个人信息权益，规范个人信息处理活动。在国家网络安全等级保护制度的基础上，落实数据安全保护措施，健全完善全生命周期安全保护体系。加强数据安全监督管理、检测评估、通报预警和应急处置等工作，严厉打击危害数据安全违法犯罪活动，有效防范网络和数据安全风险。促进生活性服务业与其他产业深度融合，推进数据资源共享，构建生活服务数字化发展生态体系。（来源：商务部）

7. 国家发展改革委等五部门印发《关于深入实施“东数西算”工程 加快构建全国一体化算力网的实施意见》

12 月 25 日，国家发展改革委、国家数据局、中央网信办、工信部、国家能源局联合印发《关于深入实施“东数西算”工程 加快构建全国一体化算力网的实施意见》。

意见从通用算力、智能算力、超级算力一体化布局，东中西部算力一体化协同，算力与数据、算法一体化应用，算力与绿色电力一体化融合，算力发展与安全保障一体化推进等五个统筹出发，推动建设联网调度、普惠易用、绿色安全的全国一体化算力网。

安全方面，意见要求完善算网安全保障体系，构建促发展保安全机制。具体要求加强通信网络安全防护管理，提升网络安全防护能力水平，创新数据中心灾备建设，形成可靠稳定算力布局。打造自主创新的技术供给能力，强化国家枢纽节点自主防护能力，统一应急处置、统一安全监测、统一运行监控，构筑全生命周期的安全管控措施，实现集群内网络和数据安全“可知、可视、可管、可控、可溯”，推动建设国家算力网基础安全服务保障平台，打造一体化的安全保障服务能力。打造网络和数据攻防演习靶场，推动国家枢纽节点地区定期开展网络和数据攻防演习，加强网络稳定性监测，确保数据传输安全。面向党政机关、关键信息基础设施服务的云平台应当通过云计算服务安全评估，支持云平台建立健全安全检测、通报预警、应急响应与处置机制。（来源：国家发展改革委）

8. 国家发展改革委、国家数据局印发《数字经济促进共同富裕实施方案》

12 月 25 日消息，国家发展改革委、国家数据局近日印发《数字经济促进共同富裕实施方案》，明确以数字经济促进共同富裕的指导思想、发展目标、重点举措和保障措施。

实施方案部署四方面重点举措：一是推动区域数字协同发展。推进数字基础设施建设，推进产业链数字化发展，加强数字经济东西部协作；二是大力推进数字乡村建设。加快乡村产业数字化转型步伐，加大农村数字人才培养力度，提升乡村数字治理水平；三是强化数字素养提升和就业保障。加强数字素养与技能教育培训，实施“信息无障碍”推广工程，加强新就业形态劳动者权益保障；四是促进社会服务普惠供给。促进优质数字教育资源共享，强化远程医疗供给服务能力，提升养老服务信息化水平，完善数字化社会保障服务。（来源：国家数据局）

9. 国家新闻出版署发布《网络游戏管理办法（草案征求意见稿）》

12 月 22 日，国家新闻出版署发布《网络游戏管理办法（草案征求意见稿）》。征求意见稿共 8 章 64 条，对网络游戏出版经营单位的设立与管理、网络游戏的出版经营、未成年人保护、监督管理等作出规定。

征求意见稿规定网络游戏出版经营单位应当按照法律、行政法规规定采取措施保证网络信息安全，依法保护国家秘密、商业秘密和用户个人信息。网络游戏出版经营单位通过网络处理用户个人信息，应当遵循合法、正当、必要和诚信的原则，公开专门的处理规则，明示处理的目的、方式

和范围，依法告知法律、行政法规规定的相关事项。（来源：国家新闻出版署）

10. 国家金融监督管理总局修订发布《银行保险机构操作风险管理办法》

12 月 29 日，国家金融监管总局修订发布《银行保险机构操作风险管理办法》，于 2024 年 7 月 1 日起施行。

办法要求，银行保险机构应当制定网络安全管理制度，履行网络安全保护义务，执行网络安全等级保护制度要求，采取必要的管理和技术措施，监测、防御、处置网络安全风险和威胁，有效应对网络安全事件，保障网络安全、稳定运行，防范网络违法犯罪活动。银行保险机构应当制定数据安全管理制度，对数据进行分类分级管理，采取保护措施，保护数据免遭篡改、破坏、泄露、丢失或者被非法获取、非法利用，重点加强个人信息保护，规范数据处理活动，依法合理利用数据。

办法规定，银行保险机构应当在知悉或者应当知悉以下重大操作风险事件 5 个工作日内，按照监管职责归属向国家金融监督管理总局或其派出机构报告：（1）重要信息系统出现故障、受到网络攻击，导致在同一省份的营业网点、电子渠道业务中断 3 小时以上；或者在两个及以上省份的营业网点、电子渠道业务中断 30 分钟以上；（2）因网络欺诈及其他信息安全事件，导致本机构或客户资金损失 1000 万元以上，或者造成重大社会影响；（3）严重侵犯公民个人信息安全和合法权益的事件。（来源：国家金融监管总局）

11. 全国信安标委发布《网络安全标准实践指南——大型互联网平台网络安全评估指南（征求意见稿）》

12 月 23 日，全国信安标委发布《网络安全标准实践指南——大型互联网平台网络安全评估指南（征求意见稿）》，面向社会公开征求意见。征求意见稿从影响或者可能影响社会稳定和公共利益的角度，给出了开展大型互联网平台网络安全评估的评估内容和评估方法，为大型互联网平台开展网络安全评估提供参考。（来源：全国信安标委）

（三）地方层面动向

1. 海南省印发《海南省培育数据要素市场三年行动计划（2024—2026）》

12 月 5 日，海南省人民政府办公厅印发《海南省培育数据要素市场三年行动计划（2024—2026）》。行动计划明确实施数据要素基础制度创新行动、数据供给能力提升行动、数据开发能力提升行动、数据安全治理行动、数据跨境应用创新行动等九项具体任务。

数据安全治理行动方面，行动计划要求：（一）健全政府数据管理机制行动。健全数据接入开发流通过程的安全风险评估、合规公证、信息共享、监测预警和应急处置机制。强化分行业监管和跨行业协同监管，建立健全数据联管联治机制与容错纠错机制；（二）压实企业数据处理责任行动。企业应严格遵守反垄断法等相关法律规定，不得利用数据、算法等优势和技术手段排除、限制竞争；（三）促进社会力量多方参与协同安全治

理行动。鼓励行业协会等社会力量积极参与数据要素市场建设，支持开展数据流通相关安全技术研发和服务，促进不同场景下数据要素安全可信流通。（来源：海南省人民政府）

2. 海南省大数据管理局发布《海南省数据产品超市数据产品确权登记实施细则（暂行）》

12 月 14 日，海南省大数据管理局发布《海南省数据产品超市数据产品确权登记实施细则（暂行）》。

实施细则适用于申请对象利用海南省数据产品超市所提供的数据资源，通过实质性加工和创新性劳动形成并在海南省数据产品超市内上架应用服务或流通交易的数据产品的确权登记；或申请对象利用自有数据资源所加工形成的数据产品，根据自身情况自愿进行数据产品确权登记的情形。

细则要求，申请对象发起数据产品确权登记申请，应当提交的材料包括但不限于：（一）申请对象主体资格证明材料；（二）确权登记申请表；（三）数据产品介绍说明书；（四）数据来源证明材料；（五）数据授权通道证明材料；（六）安全合规体系说明材料；（七）联合拥有的权益比例证明材料；（八）第三方确权登记服务机构进行合规性审核所需要的其他必要材料。（来源：海南省大数据管理局）

3. 北京市经济和信息化局印发《北京市公共数据专区授权运营管理办法（试行）》

12 月 5 日，北京市经济和信息化局印发《北京市公共数据专区授权运营管理办法（试行）》。

办法明确，公共数据是指本市各级国家机关、经依法授权具有管理公共事务职能的组织在履行职责和提供公共服务过程中处理的各类数据。公共数据专区是指针对重大领域、重点区域或特定场景，为推动公共数据的多源融合及社会化开发利用、释放数据要素价值而建设的各类专题数据区域的统称，一般分为领域类、区域类及综合基础类。

办法要求，专区运营单位应以网络安全等级保护三级标准建设数据开发与运营管理平台，做好授权数据加工处理环节的管理。数据开发与运营管理平台的功能包括但不限于数据加工处理人员的实名认证与备案管理，操作行为的记录和审计管理，原始数据的加密和脱敏管理，元数据管理，数据模型的训练和验证功能，数据产品的提供、交易和计价功能。（来源：北京市人民政府）

4. 山东青岛市发布《青岛市数据要素市场化配置改革三年行动方案》《青岛市公共数据管理办法》

12 月 5 日，数字青岛建设领导小组办公室印发《青岛市数据要素市场化配置改革三年行动方案》。行动方案明确三大主要任务：一是全面推进数据资源化；二是有序推进数据资产化；三是创新推进数据产业化。基于三大任务提出五项专项行动，分别是数据基础制度建设行动、数据开发利

用创新行动、数据流通交易增效行动、数据合规安全护航行动以及数据要素素养提升行动。

12 月 18 日，青岛市人民政府发布《青岛市公共数据管理办法》。办法共 8 章 52 条，主要围绕公共数据收集与汇聚、公共数据共享、公共数据开放、公共数据利用、公共数据安全等方面做出规定。

管理办法明确，公共管理和服务机构是本机构公共数据质量责任主体，应当按照规定开展公共数据治理工作，建立公共数据质量检查和问题数据纠错机制，对收集、产生的公共数据进行校核、确认，确保公共数据完整、准确、可用。公共管理和服务机构提出共享需求应当遵循最少、够用原则，明确公共数据应用场景，承诺其真实性、安全性、合规性。公共管理和服务机构通过共享获取的公共数据，应当专事专用、规范使用，不得扩大使用范围，不得以任何形式提供给第三方。大数据工作主管部门、公共管理和服务机构依法委托第三方服务机构开展信息化项目建设以及运行维护的，应当按照国家和省有关规定对第三方服务机构进行安全审查，签订公共数据安全保密协议，并监督第三方服务机构履行公共数据安全保护义务。（来源：青岛市人民政府）

5. 安徽省数据资源管理局发布《安徽省公共数据授权运营管理办法（试行）（征求意见稿）》

12 月 7 日，安徽省数据资源管理局发布《安徽省公共数据授权运营管理办法（试行）（征求意见稿）》。征求意见稿共 7 章 32 条，适用于在安徽省行政区域范围内开展公共数据授权运营及其相关管理活动。

征求意见稿明确，运营主体在公共数据运营平台上，通过隐私计算、联邦学习、数据模型等安全、合规、可信的方式加工处理公共数据，提供公共数据产品，实现“原始数据不出域、数据可用不可见”。运营主体根据授予的公共数据加工使用权、数据产品经营权，按照提供的公共数据产品的价值贡献获取合理收益。运营主体应当向社会公示公共数据产品和服务能力清单，并定期披露公共数据运营情况。（来源：安徽省数据资源管理局）

6. 河北石家庄市数据资源管理局发布《石家庄市公共数据管理规定（征求意见稿）》

12 月 11 日，河北省石家庄市数据资源管理局发布《石家庄市公共数据管理规定（征求意见稿）》。

征求意见稿明确，公共数据有下列情形之一的，不予开放：（一）开放后危及或者可能危及国家安全的；（二）开放后可能损害公共利益的；（三）涉及个人信息、商业秘密或者保密商务信息的；（四）法律、法规规定不得开放的。涉及个人信息、商业秘密或保密商务信息的公共数据有下列情形之一的，可以列入有条件开放或者无条件开放数据：（一）涉及个人信息的公共数据经匿名化处理的；（二）涉及商业秘密、保密商务信息的公共数据经脱敏、脱密处理的；（三）涉及个人信息、商业秘密、保密商务信息的公共数据指向的特定自然人、法人或者非法人组织依法授权同意开放的。（来源：石家庄市人民政府）

7. 重庆市人民政府办公厅印发《数据要素市场化配置改革行动方案》

12 月 20 日，重庆市人民政府办公厅印发《数据要素市场化配置改革行动方案》。

方案明确四项重点任务，分别是：（1）构筑坚实的数据资源基础。健全公共数据管理机制，加大数据资源供给，充分挖掘数据应用场景；（2）创新数据要素确权授权制度。探索分类开展数据资产登记，规范公共数据授权运营，推动企业数据和个人信息数据授权使用；（3）加快培育数据交易流通市场。健全数据要素合规交易流通规则体系，加快升级西部数据交易中心，加快培育数据交易流通生态，推动数据区域间合作与跨境有序流通，推动数据资产评估和金融创新，建立数据收益分配制度；（4）加强数据要素市场安全监管。完善数据安全管理制度，强化数据安全监管，创新数据流通监管。（来源：重庆市人民政府）

8. 贵州省大数据发展管理局印发《关于建设贵州省一体化公共数据资源体系工作方案》

12 月 26 日，贵州省大数据发展管理局印发《关于建设贵州省一体化公共数据资源体系工作方案》，旨在加强公共数据资源归集治理、共享应用和开放开发，促进数据高效流通。

方案明确四项重点任务，分别是：（1）构建一体化公共数据基础设施体系。建设公共云平台体系，建设公共数据平台，建设公共数据区；（2）构建一体化公共数据归集治理体系。编制全量公共数据目录“一本账”，

规范维护公共数据目录，合规采集公共数据，分级分类归集公共数据，提升公共基础数据和主题数据归集水平，加强公共数据质量管理；（3）构建一体化公共数据共享应用体系。深化公共数据共享，拓展公共数据场景应用；（4）构建一体化公共数据开放开发体系。加快公共数据开放，推进公共数据开发利用。（来源：贵州省大数据发展管理局）

9. 上海市人大常委会通过《上海市推进国际贸易中心建设条例》，探索建立合法安全便利的数据跨境流动机制

12 月 28 日，上海市人大常委会通过《上海市推进国际贸易中心建设条例》，自 2024 年 2 月 1 日起施行。

条例明确，上海市创建“丝路电商”合作先行区，在中国（上海）自由贸易试验区及临港新片区的海关特殊监管区域打造中心功能区，对接国际高标准电子商务规则，促进数字经济国际合作。上海市网信、发展改革、经济信息化、通信管理、公安、商务等部门应当在国家有关部门的指导下，开展跨境数据流动分类分级管理，探索建立合法安全便利的数据跨境流动机制，推动数字身份认证在数字贸易领域的应用，促进数据跨境安全、自由流动，鼓励国内外企业及组织依法开展数据跨境流动业务合作。上海市网信、经济信息化、商务、知识产权、通信管理等部门应当在数字贸易主体监管、个人信息保护、重要数据出境等方面协调联动，加强风险防范，规范数字贸易治理。上海市网信、发展改革、经济信息化等部门应当实施数据安全管理认证制度，引导企业提升数据安全管理能力和水平。（来源：上海人大）

境内前沿观察三：治理实践

导读：网络谣言、网络暴力打击治理是2023年公安、网信等部门监管重点之一。12月，公安部通报全国公安机关依法严厉打击整治网络谣言违法犯罪活动举措成效情况。在侦办网络谣言类、网络暴力类违法犯罪案件的同时，全国公安机关高度重视各类网站平台在相关违法犯罪案件中的作用，持续加强平台综合治理。公安机关以重大网络谣言案件为切入点，拉网式排查网站平台漏洞问题，通过警告、责令整改、罚款等措施查处了一批不履行主体责任和义务的平台，并不断加强互联网安全监督检查，敲打整治各类网站平台1.2万家次。此外，公安部党委决定将2024年作为打击整治网络谣言专项行动年，部署全国公安机关开展为期一年的专项行动。公安机关也将强化源头治理，压实平台责任，对网络谣言案事件频发、实名制落实不到位、产品风险漏洞多的网络平台，采取提醒、约谈、限期整改等措施，对整改不力的依法依规严肃查处。

国家安全机关会同有关部门开展地理信息数据安全风险专项排查治理，指导、协助涉事单位开展清查整改，及时消除重大数据窃密、泄密等安全隐患。中央网信办开展为期一个月的“清朗·整治短视频信息内容导向不良问题”专项行动，集中整治短视频传播虚假信息、展示不当行为、传播错误观念三类突出问题。

结合12月公布的行政案件中的违法行为，组织在开展合规工作时应注意以下方面：1.制定内部安全管理制度和操作流程，建立健全全流程网络

数据安全管理制度，依法组织开展网络数据安全教育培训；2. 确定网络安全负责人；3. 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，采取相应技术措施和其他必要措施保障数据安全；4. 设立防火墙，安装网络流量监测软件，及时更新安全策略，并按要求留存访问日志；5. 定期开展等级评测；6. 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。需要注意的是，除《网络安全法》《数据安全法》《个人信息保护法》等法律外，组织还需对自身所处行业领域的特殊性规定保持关注，如证券行业的《证券期货业网络和信息安全管理办法》，落实相应安全保护义务，避免法律风险。

关键词：网络谣言违法犯罪、平台责任、短视频专项整治行动、地理信息数据安全风险专项排查治理

（一）公安机关治理实践

1. 公安部通报打击整治网络谣言违法犯罪活动举措成效：侦办网络谣言类案件4800余起

12月22日，公安部在京召开新闻发布会，通报全国公安机关依法严厉打击整治网络谣言违法犯罪活动举措成效情况。

发布会指出，全国公安机关依法严厉打击扰乱社会公共秩序的造谣传谣违法犯罪活动。截至目前，全国公安机关已侦办网络谣言类案件4800余起，依法查处造谣传谣人员6300余名，依法关停违法违规账号3.4万个。同时，依法严厉惩治造谣诽谤等网络暴力违法犯罪活动。截至目前，共查处网络暴力违法犯罪案件110起，刑事打击112人，行政处罚96人，批评教育472人，指导重点网站平台阻断删除涉网络暴力信息2.7万条，禁言违规账号500余个。此外，公安机关持续加强各类网站平台综合治理。一方面，立足公安机关职责定位，坚持以打促治、以打促管，以重大网络谣言案件为切入点，拉网式排查网站平台漏洞问题，通过警告、责令整改、罚款等措施查处了一批不履行主体责任和义务的平台；同时不断加强互联网安全监督检查，敲打整治各类网站平台1.2万家次。

发布会表示，公安部党委决定将2024年作为打击整治网络谣言专项行动年，部署全国公安机关开展为期一年的专项行动。针对网站平台的监管举措和工作安排方面，发布会表示，下一步，公安机关将立足综合监管和行政执法职能，研究采取多项综合治理措施，强化源头治理，压实平台责

任。一是对网络谣言案事件频发、实名制落实不到位、产品风险漏洞多的网络平台，采取提醒、约谈、限期整改等措施，对整改不力的依法依规严肃查处；二是充分动员互联网企业、行业协会、网民志愿者、科研院所等共同参与网络谣言乱象治理，推动纠治自媒体、电商、文娱等领域“流量为王”的价值取向；三是逐步探索建立黑名单制度，并从单个平台向多平台、全平台推广，限制造谣传谣劣迹人员从事内容生产行业。（来源：公安部网安局）

2. 因网络安全管理不到位，四川多家单位被处罚

12 月 17 日，网信四川发布两起网络安全行政处罚案例。

案例一：四川省某医院遭受网络攻击，造成全院系统瘫痪。公安机关迅速调集技术力量赶赴现场，指导相关单位开展事件调查和应急处置工作。经调查发现，该医院未制定内部安全管理制度和操作流程，未确定网络安全负责人，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，导致被黑客攻击造成系统瘫痪。公安机关根据《网络安全法》第二十一条和五十九条，对该院处以责令改正并警告的行政处罚。

案例二：四川省某单位互联网门户网站被攻击篡改，公安机关第一时间督促采取应急处置措施，并立案对该单位遭受攻击事件开展调查，通过工作发现，该单位信息系统未按规定设立防火墙，未安装网络流量监测软件，未记录网站访问日志，未采取防范计算机病毒和网络攻击、网络入侵等危害网络安全行为的技术措施，网站建设完成至今，未更新安全策略、未落实等级测评等安全防护措施。公安机关根据《网络安全法》第二十一

条、第五十九条之规定对负有主体责任的该单位作出罚款1万元，对直接责任人作出罚款5千元的行政处罚；对托管单位某公司作出罚款1万元、对直接责任人作出罚款5千元的行政处罚。（来源：网信四川）

3. 陕西西安警方公布多起网络安全行政执法案件

12月28日，陕西省西安市公安机关公布多起网络安全行政执法案件。

案件一：西安经开网警

2023年10月，境外黑客对某科技股份有限公司所属“OA系统”实施远程漏洞攻击窃取文件信息，该公司属于高精尖技术产业科技公司，其内部存储有大量敏感、重要数据。按照“一案双查”原则，经开网警对该单位进行网络安全监督检查。经查，该公司未履行网络安全保护义务、未按照相关法律规定采取防范网络攻击、网络入侵等危害网络安全行为的技术措施，造成严重网络安全后果和恶劣社会影响。根据《网络安全法》第五十九条第一款，西安经开网警分别依法对该公司主体及其网络安全直接责任人予以行政处罚。

案件二：西安西咸网警

2023年9月，陕西某网络科技有限公司报案称其在陕西某数联信息技术有限公司租赁的服务器遭受网络攻击，导致三台服务器上存放的200余个网站无法打开。按照“一案双查”原则，西咸网警对该单位进行网络安全监督检查。经查，该网络科技有限公司将网站存放于租赁的服务器上以来，未履行网络安全保护义务、未按照相关法律规定采取防范网络攻击、网络入侵等危害网络安全行为的技术措施，导致其公司服务器遭受网络攻

击无法打开，客户网站关停、被篡改为色情网站，造成严重网络安全后果和恶劣社会影响。根据《网络安全法》第二十一条、第二十五条、第五十九条，西安西咸网警依法对涉事公司及相关负责人予以行政处罚。

案件三：西安莲湖网警

西安莲湖网警在工作中发现，辖区某单位重要网站被篡改并植入涉黄非法暗链，警方立刻对该公司开展网络安全事件处置工作，最终确认暗链所在位置并及时清除。按照“一案双查”原则，莲湖网警对该单位进行网络安全监督检查。经查，该公司未履行网络安全保护义务，未采取网络安全技术保护措施、未落实网络安全保护管理制度，造成恶劣社会影响。根据《网络安全法》第二十一条、第五十九条，西安莲湖网警依法对该单位开具《整改通知书》,限期一个月完成整改,尽快消除网络安全风险隐患。（来源：西安网警）

4. 北京警方破获一起利用“撞库”破坏计算机信息系统案

12 月 1 日消息，北京警方近日破获一起破坏计算机信息系统案件。

本案中，北京警方接到辖区内一互联网公司报案，称该公司的求职招聘类app的短信验证码接口遭受攻击达 1300 余万次。这次攻击还成功匹配注册账号 30 余万个，造成经济损失的同时危及群众信息安全。北京警方迅速研判，确定这是一起黑客利用网站漏洞非法获取账号信息并用于违法活动的案件。

针对此案件，北京市公安局网安总队会同朝阳分局立即成立专案组开展侦查，最终确定喻某有重大作案嫌疑，迅速在四川省自贡市将其抓获。

据喻某交待，其于2022年10月18日注册该招聘网站账号，数次尝试验证接口。他发现该网站的签名算法相对单一，于是利用此弱点编写指令，制作黑客软件，对该网站进行撞库攻击。同时喻某还长期使用类似的方式对其它各大网站进行渗透并伺机查找网站漏洞，并以此为诱饵向他人兜售自己编写的恶意程序和黑客工具，从中牟取利益。

通过对喻某的审查，一个集编写恶意程序、实施撞库攻击、泄露数据资料为一体的“撞库黑客”团伙逐渐浮出水面。在办案民警的不懈努力下，专案组成功在四川成都将另一名嫌疑人焦某抓获，现场起获各类公司、人员数据330余万条。据交待，该人以3000元的价格从喻某手中购来其编写的恶意程序，长期在境外网站盗卖由撞库非法获取的大量公民个人信息及公司账号数据，并使用虚拟币进行交易。

目前，犯罪嫌疑人喻某、焦某因破坏计算机信息系统被依法刑事拘留，案件正在进一步办理中。（来源：公安部网安局）

5. 山西警方破获一起利用“地推”侵犯公民个人信息案

12月15日消息，山西省晋中市公安机关近日破获一起侵犯公民个人信息案。本案中，2022年8月，郭某某组织陈某某、杨某、乔某某等人在“地推群”中购买手机号码与手机验证码，并用之注册某电商APP账户。同年10月，山西省晋中市公安局城区分局网安大队将犯罪嫌疑人郭某某、陈某某等人抓获。

经郭某某供述，他们买到账号后通过专用软件操作，在手机号码原机主不知情的情况下登陆原机主的某电商APP，领取APP账户内的优惠券来低

价购买物品并倒卖。之后，他们再将注册好的某电商APP账户二次贩卖给其他人，从中获利。经查，自2022年8月以来，犯罪嫌疑人郭某某、陈某某等人从多个地推群里购买了4519个电话号码和注册某电商APP账户的验证码。其中，未注册过某电商APP账户的电话号码和验证码价格14元至16元不等，已注册过某电商APP账户的电话号码和验证码价格7元至9元不等。后郭某某通过微信将某电商APP账户转卖至其他人。其中，新注册的某电商APP账户价格16元至17元不等，已注册过的某电商APP账户价格11元至12元不等。截至被查，郭某某通过倒卖某电商APP账户共获利5.2万元。

近日，此案宣判。被告人郭某某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑四年，并处罚金人民币八万元。被告人陈某某犯侵犯公民个人信息罪，判处有期徒刑一年五个月，缓刑二年，并处罚金人民币一万二千元。（来源：公安部网安局）

6. 新疆公安厅公布8起典型案例，包含涉嫌帮助信息网络犯罪活动案等

12月16日，新疆维吾尔自治区公安厅公布8起典型案例，其中包括两起涉嫌帮助信息网络犯罪活动案，两起侵犯公民个人信息罪案以及一起提供侵入、非法控制计算机信息系统程序、工具案。具体案件如下：

（一）王某等人涉嫌帮助信息网络犯罪活动案。2023年2月9日，呼图壁县公安机关发现，辖区居民王某等人帮助电信网络诈骗团伙实施“跑分”洗钱违法犯罪活动，涉案金额巨大。目前，公安机关依法对王某、伊某等8人以帮助信息网络犯罪活动罪移送检察机关起诉。

（二）张某、赖某涉嫌帮助信息网络犯罪活动案。2023年3月15日，塔城市公安机关工作发现，犯罪嫌疑人张某、赖某二人以注册公司方式，办理多个固定电话，架设GOIP设备，帮助境外电诈团伙实施电信诈骗违法犯罪活动。塔城市人民法院以帮助信息网络犯罪活动罪，分别判处张某有期徒刑一年六个月、赖某有期徒刑一年。

（三）马某涉嫌提供侵入、非法控制计算机信息系统程序、工具案。2023年9月26日，托里县公安机关工作发现，辖区网民马某利用APP漏洞，编写软件协议非法获取公民个人信息。目前，公安机关依法对马某以提供侵入、非法控制计算机信息系统程序、工具罪，移送检察机关起诉。

（四）买某侵犯公民个人信息案。2023年7月20日，库车市公安机关工作发现，辖区网民买某利用电信营业厅代办点工作之便，非法获取大量手机号、验证码和居民身份证信息，批量注册、贩卖各类平台网络账号，非法牟利2.5万余元。目前，公安机关依法对买某采取刑事强制措施。

（五）丁某侵犯公民个人信息案。2023年9月15日，喀什市公安机关工作发现，辖区网民丁某利用从事装修行业工作之便，非法贩卖公民个人信息9800余条，非法牟利1.3万余元。目前，公安机关依法对丁某采取刑事强制措施。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办开展“清朗·整治短视频信息内容导向不良问题”专项行动

12 月 5 日，中央网信办发布通知，自即日起开展为期一个月的“清朗·整治短视频信息内容导向不良问题”专项行动，集中整治短视频传播虚假信息、展示不当行为、传播错误观念三类突出问题。

专项行动强调加强短视频平台管理。一是优化推荐机制。着力解决短视频平台算法价值导向存在偏差、优质短视频呈现不足等问题。优化流量分配机制，防止“重指标轻质量”，片面以点赞率、转发率等量化指标作为流量分配依据。二是强化平台审核把关。着力解决短视频平台审核机制不规范和审核标准不够全面等问题，防止出现审核过于简单化或一刀切以及人工复审走过场等现象。（来源：网信中国）

2. 网信部门依法查处花椒直播、天天吉历 APP 等破坏网络生态案件

12 月 29 日消息，针对花椒直播、天天吉历APP、超级手电筒APP、大姨妈APP等网站平台破坏网络生态问题，国家网信办近日指导北京市、上海市网信办，依据《网络安全法》《网络信息内容生态治理规定》等有关规定，依法约谈上述网站平台负责人，责令限期整改、从严处理责任人，整改期间采取自行暂停新用户注册、暂停问题版块信息更新等处置措施。

经查，花椒直播“跳舞”版块多名主播在直播中存在衣着暴露、行为挑逗等问题，平台未有效履行主体责任，未采取防范和抵制措施，在重点环节呈现上述不良信息，违反《网络安全法》《网络信息内容生态治理规定》相关规定。北京市网信办约谈花椒直播负责人，责令其整改7日，整改期间自行暂停“跳舞”版块信息更新，全面排查清理低俗不良信息，依法依约处置账号，从严处理相关责任人。

超级手电筒APP在首页首屏“娱乐头条”版块推荐大量娱乐明星隐私八卦等不良信息，炒作绯闻、丑闻、劣迹，平台未有效履行主体责任，未采取防范和抵制措施，在重点环节呈现上述不良信息，违反《网络安全法》《网络信息内容生态治理规定》相关规定。北京市网信办约谈超级手电筒APP负责人，责令其整改30日，整改期间自行暂停“娱乐头条”版块信息更新，从严处理相关责任人。

大姨妈APP首屏“她说”版块多名用户发布色情网站链接等违法违规信息和低俗不良信息，平台未有效履行主体责任，对用户发布的违法违规信息未停止传输、采取消除等处置措施，违反《网络安全法》《网络信息内容生态治理规定》相关规定。北京市网信办约谈大姨妈APP负责人，责令其整改30日，整改期间自行暂停新用户注册功能，从严处理相关责任人。

天天吉历APP“运势测算”等多个版块提供有偿算命、占卜服务，宣扬封建迷信，平台未有效履行主体责任，对上述违法违规信息未采取停止传输、消除等处置措施，违反《网络安全法》《网络信息内容生态治理规定》相关规定。上海市网信办约谈天天吉历APP负责人，责令其全面下线封建迷信违规版块，在稳妥处置用户退款后限期自行关闭。（来源：网信中国）

3. 2023年北京市App收集使用个人信息专项检查成效显著

12月29日，北京市委网信办公布2023年北京市App收集使用个人信息专项检查成果。自2023年5月起，北京市委网信办组织开展2023年度北京市App收集使用个人信息专项检查。检查涵盖下载量靠前、密切关系民生的39类271款App，并对20家重点App运营企业进行数据安全风险现场检查。专项检查共排查整改违规收集使用个人信息问题788项，数据安全风险215项，问题总量相较去年下降30%，有力推动改善属地App违规收集使用个人信息情况。

综合分析检查情况，违规问题呈明显集中态势，仅前两项占比高达86.34%。其中，“违反必要原则，收集与其提供的服务无关的个人信息”现象最为突出，占总数的63.34%，主要体现在两个方面：一是收集的个人信息或调用的权限与实际业务功能并无直接关联，二是当用户拒绝提供非必要的个人信息或权限时，App会拒绝提供服务。此外，“未明示收集使用个人信息的目的、方式和范围”问题占比较高，达到23%。

现场检查发现，多家App运营企业存在数据安全风险：一是安全管理风险，如数据资产梳理不完整、数据分类分级存在偏差、安全管理制度落实不到位等；二是数据处理活动风险，如账号权限分配不合理、缺乏敏感数据管控手段等；三是安全技术风险，如缺乏数据库敏感操作行为审计、未定期对日志进行备份等。（来源：网信北京）

4. 北京市网信办启动加强未成年人网络保护专项行动

12 月 30 日，北京市网信办发布《关于启动加强未成年人网络保护专项行动的公告》，决定自 2024 年 1 月 1 日起，在属地网站平台开展为期 3 个月的未成年人网络保护专项行动。本次专项行动立足广大网民反映强烈的典型乱象，集中整治内容导向不良、未成年人网络沉迷、个人隐私保护不力 3 类 9 个方面影响未成年人身心健康的突出问题。（来源：网信北京）

5. 因存在数据泄露，重庆市渝中区网信办对某科技公司处以 10 万元罚款

12 月 11 日消息，因数据泄露，重庆市渝中区网信办近日对某科技公司处以 10 万元罚款。

本案中，渝中区网信办根据上级部门移交的线索，查实发现某科技公司开发运营的某OA信息系统因未履行好网络数据安全保护义务，导致大量数据泄露，情节严重。且该公司作为网络数据处理者，未依法建立健全全流程网络数据安全管理制度，未依法组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施等保障网络数据安全。

该公司上述行为违反《网络安全法》《数据安全法》《个人信息保护法》等法律法规。渝中区网信办依据《数据安全法》规定，对该公司作出限期五日改正、给予行政警告，并处罚款 10 万元的行政处罚。目前，该公司已完成整改，建立健全相关管理制度，并全额缴纳罚款。（来源：网信重庆）

6. 因未及时处置系统漏洞，重庆市丰都县网信办依法对属地某网站作出行政处罚

12 月 16 日消息，重庆市丰都县网信办近日依法对属地某网站进行立案查处。经查，该网站没有及时履行处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险的义务，违反《网络安全法》第二十五条规定，丰都县网信办依据《网络安全法》第五十九条规定，对该单位予以行政警告处罚，并责令其限期整改。（来源：网信重庆）

7. 因存在未授权访问漏洞，重庆市南岸区网信办依法约谈区级某部门

12 月 29 日消息，重庆市南岸区网信办近期巡查发现区级某部门业务系统存在未授权访问漏洞情况。南岸区网信办依据《网络安全法》《党委（党组）网络安全工作责任制实施办法》有关规定，对该部门进行约谈，要求该部门严格落实网络安全工作主体责任和本行业本领域的网络安全指导监管责任，紧紧围绕网络安全风险防范，开展自查整改。（来源：网信重庆）

8. 因扫码付停车费被诱导关注商场公众号，上海市网信办会同静安区网信办约谈“兴业太古汇”

12 月 18 日，上海市网信办会同静安区网信办依法约谈“兴业太古汇”运营企业冠丰（上海）房地产发展有限公司，要求企业立即整改，切实维护消费者的合法权益。约谈中，企业参加人员未得到充分授权，整改态度

不积极。约谈明确指出，若企业拒不改正，网信部门将依据《个人信息保护法》严肃查处。

本案中，网民举报“兴业太古汇”商场在消费者停车缴费服务中存在违法收集个人信息的情况。经核实，该商场停车场未提供“纯净版”停车码等便捷缴费方式，同时存在缴费入口设置隐蔽、诱导用户关注商场公众号，以及隐私政策需要消费者提供“身份证号码”等个人信息授权同意（但技术检测并没有实际收集）等问题。

目前“兴业太古汇”商场停车场已完成初步整改。针对扫码缴费环节诱导消费者关注商场公众号的问题，企业已在停车场主要通道、墙柱、进出口的明显位置张贴“纯净版”停车缴费二维码，标注“即刻缴费，快速出库”。针对隐私政策需要消费者提供“身份证号码”等个人信息授权同意（但技术检测并没有实际收集）的问题，新版隐私政策已修改相关条款表述并上线。（来源：网信上海）

9. 因未尽生成信息审核管理义务，福建宁德网信办对属地一公司罚款 10 万元

12 月 30 日消息，福建省宁德市网信办近日依据《网络安全法》对属地一网站运营公司罚款 10 万元 。经查，该公司所属网站存在法律、行政法规禁止发布或者传输的信息，网站运营主体未能履行主体责任，未能尽到对生成信息的审核管理义务，违反《网络安全法》第四十七条的规定。依据《网络安全法》第六十八条规定，宁德市网信办对该公司依法作出行政处罚的决定，责令其关闭网站，并处人民币 10 万元罚款。（来源：网信福建）

（三）通信管理部门治理实践

1. 工信部组织开展网络安全保险服务试点工作

12 月 14 日，工信部办公厅印发通知，组织开展网络安全保险服务试点工作。

试点险种主要包括网络安全财产类保险和网络安全责任类保险两大类。网络安全财产类保险，主要保障因网络安全事件造成的第一方直接损失以及因此产生的技术服务费用，包括直接物理损失、营业中断损失、数据资产重置费用、硬件改善成本、应急处置费用，以及因网络安全事件导致的公关费用、法律费用等。网络安全责任类保险，主要保障因网络安全事件引起的对第三方个人或机构需要承担的赔偿责任，包括数据泄露责任、网络安全事件责任、媒体侵权责任、外包商相关责任、产品责任或技术服务职业责任等。

试点对象分为两类，一是企业类，以企业法人为被保险方，主要保障网络安全事件对其造成的财产损失或赔偿责任，面向电信和互联网、工业互联网、车联网等重点行业；二是产品服务类，以产品服务的购买方为保障对象，主要保障因网络安全事件造成的财产损失或赔偿责任，面向网络安全产品、网络安全服务和信息技术产品。（来源：工信部）

2. 工信部等十四部门部署开展网络安全技术应用试点示范工作

12 月 15 日，工信部、国家网信办、人力资源社会保障部等十四部门联合印发通知，部署开展网络安全技术应用试点示范工作。

试点示范工作将面向公共通信和信息服务、人力资源社会保障、水利、卫生健康、应急管理、广播电视、金融、交通运输、邮政等重要行业领域网络和数据安全保障需求，从基础网络安全、云计算安全、人工智能安全、大数据安全、信创安全、商用密码、车联网安全、物联网安全、中小企业数字化转型安全、网络安全共性技术、网络安全创新服务、教育技术产业融合发展联合体、网络安全“高精尖”创新平台等13个重点方向，遴选一批技术先进、应用成效显著的试点示范项目。（来源：工信部）

3. 工信部加快培育数据要素市场，推进数据高效流通

12月26日,工信部产业政策与法规司在国务院政策例行吹风会上表示，推动建设全国统一大市场，在深化数据要素市场化改革、培育数据要素市场方面，既要推进数据的高效流通、市场化配置，又要发挥数据要素作用，更好赋能产业发展。

发布会指出，围绕推动数据要素高效流通，工信部主要开展了三方面工作：一是加强政策引导，推动构建数据基础制度体系；二是完善标准体系，组织开展数据领域标准研究，发布33项国家标准；推进数据流通交易、数据资产登记等标准研究和试点示范，加快建立健全数据市场标准规范；三是培育经营主体。主要是支持平台企业、龙头企业参与数据要素市场建设，引导数据交易机构开展跨地域服务，培育多样化的数据服务型企业。

下一步，工信部将进一步加大工作力度，加强产品主数据标准服务平台建设，持续开展大数据产业发展示范，支持各类经营主体探索数据利用模式，加强数据交易流通、开放共享、安全认证、工业数据资产登记等制

度规范的研究制定，加快培育数据要素市场，扎实推进数据高效流通，赋能产业发展。（来源：国新网、新京报）

4. 工信部、多地通信管理局通报问题 APP

（1）工信部

12 月 15 日，工信部通报 2023 年第 9 批，总第 35 批侵害用户权益的APP（SDK）。通报指出，工信部近期组织第三方检测机构对群众关注的实用工具、本地生活、网络游戏等APP及SDK进行检查。发现 24 款APP、SDK存在侵害用户权益行为，涉及欺骗误导强迫用户、强制频繁过度索取权限、超范围收集个人信息、应用分发平台上的APP信息明示不到位、违规收集个人信息等内容。通报要求相关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）浙江省通信管理局

12 月 1 日，浙江省通信管理局通报 2023 年第 10 批侵害用户权益的APP。通报指出，浙江省通信管理局近期组织第三方检测机构对群众关注的实用工具、网上购物、即时通讯等类型APP进行检查，并书面要求违规APP开发运营者限期整改。截至目前，尚有 9 款APP未按要求完成整改，现予以通报。请上述APP开发运营者在 12 月 11 日前完成整改落实工作，整改落实不到位的，将视情采取下架、关停、行政处罚等措施。9 款APP所涉问题为强制、频繁、过度索取权限，违规收集个人信息，违规使用个人信息。

（3）广东省通信管理局

12 月 27 日，广东省通信管理局公开通报 4 款未按要求完成整改APP。通报指出，广东省通信管理局近日持续开展APP隐私合规和数据安全专项整治行动，发出《违法违规APP处置通知》责令APP运营者限期整改，并通知相关应用商店协助督促APP运营者整改。截至目前，尚有“家慧库”“福袋生活”等 4 款APP未完成整改，现予以通报。被通报的APP应在 2024 年 1 月 4 日前完成整改及反馈工作。4 款APP所涉问题为强制、频繁、过度索取权限，违规收集个人信息，违规使用个人信息。

同日，广东省通信管理局宣布下架 4 款侵害用户权益的APP。通报指出，截至通报规定时限，经核查复检，尚有“肇庆市博物馆参观预约”“点购广场”等 4 款APP未按照要求完成整改反馈。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。

（4）北京市通信管理局

12 月 29 日，北京市通信管理局通报 2023 年第十一期问题APP。通报指出，近期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。截至通报之日仍有“智慧树”“学而思科学”等 7 款APP未整改或整改不到位，现予以通报。同时，11 月 30 日曾通报本市部分存在侵害用户权益行为的APP并要求整改，截至通报之日仍有“艺考生”等 4 款APP

未整改或整改不到位，现予以全网下架处置。（来源：工信部，浙江省、广东省、北京市通信管理局）

（四）其他部门治理实践

1. 国家安全机关会同有关部门开展地理信息数据安全风险专项排查治理

12 月 11 日消息，国家安全机关近期在工作发现，我国有关重要行业领域使用的境外地理信息系统软件存在搜集外传地理信息数据的情况，部分数据重要敏感，甚至涉及国家秘密，对我国家安全构成严重威胁。针对上述情况，国家安全机关会同有关部门开展地理信息数据安全风险专项排查治理，指导、协助涉事单位开展清查整改，及时消除重大数据窃密、泄密等安全隐患。（来源：国家安全部）

2. 上海高院发布 10 个服务保障数字经济发展典型案例

12 月 18 日，上海市高级人民法院发布 10 个服务保障数字经济发展典型案例。典型案例按照“涉个人信息处理或利用网络侵害其他人格权案件”“涉数据形态财产权益及市场竞争秩序保护案件”“涉平台经营者/数据算法运用者法定义务及相关主体权益保护案件”“涉侵害数据形态权益、利用数据技术实施网络犯罪及黑灰产业防治案件”四大分类研究体系梳理而成，涉及刑事、民事等各个审判领域。

在第一类“涉个人信息处理或利用网络侵害其他人格权案件”中，有一起“员工个人信息合理使用的认定案”。某实业公司在未征得其关联公司离职人员同意的情况下，将其手机号码作为企业联系方式对社会公示，给离职人员生活和工作带来不利影响。人民法院判决解除该手机号与公示信息的绑定及关联，并支持了离职人员要求实业公司赔礼道歉的诉请，为员工个人信息的合理使用判定提供重要指引。（来源：上海市高级人民法院）

3. 北京市人民检察院发布《北京市检察机关网络犯罪检察白皮书》及维护网络安全和数据安全典型案例

12 月 19 日，北京市人民检察院发布《北京市检察机关网络犯罪检察白皮书》，通报北京市检察机关维护网络安全和数据安全典型案例。

白皮书显示,2021 年以来,北京市检察机关办理网络犯罪案件共计 8203 件 11625 人。案件主要呈现以下特点和趋势：一是数字经济新业态伴生犯罪增长态势明显；二是网络犯罪向民生领域侵蚀蔓延；三是黑灰产业链为网络犯罪“输血供粮”；四是匿名“洗钱”手段助推上游犯罪滋生；五是互联网企业数据安全存在风险隐患。

会议发布 8 起维护网络安全和数据安全典型案例，包括利用抢号软件抢挂医院就诊号、通过软件控制考场电脑屏幕帮助他人考试作弊、以“投资引流”方式帮助实施电信网络诈骗犯罪、通过“暗网交易”非法买卖公民个人信息、假借网络交易平台名义实施新型传销活动等类型。（来源：京检在线）

4. 因 APP 个人信息保护合规性检测不充分等多项违规行为，黑龙江证监局对江海证券公司出具警示函

12 月 25 日，黑龙江证监局公开《关于对江海证券有限公司采取出具警示函措施的决定（监管措施〔2023〕20 号）》。

决定显示，江海证券有限公司存在以下问题：一是关于IT治理、网络安全管理的内部决策、执行机制不健全，违反《证券期货业网络和信息安全管理办法》（证监会令第 218 号）第九条第一款规定；二是公司APP个人信息保护合规性检测不充分，存在APP强制、频繁、过度索取权限问题，违反《证券期货业网络和信息安全管理办法》第三十条规定。

根据《证券期货业网络和信息安全管理办法》第六十二条第二款规定，决定对该公司采取出具警示函的行政监管措施。完成上述整改工作后，应报送整改报告。（来源：中国证券监督管理委员会）

境外前沿观察：月度速览十则

导读：12 月，美国总统拜登签署《2024 财年美国国防授权法》，向国防部拨款 8167 亿美元，强化网络安全管理，启动半导体供应链网络安全试点计划，实施网络边界和跨域防御现代化计划对抗网络攻击，同时，扩大对中国经济和技术能力的年度评估及汇报范围，重点关注中国在人工智能等技术方面的情况。欧盟理事会与欧洲议会就《网络弹性法案》达成临时协议，对数字产品全生命周期提出强制性网络安全要求。

美国对 TikTok 的打压还在继续，美国亚拉巴马州、犹他州、田纳西州、俄克拉荷马州、得克萨斯州、马里兰州、南卡罗来纳州在内的 7 个州宣布在州政府设备或网络上禁用 TikTok。

英国北爱尔兰警察局披露英国警务史上最大数据泄露事件审查结果，包含警局在职员工敏感信息的标签被隐藏在 Excel 电子表格中，但工作人员在发布该表格前没有注意到这一点。审查报告认为该事件并非由个人、团队或部门单个决定、行为或事件造成，是北爱尔兰警察局作为一个组织没有更好、更主动地保护其数据安全，及早识别和预防风险导致的。

关键词：供应链网络安全、禁用 TikTok、警察局数据泄露、政府机构服务中断

1. 美国总统拜登签署《2024 财年美国国防授权法》，强化网络安全管理，中美技术竞争凸显

12 月 22 日，美国总统拜登签署《2024 财年美国国防授权法》，向国防部拨款 8167 亿美元。该法中网络安全相关要点包括：（1）国防部承担国防工业基础网络安全和关键基础设施保护的责任；（2）启动半导体供应链网络安全试点计划，降低由网络攻击引起的对设计、制造、组装、封装和测试供应链的干扰风险；（3）实施网络边界和跨域防御现代化计划对抗网络攻击，在 2026 年 10 月前将现代化网络边界防御能力扩展到国防部信息网络的所有互联网接入点。

该法纳入多项与中国相关的内容，要点包括：（1）不再将中国认定为发展中国家，并将寻求在现有的以及正在协商中的各个国际条约中，移除对中国的发展中国家定位，转而认定为发达国家；（2）扩大对中国经济和技术能力的年度评估及汇报范围，评估中国在人工智能、下一代能源技术、生物技术方面的情况，确定中国与上述技术相关的竞争实践以及美国在这些技术供应链中的脆弱性；（3）加强对受限移动应用的管理，国防部对美国政府和美国国防信息网络中安装 Tiktok 以及其他字节跳动开发的软件的情况进行审查汇报。（来源：美国国会）

2. 欧盟就《网络弹性法案》达成协议，强化数字产品安全

11 月 30 日，欧盟理事会与欧洲议会就《网络弹性法案》达成临时协议，对数字产品的全生命周期提出强制性网络安全要求。法案要求数字产品只有满足特定网络安全基线要求时才能上市销售，并且要求制造商将网络安全嵌入数字产品的设计开发中。面向最终用户方面，法案要求制造商在向用户告知网络安全方面保持透明度。

此次达成的临时协议针对法案提出以下建议：（1）简化法案所涵盖的数字产品的分类方法；（2）明确企业主动向国家主管当局报告漏洞和安全事件的义务，并强化欧盟网络安全局职能；（3）为小微企业提供合规支持。（来源：欧洲议会）

3. 美国 7 个州相继宣布政府设备禁用 TikTok

12 月以来，美国对 TikTok 的打压还在继续，美国亚拉巴马州、犹他州、田纳西州、俄克拉荷马州、得克萨斯州、马里兰州、南卡罗来纳州在内的 7 个州宣布在州政府设备或网络上禁用 TikTok。

5 日，南卡罗来纳州州长宣布所有由该州行政部门管理的政府电子设备禁止访问 TikTok。6 日，马里兰州州长以 TikTok 引发国家安全担忧为由，发布网络安全紧急命令，禁止该州政府雇员在政府部门平台上使用 TikTok。此外，其他一些中国和俄罗斯的产品和平台也在封禁之列。7 日，得克萨斯州州长对该州政府机构发布禁令，禁止在政府下发的设备上使用 TikTok，原因是担忧这款中国公司拥有的应用程序处理有关美国基础设施的数据和

其他敏感数据信息。8 日，为应对所谓 TikTok 对美国国家和网络安全构成的持续威胁，俄克拉荷马州州长发布行政令，禁止州政府机构、相关雇员和承包商在政府网络或政府下发的设备上使用 TikTok。10 日，田纳西州州长办公室称已经采取措施，在所有接入该州政府网络的设备上禁止使用 TikTok。12 日，美国亚拉巴马州、犹他州州长以国家数据安全为由，宣布在州政府设备或网络上禁用 TikTok。（来源：路透社、环球网）

4. 意大利云服务商被黑，上千个政府机构服务中断、数据丢失

12 月 8 日，意大利云服务提供商 Westpole 遭遇网络攻击，殃及 Westpole 客户、政务服务商 PA Digitale。PA Digitale 通过旗下 Urbi 平台为地方政府机构和组织提供服务，服务对象包括 1300 家公共管理机构，其中有 540 家为市政机构。这是意大利公共管理部门迄今为止遭受的最严重网络攻击。

对此，意大利国家网络安全局发表声明称，已恢复遭受攻击的涉及 700 多家与 PA Digitale 公司供应链相关的国家和地方公共实体数据，对于其他管理部门，约 1000 家公共实体与 PA Digitale 公司签订各类管理服务提供合同，攻击发生当日之前 3 天至今的数据尚未恢复。（来源：安全内参）

5. 英国北爱尔兰警察局发布警务史上最大数据泄露事件审查结果

12 月 11 日，英国北爱尔兰警察局披露英国警务史上最大数据泄露事件审查结果。2023 年 8 月，北爱尔兰警察局发生网络安全事件，9483 名警官和文职人员的个人数据遭到泄露，其中包括警局在职员工的姓氏和姓名缩

写、军衔或级别以及工作地点和部门。该事件是英国警务史上最重大的数据泄露事件。

审查报告指出，上述包含警局在职员工敏感信息的标签被隐藏在 Excel 电子表格中，但工作人员在发布该表格前没有注意到这一点。该事件并非由个人、团队或部门的单个决定、行为或事件造成，是北爱尔兰警察局作为一个组织没有更好、更主动地保护其数据安全，及早识别和预防风险导致的。目前，包括平民和警官在内的 4000 多名员工正在对北爱尔兰警察局采取法律行动，这些诉讼可能会让北爱尔兰警察局损失 2400 万至 3700 万英镑。（来源：英国北爱尔兰警察局）

6. 乌克兰最大移动运营商遭黑客攻击瘫痪

12 月 12 日，乌克兰最大移动运营商“基辅之星”总裁表示，该公司的通信基础设施“遭到非常强大的黑客攻击，部分基础设施损坏”。从当天早上 7 点起，拥有 2400 万用户的“基辅之星”断网引发乌全国性移动通信和互联网接入瘫痪，乌克兰国家储蓄银行等多家金融机构报告当天遭到网络攻击并出现大范围服务终端瘫痪。此外，“基辅之星”断网还导致乌首都基辅市、基辅州、苏梅州、第聂伯罗彼得罗夫斯克州、切尔卡瑟州、利沃夫州等多个州的市政及防空警报系统出现故障。乌克兰国家安全局同日在社交媒体发文表示，俄罗斯特种部队可能参与了此次网络攻击，国家安全局已对该事件展开刑事调查。（来源：新华网）

7. 欧盟根据《数字服务法》对社交网络 X 平台启动正式诉讼

12 月 18 日，欧盟委员会宣布对 X 启动正式程序，以评估 X 是否在风险管理、内容审核、黑暗模式、广告透明度和研究人员数据访问等方面违反《数字服务法》（DSA），这是自 DSA 实施以来首例针对大型在线平台的正式诉讼。

正式程序将围绕四个方面展开调查：（1）非法内容的传播，研究 X 是否采取充分措施遏制非法内容在其 1.12 亿欧洲用户中传播；（2）X 打击虚假信息的有效性，是否让用户在帖子和广告中标记非法内容以便迅速删除，以及 X 是否遵守了自身对于敏感内容的限制政策；（3）透明度，是否限制研究人员访问 X 的数据及其广告数据库；（4）欺骗性设计，X 的界面涉嫌通过“黑暗模式”欺骗用户。如果被证实有违反 DSA 的行为，X 最高可被处以其全球收入 6%的罚款。（来源：欧盟委员会）

8. 美国 NSA 发布《2023 年度 NSA 网络安全回顾》，强调国家安全系统与人工智能安全

12 月 19 日，美国国家安全局（NSA）发布《2023 年度 NSA 网络安全回顾》，详细介绍 2023 年 NSA 在网络安全方面的工作进展，要点包括：（1）保护国家安全系统（NSS）。NSA 向国防部承包商提供免费的网络安全服务，这些服务得益于 NSA 在编码和解码方面几十年的专业知识，旨在防御外国对手针对美国国防工业基础设施发起的攻击活动。2023 年，得益于积极宣传和发展，NSA 的网络安全服务采用率提升 4 倍。NSA 正在向国防部供应链

内的600多家公司提供网络安全协助，包括一些缺乏足够网络安全资源的供应商；（2）保障人工智能应用安全。NSA在网络安全协作中心下设立人工智能安全中心，推动在国家安全系统和国防工业基础设施中对人工智能进行安全开发、集成和采用。中心还充分利用NSA独特的外国情报见解，帮助业界了解对手如何使用、针对人工智能。通过深化与美国行业领导者、国家实验室、学术界、情报界以及国际合作伙伴的合作，中心将协助制定人工智能安全最佳实践和指导方针。（来源：美国国家安全局）

9. 美国众议院要求阿里、SHEIN等多家中国电商对数据安全相关问题作出答复

12月20日，美国众议院能源与商业委员会，创新、数据和商务小组委员会致函TikTok、Whaleco、SHEIN、阿里巴巴等多家中国电商，要求在2024年1月12日前对数据安全等问题作出答复。信中要求相关公司说明的问题包括：（1）要求第三方采取的数据实践；（2）要求服务提供商采取的数据实践；（3）对未成年人的数据保护措施；（4）确认是否收集宗教信仰、政治观点、遗传数据等敏感个人信息；（5）应用程序签名密钥存储位置及保护措施；（6）移动应用程序或后端安全测试频率、测试人员、测试标准；（7）移动应用程序组件及开发者信息等。（来源：美国众议院）

10. 美国商务部启动半导体供应链审查，重点关注中国制造芯片的采购与使用

12 月 21 日，美国商务部宣布将于 2024 年 1 月启动一项重要的半导体供应链审查，以解决来自中国芯片的“国家安全”担忧，重点关注美国关键行业供应链中中国制造的传统芯片的使用和采购情况。美国商务部称，半导体供应链审查有助于促进传统芯片生产的公平竞争环境，解决外国政府威胁美国传统芯片供应链的非市场行为。在过去十年中，中国向半导体行业提供约 1500 亿美元补贴，给美国和其他外国竞争对手创造“不公平的全球竞争环境”。总部位于美国的公司约占全球半导体收入的一半，但在外国补贴的支持下面临着激烈竞争。对此，中国驻华盛顿大使馆回应称，美国“不断扩大国家安全概念，滥用出口管制措施，对其他国家企业实行歧视性和不公平待遇，将经济和科技问题政治化、武器化”。（来源：美国商务部、中国驻华盛顿大使馆）

行业前沿观察一：工业互联网安全

导读：随着工业互联网技术的广泛应用，制造业正加速迈入数字化转型升级的重要阶段，与此同时，工业互联网环境也面临着前所未有的安全威胁与挑战。面对日益频繁的网络攻击与数据安全事故，如何保障安全稳定运营，已成为企业数字化转型面临的重大课题。

关键词：网络安全，工业互联网，安全隐患，企业数字化转型

1. 工业互联网安全形势严峻

随着工业互联网技术的广泛应用，制造业正加速迈入数字化转型升级的重要阶段，与此同时，工业互联网环境也面临着前所未有的安全威胁与挑战。面对日益频繁的网络攻击与数据安全事故，如何保障安全稳定运营，已成为企业数字化转型面临的重大课题。

安全事件频发，政策持续强化安全保障措施

2023 年以来，勒索软件的活动十分猖獗，在数量上再次创下历史新高。据 Zscaler 发布的《2023 年全球勒索软件报告》显示，截至 2023 年 10 月，全球勒索软件攻击数量同比增长 37.75%，勒索软件的有效攻击载荷激增了 57.50%。

近来，知名企业也频频成为勒索攻击的目标，导致运营受到严重影响。10 月，江森自控国际公司遭遇大规模勒索攻击，要求支付 5100 万美元赎金；11 月，澳大利亚环球港务集团遭网络攻击，导致四大港口数以万计的货物集装箱滞留在码头。此外，黑客组织、勒索团伙、国家级 APT 等也频繁制造麻烦，使得工业互联网安全形势更加复杂严峻。

在此背景下，各国对工业互联网安全的认识不断提升，并将其视为关键基础设施的守护者。为了应对不断演变的网络威胁，各国都在积极推动工业互联网安全技术的研发与应用。2023 年以来，我国也出台了多项政策以加强安全保障，推动工业互联网安全产业的健康发展。

2023 年 1 月，工信部、国家网信办、国家发展改革委等十六部门联合发布《关于促进数据安全产业发展的指导意见》提出到 2025 年，数据安全产业基础能力和综合实力明显增强，建成 5 个省部级及以上数据安全重点实验室，攻关一批数据安全重点技术和产品。

2023 年 2 月，中共中央、国务院印发了《数字中国建设整体布局规划》指出要强化数字中国关键能力，其中包括筑牢可信可控的数字安全屏障，切实维护网络安全，完善网络安全法律法规和政策体系。

2023 年 10 月，工信部就《工业互联网安全分类分级管理办法（公开征求意见稿）》公开征求意见，指出要建立健全企业内部网络安全管理制度，积极将网络安全纳入企业发展规划和工作考核，加大网络安全投入，加强网络安全防护能力建设，有效防范化解网络安全风险。

2023 年 12 月，工业和信息化部发布通知，组织开展网络安全保险服务试点工作，以促进企业提升网络安全风险应对能力，积极利用网络安全保险防范网络安全风险，完善网络安全风险管理体系。

企业发力，助力工业互联网安全生态链蓬勃发展

今年以来，工业互联网安全领域的企业不仅在技术手段和产品方面进行了大量创新，还通过不断研发和优化，为工业互联网安全生态链的发展提供了强有力的支持。例如，中国联通研究院与安恒信息共同组建工业互联网安全联合创新实验室。该实验室将围绕技术标准及规范制定、工业互

联网安全实验环境及安全靶场等方面开展研究，为工业互联网安全行业的生态链创新发展积极赋能。

上海松江区政府与浪潮云洲签署战略合作协议，浪潮云洲工业安全产业总部项目落户松江，政企携手全力构筑主机安全、边界安全、应用安全、数据安全等全方位安全防护体系，共建安全产业高地。

广东联通发布自主研发的“天玑·工业安全平台”。该平台纳管超200个产品，拥有在线等保、在线密评、安全纳管等优势能力，可为工业企业提供安全技术体系化、安全数据集中化、安全管理可视化、安全服务标准化、安全运营流程化的全生命周期安全保障服务。

在工业互联网迅猛发展的背景下，安全标准的统一显得尤为重要。然而，工业互联网安全方案千差万别，服务能力参差不齐，尚未形成统一的安全框架模式和安全标准。

尽管安全标准的统一仍然面临挑战，但探索的步伐从未停歇。2023年，由我国牵头提出的网络安全国际标准ISO/IEC 24392：2023《网络安全 工业互联网平台安全参考模型》发布，用于解决工业互联网应用和发展过程中的平台安全问题，可系统指导工业互联网企业及相关研究机构，针对不同的工业场景，分析工业互联网平台的安全目标，设计工业互联网平台安全防御措施，增强工业互联网平台基础设施的安全性。

面对复杂多变的网络威胁环境，多元化的攻击手段时刻提醒着我们工业互联网安全防护的重要性。确保工业系统的可用性、可靠性和安全性，

不仅是技术挑战，更是全社会共同的责任。展望未来，相信工业互联网安全能够呈现更加乐观而积极的趋势，为工业的可持续发展提供坚实的保障。

（来源：工联网 iitime 作者：刘艳玲）

2.工业互联网安全领域首个 ISO/IEC 国际标准发布

近日，从全国信息安全标准化技术委员会官网获悉，我国牵头提出的国际标准 ISO/IEC 24392：2023《网络安全 工业互联网平台安全参考模型》（以下简称《IIP 参考模型》）正式发布。

《IIP 参考模型》国际标准用于解决工业互联网应用和发展过程中的平台安全问题，可以系统指导工业互联网企业及相关研究机构，针对不同的工业场景，分析工业互联网平台的安全目标，设计工业互联网平台安全防御措施，增强工业互联网平台基础设施的安全性。

ISO/IEC 24392 作为工业互联网安全领域的首个国际标准，首次提出了基于工业互联网平台安全域、系统生命周期、业务场景三个维度的视角洞察工业互联网安全。

该国际标准适用于解决工业互联网应用和发展过程中的平台安全问题。在该标准的指导下，工业互联网企业及相关研究机构可以针对不同工业场景分别制定工业互联网平台安全方案，设计防御措施，增强工业互联网平台基础设施的安全性。

当前，我国已经把工业互联网建设作为战略建设之一，成为推动新型工业化的关键基础设施组成部分，是加快制造强国和网络强国建设的关键路径。目前，工业互联网已成为国家关键信息基础设施的重要组成部分，

其自身安全则是产业安全和国家安全的重要基础和保障。《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》《十部门关于印发工业互联网安全工作的指导意见的通知》《工业互联网发展行动计划(2021-2023 年)》等国家政策对工业互联网安全建设也相继提出了明确的要求和期望。

该提案于 2018 年 4 月提交至 ISO/IEC JTC1/SC27，2019 年 6 月正式立项，近日正式发布。标准发布后被英国直接采纳为其国家标准。本标准将推动工业互联网平台研发在技术层面达成国际共识，从而实现工业互联网平台的安全技术保障，对我国先进工业发展产生全方位、深层次、可持续的积极影响。（来源：北京工业大学）

3. 工业互联网网络安全突出问题及安全技术

工业互联网网络一般由组织内外网构成，内网包括办公网、控制网、现场生产网、管理网和专用网；外网包括无线网、移动网、互联网和骨干网。工业互联网网络的具体组成主要包括设备、服务等，如工业通信网关、通信模组、交换机、光纤接入等设备，工业无线、工业专线、深度覆盖、标识解析等服务。网络安全侧主要涉及网关隔离、访问控制、工业防火墙和安全态势感知系统。

工业互联网网络体系将连接对象延伸到工业全系统、全产业链、全价值链，打通“人、机、料、法、环”等全要素，实现设计、研发、生产、

管理、服务等深度互联，促进了端到端网络、5G+、边缘计算等关键技术与工业互联网的融合应用。

工业互联网网络易受攻击性

互联互通性是释放工业互联网全部潜在价值的关键所在，但却系统性地增加了网络攻击面。当工业互联网中的装置、设备、系统等全面连接广域分布的公司网络甚至互联网时，攻击者将可以从多个角度实施网络攻击，攻击来源可以来自外部或内部。安全通信、安全网络监控、安全数据和现场设备级别的安全代码执行等信息安全技术机制是必不可少的，而不是可选择的。工业互联网的信息安全问题将更加复杂多样，大规模网络连接因素(如工业云、工业大数据、供应链等)产生的影响将占有重要地位，工业控制设备、系统等生产要素将与网络泛在化和持久化连接，而跨范围的网络连接将为攻击者提供入侵破坏重要工业生产过程的多种可能性和可行性。

工业互联网网络架构脆弱性

工业互联网网络脆弱性可能由网络配置、硬件、边界监控、通信验证或无线网络连接引起，包括：设计不合理的网络架构，没有足够的信息安全防护措施；未存储网络详细配置文件或缺少备份，在无线网络边界接入点位置缺少身份认证机制或身份认证不完善，对网络密码的错误管理措施；没有定义明确的网络安全边界，防火墙缺失或配置不当，导致网络控制设置不足以满足系统的安全防护要求；未配置网络流量监控技术措施，特别

是未使用加密机制的标准协议，如远程终端协议(Telnet)或文件交换协议(File Exchange Protocol，FTP)；未部署完整性检查(网络中存在未经授权的设备)技术机制，缺少用于数据机密性保护的协议加密(例如在无线连接中)机制等。

工业互联网网络协议脆弱性

工业互联网协议脆弱性是有线和无线通信中使用的协议所固有的，如缺少消息身份认证、缺少消息加密等，工业控制系统网络脆弱性可能由网络配置、硬件、边界监控、通信验证或无线网络连接引起，包括：设计不合理的网络架构，没有足够的信息安全防护措施；未存储网络详细配置文件或缺少备份；在无线网络边界接入点位置（例如，在无线客户端和接入点之间)缺少身份认证机制或身份认证不完善；对网络密码的错误管理措施，如使用默认密码、密钥存储未加密、不定期更改密码；使用不安全的网络端口；没有定义明确的网络安全边界；防火墙缺失或配置不当；网络控制设置不足以满足工业控制系统的安全防护要求；未配置网络流量监控技术措施；使用没有增加加密机制的标准协议，如 Telnet 或 FTP；未部署完整性检查(网络中存在未经授权的设备)技术机制；缺少用于数据机密性保护的协议加密(例如在无线连接中)机制等。

工业互联网安全技术

分段分层技术

工业互联网中各层次网络不能不加区别地相互连接，工业安全国际标准(如 ISA/IEC 62443-1-1、NIST SP 800-821)建议将网络分成若干部分，并且每个部分包含具有类似安全策略和通信要求的资产。为每个网段都分配一个信任级别，并保护通过网络边缘的通信连接过程，特别是保护不同信任级网段之间的通信和连接。

网络分段细粒度划分的候选对象包括公共网络、商业网络、运营网络、工厂网络、控制网络、设备网络、保护网络和安全网络。分段技术可以提供有效的流量管理，尽管每个可以访问管理和操作网络的双端口设备，都可以作为从一个网络跳转到另一个网络的攻击的中心点，但分段技术限制了攻击面的影响范围，可以最大化地降低安全威胁带来的影响。

网关过滤技术

工业网关过滤技术可以从网络接口的一条或多条消息中提取特定类型的应用程序级信息，并将该信息转发到另一个网络中，同时不保留原始网络消息结构的任何部分。网关还可以对重要的应用程序功能进行编码，例如，可以将工业互联网中的 IT 与 OT 接口位置的双端口历史数据服务器看作一个双向信息网关，具有明显的持续性分析功能。历史数据服务器使用工控设备专用通信协议，通过一个网络接口从 OT 网络收集数据，并使用客户机/服务器协议通过第二个网络接口将数据发布到 IT 网络。通过为不同种类的网关提供不同程度的安全防护能力，重要的工业互联网过滤技术包括以下几个流程。

第一层过滤：物理隔离是指网段与任何外部网络之间不存在有线或无线方式的在线连接。物理隔离是最强大的过滤形式，但不能提供任何形式的连接。

第二层过滤：分离物理网络中的信令系统，但转发开放系统互联(Open System Interconnection，OSI)模型第二层的网络帧，托管交换机和桥接防火墙是基于以太网媒体访问控制(Media Access Control，MAC)地址或其他设备级寻址过滤消息的典型技术。虚拟局域网(Virtual Local Area Network，VLAN)交换机用于流量管理，但其本身并不是安全设备，因此不建议将VLAN作为不同信任级别网段的边界保护技术措施。

第三/四层过滤：最常用的工业互联网消息过滤器是指能够根据网络地址、端口号和连接状态过滤消息的防火墙，这种过滤技术被称为包过滤器和状态检测。

网络防火墙技术

工业互联网网络防火墙广泛用于分割复杂的工业互联网的网络，大多数防火墙是第二层、第三层或第四层IP路由器/消息转发器，具有复杂的消息过滤器。防火墙的形态可以是物理设备或虚拟网络设备，防火墙的过滤功能检查防火墙接收到的每条消息。如果筛选器确定消息符合防火墙配置的流量策略，则消息将传递到防火墙的路由器组件以进行转发。防火墙也可以重写消息，最常见的方式是通过执行加密或网络地址转换(Network Address Translation，NAT)。

设备级防火墙旨在保护终端节点，可以是具有深度包检查功能的传统防火墙，或具有深度包检查过滤器的第二层 IP 路由器，后者可以在不重新配置现有终端设备中的路由规则的情况下进行部署。

上文提到的过滤器技术(自学习过滤技术)可用于设备防火墙应用程序级过滤，该技术通过监视一段时间内的流量，并自动创建过滤规则，将所有观察到的流量标识为正常和允许的流量。学习模式完成后，可以将防火墙配置为仅转发符合筛选器的流量，并丢弃所有其他流量。同时，可以设置可配置操作，允许某些应用程序级的内容通过，并禁止其他无关的内容。例如，允许写入某些现场控制设备寄存器，而不是其他寄存器的策略；允许读取和写入任何寄存器，但不允许下载现场控制设备固件的策略。

网络访问控制技术

工业互联网网络访问控制结合网络控制和网络安全控制，允许或限制对通信网络的逻辑访问。一个众所周知的授权访问机制是 IEEE 802.1X，基于每个设备的凭据(如身份证书及用户名和密码)，允许或拒绝设备访问网络，IEEE 802.1X 允许网络运营商对可以在网络中通信的设备集合保持强大的控制。

在一些情况下，网络设备可以同时具有认证者和请求者的特征。请求者从身份认证器请求访问，该身份认证器将访问请求转发给身份认证服务器以供审查。完成认证之后，交换机或无线接入点启用端口或无线连接进行除 IEEE 802.1X 认证帧外的业务，身份认证服务器可以集成到工业现场控制设备中。身份认证服务器也可以作为整个网络的集中资源，通过远程

身份认证接入服务(Remote Authentication Dial In User Service,RADIUS)实现。之后，可以集中管理用户名和密码等访问凭据，并可供作为身份认证程序的所有网络设备访问。此外，用户特定的配置信息可以通过 RADIUS 输出， 并通过 IEEE 802.1X 分配， 例如特定 VLAN 的成员资格。

工业互联网安全体系新技术

态势感知技术

态势感知技术是对相关环境的理解，包括态势数据的收集、分析、警报、呈现、使用操作，以及安全信息的生成和维护活动，有助于形成一个整体的操作图景。在理想情况下，工业互联网安全和实时态势感知应该无缝地跨越 IT 和 OT 子系统，并且不干扰任何正常的工业控制运营业务流程，设计中必须考虑到安全性，应该尽早评估风险，而不是事后考虑安全性。由工业互联网网络安全态势感知系统提供从各种生产现场传感器和设备收集信息所需的“网络-物理-人”的耦合数据，并提供一个报告和控制接口，便于在管理和保护生产与关键基础设施的物理元素时有效地实现人在回路的参与。

工业互联网态势感知对于攻防对抗环境中的人类决策极为重要，安全分析人员必须了解正在发生的事情，以便提高决策的速度和有效性，并确定如何在未来更有效地缓解威胁。态势感知取决于任务的具体背景和任务中个人的角色，传感器和操作数据提供了有关正在发生的事情的原始资料。

大数据分析和人工智能将态势信息转化为对正在发生的事情及对任务的影响，同时可以实现对感知预期结果的理解。

蜜罐和蜜网技术

在工业互联网的上下文中，蜜罐可以以不同的方式实现，其主要取决于应用场景。例如，在 OT 网络中，低交互蜜罐可以模拟网络服务器(例如生产过程中的控制站)的操作，而在现场网络中，蜜罐使用能够模拟远程终端控制系统(Remote Terminal Unit，RTU)操作的实现，如协议仿真器(Supervisory Control and Data Acquisition，SCADA)。在企业的流程控制网络或信息与通信网络中，高交互蜜罐是有足够运行技术条件的(甚至以虚拟机的形式在同一主机上共存)，同时还可以模拟最小服务的低交互蜜罐。此外，在某些情况下，一些针对系统的攻击可以重定向到蜜罐，从而提供有关攻击者及其意图的更多信息。

现场总线蜜罐运行于工业现场控制网络中，与网络中已有的可编程控制器(Programmable Controller，PLC)、RTU、传感器和执行器互联互通和信息共享，并绑定网络中未使用的 IP 地址段。其基本工作原理是：通过最大限度地模拟生产控制环境中的 PLC、RTU 及执行器的行为和服务。现场总线蜜罐主要工作于现场总线层，因此具有较高的迷惑性，可以引诱攻击者更加深信当前面对的是一个值得攻击的目标。同时，通过充当工业互联网的诱饵，向上一级分布式生产控制系统(例如 SCADA 系统、分布式控制系统(Distributed Control System，DCS)的主站系统、PLC 系统的上位机等)发送异常工业互联网设备事件及设备相应 ID，并引导攻击事件的应急响应

过程。现场总线蜜罐的存在形态一般是模拟PLC，模仿真实PLC的行为和操作，也可以模拟RTU、传感器或执行器等。在正常情况下，现场总线蜜罐将等待来自某个探测网络或假冒主站的入侵者试图访问网络的连接尝试。实际上，任何连接该蜜罐设备的尝试都可能产生安全事件，因为根据蜜罐的设计初衷，现场总线蜜罐中的任何活动都是非法和未经授权的(除蜜罐本身的管理操作外)。

密网技术是在蜜罐技术的基础上发展而来的，工业互联网入侵行为的网络特性需要更大范围的诱捕技术，通过在工业互联网网络上设置一些特殊的诱捕机群，并在其上运行专用的模拟软件，模拟工业互联网网络上运行操作系统的主机群，将其并入到网络上的安全域，对其进行低级别的安全保护，可以让入侵者更容易地进入系统。入侵者进入系统后，其所有行为将受到系统软件的监视和记录。通过收集关于入侵者行为的数据，系统软件可以分析入侵者的行为，达到通过蜜网构建网络攻击行为分析模型，吸引攻击者攻击的目的。

人工智能技术下的工业攻防网络

对生产制造企业实施的网络攻击通常分为工业间谍、工业破坏和数据盗窃3类，每类攻击行为追求的目标各不相同，有些目的是获取公司的机密信息，如机器或产品的最新技术发展，而有些目的则是金钱利益。在人工智能协助下实施的网络攻击将更精确、更有效地绕过工业生产控制系统，结合人工和计算机辅助方法的攻击利用办公IT信息系统和生产控制网络中

的各种数据源和通信系统识别漏洞，形成对办公 IT 信息系统、生产控制网络和人工智能系统自身的立体网络攻击。

从宏观层面分析，人工智能辅助的网络攻击有两种基本类型：技术性攻击和对组织结构的攻击。两者之间有时会有一些重叠或差异，不易区分。更简单的攻击类型包括钓鱼攻击——发送大量包含各种恶意软件链接的电子邮件，最广为人知的攻击事件之一是 WannaCry 蠕虫勒索病毒；更智能的攻击类型包括鱼叉式网络钓鱼攻击——在攻击过程中，恶意攻击者将发送个性化的电子邮件，其中包含具有后门功能的特洛伊木马等内容的链接。鱼叉式网络钓鱼攻击也可用于 0-day 攻击，0-day 漏洞是未公开的软件安全缺陷，暂时没有可用的补救补丁程序，攻击者可能会滥用这些漏洞。

工业互联网网络终端安全

工业互联网系统，特别是现场控制设备的组件常使用出厂默认密码，且在默认情况下禁用安全选项。因此，在工业互联网域中安装组件很容易，但非常不安全。一般 30%的工业应用出厂后程序无法更改，并且很难说服工业控制系统制造商研发具有安全功能的产品组件。直到最近几年，在几次工业控制信息安全事件的推动下，一些工业制造商才开始改变其产品的默认安全状态，而与此问题密切相关的威胁是在工业控制设备中包括密码在内的身份认证信息通常不加密，网络攻击者可以在内存中以明文形式，或在通信过程中通过窃听的方式获取这些重要信息。此类威胁的典型案例是一家知名制造商的 PLC 设备外包装清楚地显示钻孔模板，并说明电源插头

和非屏蔽双绞线(Unshielded Twisted Pair，UTP)电缆的连接位置，并且随设备附带的光盘和一份两页的安装手册明确说明可以在连接PLC的网络计算机设备中启动光盘。这导致PLC安装时没有任何密码保护就可以直接连接到互联网。使用Shodan类互联网搜索引擎的恶意攻击者可以很容易发现这些没有任何身份认证保护措施或只有简单防护机制的PLC设备，并进一步控制该PLC设备以实施下一步网络攻击行动。

端侧设备安全技术

终端侧安全防护技术主要有：高效灵活配置的网关过滤技术，易于识别和使用的端点通信策略，基于加密的通信端点之间的强相互认证，通过强制执行从策略派生的访问控制规则的授权机制和加密机制，确保交换信息的机密性、完整性和实时性。其中需要特别注意的是高效灵活配置的网关过滤技术，传统的工业自动控制领域强调信息流保护技术，而工业互联网则倾向于使用加密控制技术同时结合保护技术，例如应用于传输层[如传输层安全性协议(Transport Layer Security，TLS)]或中间件层[如数据分发服务(Data Distribution Service，DDS)]的加密控制等，通过终端侧配合采用各层通信链路相应的安全控制和技术机制来抵御不同的网络攻击。

端侧设备安全流程要点

建立端侧设备安全的第一步是使用支持加密的身份认证协议进行身份认证(如果建立了公钥基础设施，则通过交换身份证书进行身份认证)，然后，通信双方必须根据策略中定义的访问控制规则交换数据。例如，在医疗设备工业系统中，具备采集病人真实的医学指标的终端设备，一般不允

许共享患者的数据。为确保被交换时信息的机密性和完整性，应使用标准加密技术[如高级加密标准(Advanced Encryption Standard,AES)等对称算法和RSA等非对称算法]、消息认证技术和消息认证码，以实现端侧加密。特别需要注意的是，针对不提供交换信息的完整性和机密性的工业互联网通信协议，可以通过加密和认证的隧道式路由，或者通过信息流控制技术进行保护，进而提高这类协议的安全性。这些技术通常使用在进行身份认证过程中协商建立的加密密钥，但应注意避免没有身份认证过程的单纯加密。

此外，由于传统网络安全缺乏考虑工业场景，特别是工业制造厂商对所有机器和设备在各种环境条件下的正常和安全运行有特殊要求。因此，符合气候条件(例如灰尘、湿度、温度等)、机械条件(例如冲击、振动等)和安全条件(例如限制功耗以避免爆炸)要求，需要基于安全性额外考虑加固措施。

（来源：信息安全与通信保密杂志社 作者：郭刚,林紫微,杨超,等）

行业前沿观察二：各地协会动态

导读：各地协会近期开展了精彩纷呈的活动，上海市信息安全行业协会积极响应工信部关于开展“网络安全保险服务试点工作”的要求，举办了“网络安全保险服务试点工作”交流会；重庆信息安全产业技术创新联盟成功召开 2024 年第一次两长工作会议；辽宁省信息网络安全协会组织《数据安全工程师》职业能力网络专题培训班；安徽省计算机信息网络安全协会举办《关键信息基础设施安全保护要求》国家标准宣贯会；湖北省信息网络安全协会成功召开协会第三届一次会员大会暨换届大会；海南省网络安全和信息化协会近期组织开展了专家组换届工作，公示第三届专家组名单；广东省网络空间安全协会“品牌服务系列宣传”栏目正式上线，第一期隆重推出“职称业务报道”，广州市委网信办副主任贺忠一行莅临省协会调研；首届“强基杯”数据安全技能竞赛，新疆参赛选手获得好成绩；2023 年南宁市全民科学素质竞赛圆满落幕。

关键词：协会，活动，网络安全

1. 上海：“网络安全保险服务试点工作”交流会顺利召开

为积极响应工信部关于开展“网络安全保险服务试点工作”的要求，进一步促进网络安全保险服务试点工作的落地，2024 年 1 月 4 日下午，由上海市信息安全行业协会组织举办的“网络安全保险服务试点工作”交流会在普陀区天地科技广场顺利召开。上海市经信委、国家金融监督管理总局上海监管局、普陀区科委的相关领导，以及保险公司、再保险公司、网络安全企业、科研机构、测评机构等单位代表共计 70 余人出席会议。

上海市经信委软件和信息服务业处华宇涵为试点工作提供指导意见，并表示网络安全保险具有巨大的市场潜力和发展空间，市经信委希望能集聚各方资源，推进网络安全保险服务模式创新，促进网络安全保险产业发展。

国家金融监督管理总局上海监管局么炳楠指出，本次交流会突破行业和技术的壁垒，为保司、安全服务企业、科技企业等搭建了交流、合作的平台，期待大家能够推出国内具有领先意义的网络安全保险服务方案并积极推动试点工作落地。

市信安协会兼职副秘书长江群从试点工作背景、网络安全相关险种、试点工作申报要求及流程等进行了详细的介绍，并对一些疑点和难点进行了针对性解读。

会上，保险公司代表平安产险上海分公司政保部陈茜和大地财险营业部创新研发部洪晶晶分析了目前网络安全保险发展趋势及网络安全保险产品体系和模式，介绍了网络安全产品相关险种和应用情况，并对试点工作方向提供相关建议。

最后，参会人员针对网络安全保险服务试点工作展开了讨论和交流，会议在积极的探索声中圆满完成。（来源：上海市信息安全行业协会）

2. 重庆：联盟 2024 年第一次两长工作会议成功召开

2024 年 1 月 4 日，重庆信息安全产业技术创新联盟成功召开 2024 年第一次两长工作会议。

会议由联盟副理事长周彦晖主持，西南大学、重庆信安网络安全等级测评有限公司、全国工业过程测量控制和自动化标准化技术委员会、重庆计算机安全学会、重庆华龙网集团股份有限公司、重庆中兴网信科技有限公司、重庆南华中天信息技术有限公司、西南计算机有限责任公司、绿盟科技集团股份有限公司、重庆市通信建设有限公司、重庆长城计算机系统有限公司等理事单位代表和秘书长出席了本次会议。

会议听取了联盟 2023 年工作总结和财务报告，研究和部署了 2024 年度重点工作，评选了“2023 年度优秀会员单位”。（来源：重庆信息安全产业技术创新联盟）

3. 辽宁：举办《数据安全工程师》职业能力网络专题培训班

2024 年 1 月 4 日，为进一步增强国内行政、企事业单位等在数据安全治理与评估知识方面的了解及应用，从源头上做好数据安全的评估，帮助相关人员了解数据治理的技巧，提升各相关单位的应变能力，培养数据管理高级人才，提供高效、安全的数据治理方法，辽宁省信息网络安全协会发布通知，举办《数据安全工程师》职业能力网络专题培训班。

通知明确，参加培训并通过考试的学员由工业和信息化部教育与考试中心统一颁发《数据安全工程师》工业和信息化职业能力证书。培训内容包括数据安全基础知识和数据安全实务两大部分。线上集中培训时间为 2024 年 2 月 1 日学员线上签到，2 日、3 日全天线上培训。考试时间定为 2 月 4 日，考试方式为线上考试。

通知指出，培训对象包括：

数据安全或个人信息保护工作的主要负责人；信息化工作相关负责人；法律合规部门负责人；数据运营部门负责人；产品、IT、研发、运维部门负责人。

大型软件用户单位信息中心技术主管或分管领导，软件需求方技术负责人或主管领导，软件升级项目负责人、技术主管等；软件开发企业技术主管、项目经理、测试经理等；其他对软件性能设计与测评感兴趣人员均可报名参加。

详情请关注辽宁省信息网络安全协会微信公众号了解通知详情，也可直接联系培训报名负责人邱东，电话：15942337333，邮箱：15942337333@163.com。（来源：辽宁省信息网络安全协会）

4.安徽：《关键信息基础设施安全保护要求》国家标准宣贯会在合肥召开

2023年12月21日上午，为贯彻落实习近平总书记关于“要筑牢网络安全防线、提高网络安全保障能力、强化关键信息基础设施防护”的重要指示精神，学习关键信息基础设施安全保护政策要求，交流贯彻落实安全保护经验心得，安徽省《关键信息基础设施安全保护要求》国家标准宣贯会在合肥顺利召开。安徽省公安厅、省密码管理局、省通信管理管局相关领导出席会议。全省7家关键信息基础设施运营单位及省直65家重点单位共计180余人参加会议。

会议特邀公安部网络安全专家毕马宁分享《深化制度落实 护航数智发展》。随后公安部关保中心的李坤主任从实战化角度解读《关键信息基础设施安全保护要求》。安徽省水利厅，国网安徽省电力有限公司分别发表了关键信息基础设施安全保护经验分享，北京天融信网络安全技术有限公司，深信服科技股份有限公司为关键信息基础设施的安全建设提供了解决思路。

《关键信息基础设施安全保护要求》（GB/T39204-2022）于2023年5月1日起正式实施。此次会议旨在深入贯彻落实《网络安全法》《关键信息基础设施安全保护条例》，推进《关键信息基础设施安全保护要

求》国家标准落地实施，分享重要行业安全保护实践经验，全力做好全省关键信息基础设施安全保护工作。

（来源：安徽省计算机信息网络安全协会）

5. 湖北：省信息网络安全协会召开第三届一次会员大会暨换届大会

2024 年 1 月 19 日，湖北省信息网络安全协会在武汉市召开协会第三届一次会员大会暨换届大会，湖北省省委网信办、省公安厅、省民政厅相关领导出席大会，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。协会全体会员单位参加大会。

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”。大会通过无记名投票，选举产生新一届协会领导班子以及理事会成员。

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，湖北省公安厅网安总队相关领导致辞讲话。

（来源：湖北省信息网络安全协会）

6. 海南：省网络安全和信息化协会公示第三届专家组名单

为推动海南省网络安全人才培养、科技创新、产业融合发展，充分发挥协会专家库专家的技术支撑和辅助决策作用，海南省网络安全和信息化协会（以下简称“协会”）根据《海南省网络安全和信息化协会章程》要求，近期组织开展了专家组换届工作，经推荐报名并由协会理事会研究决定，将协会第三届专家组名单予以公示（排名不分先后）并公开征询意见。第三届专家组共 38 人，应急技术支撑专家 14 人。

（来源：海南省网络安全和信息化协会）

7. 广东：协会“品牌服务系列宣传”栏目正式上线，第一期隆重推出“职称业务报道”

为满足广大会员粉丝群体对业务交流的需求，更多的了解协会，展示协会各业务实力和成绩，扩大合作交流，做好协会的品牌服务宣传，广东省网络空间安全协会决定于 2024 年新年之际开辟“协会品牌服务系列宣传”新栏目，对协会所属品牌服务和成果进行系统宣传。

“品牌服务系列宣传”栏目的开通，增加协会品牌内容的宣发渠道，为广大会员业务交流提供了更多的优质内容，增强了协会的专业服务性。

“职称业务报道”作为广东省网络空间安全协会新年第一期，以“专业 权威 影响”为原则，坚持优质原创特色，围绕评委会成立、服务内容、服务情况等三大版块详细剖析，普及有关职称政策和评审标准，帮助广大专业技术人员尽快熟知申报职称相关要求。

2019 年 9 月，广东省人力资源和社会保障厅正式发出《关于印发〈广东省网络空间安全工程技术人才职称评价制度改革实施方案〉的通知》文件，广东省在全国率先开展网络空间安全工程职称评审工作，成立“广东省网络空间安全工程职称评审委员会”——全国第一个网络空间安全工程职称评委会，方滨兴院士出任职称评审委员会主任。

2021 年 12 月，经广州市人力资源和社会保障局批准，广州网络空间安全协会成立“广州市工程系列网络空间安全工程专业高级职称评审委员会”。2023 年 4 月，经广州市人力资源和社会保障局同意，成立“广州市工程系列网络空间安全工程专业中级职称评审委员会”。

2019 年度至 2022 年度，评委办已组织开展 4 年度职称评审活动，经评审通过并向社会进行公示；每年免费面向社会召开宣贯会、培训会、企业专场、地方专场 10 余场，共计 4000 余人参加了培训。多年来，为网络空间安全行业和社会各界输送了数百名中高级专业网络空间安全人才，为推进行业高质量发展，推动数字经济建设作出了不可磨灭的贡献。

链接

广东省网络空间安全工程职称设置

（1）设置 5 个专业：

网络空间安全技术研究（基础技术、前沿技术、关键技术研究等岗位）

网络空间安全技术应用（系统规划设计、建设运维、应急响应、网络优化等岗位）

网络空间安全系统设计（系统架构设计、关键系统软硬件系统设计、问题解决方案设计等岗位）

网络空间安全系统评测（风险评估、安全测评、产品检测等岗位）

网络空间安全管理监测（标准规范编制、人才培养、态势分析、信息挖掘、安全监管等岗位）

（2）分为三个层级五个等级：

初级职称（技术员、助理工程师）、中级职称（工程师）、高级职称（高级工程师、正高级工程师）。（来源：广东省网络空间安全协会）

8. 广东：广州市委网信办副主任贺忠一行莅临省协会调研

2024 年 1 月 15 日下午，广州市委网信办副主任贺忠一行莅临广东省网络空间安全协会调研，协会会长黄丽玲、副会长黄志豪、总工高宁、党支部专职副书记黄汝锡等热情接待了贺主任一行，并对他们的到来表示热烈欢迎。在黄丽玲会长陪同下，贺忠副主任一行参观了协会办公环境，了解协会架构、平台建设、业务开展等情况。

座谈会上，黄丽玲会长介绍了协会基本情况和主要工作，她说，协会是全国网安联秘书处单位、网民网络安全感满意度调查活动的牵头发起单位，核心团队二十多年以来在全国范围内组织开展过多种形式的网络安全宣传公益活动，有着成熟的运作模式。今年协会将在市委网信办的指导下，以饱满的工作热情、强烈的责任感，围绕网安周重点议题，

组织精干力量、采取多项措施，积极发动各方力量广泛参加2024年网络安全宣传教育活动，让各项活动做细落实，有声有色，深入人心。

协会秘书长周贵招就6年来每年一届的网民网络安全感满意度调查活动的活动规模和组织亮点、取得成效和未来规划做了汇报，并介绍已经走进千家万户的“安全满意四宝”和“安全满意之歌”等活动品牌形象。志愿服务部部长张彦介绍了网安联志愿服务活动总队成立3年以来的队伍规模和运作模式，重点展示“网安联”小程序上积累的成果，包括通俗易懂的“网安课堂”、活泼亲和的动漫和大量专题宣传视频等。

贺忠副主任表示，协会多年来深耕于网络空间领域，拥有雄厚的技术实力和丰富的行业经验，精英团队的专业敬业、原创文化作品的丰富多样，都超出他的预期。他强调，作为广州本土成长的行业协会，今天的成就来之不易，当前是富有活力的信息和网络时代，要坚定理想信念、紧握时代脉搏，在上级部门的正确领导下，继续发挥行业优势、攻坚克难，为网络强国做出应有的贡献。他指出，广州市是2024年国家网络安全宣传周开幕式等重要活动承办城市，作为具有行业代表性的优秀社会组织要积极参与到活动中来，要及时整理积累的网络安全专业知识和各类文化素材、发扬富有创造力和执行力的优良传统，争取在活动中有更多的协助和更美的展示，为今年国家网络安全宣传周在广州的成功举办贡献力量。

会议最后，围绕如何做好2024年国家网络安全宣传周筹备工作进行讨论。黄丽玲会长表示，协会将全力以赴、调动所有平台和人力资源，按照市委网信办的统一部署，高质量完成各项工作任务。

（来源：广东省网络空间安全协会）

9. 新疆：首届“强基杯”数据安全技能竞赛，新疆参赛选手获得好成绩

2024年1月5日，首届“强基杯”数据安全技能竞赛颁奖仪式在2024（第十四届）中国互联网产业年会举行。工业和信息化部网络安全管理局、中国互联网协会及中国信息通信研究院有关领导出席活动。

本届“强基杯”数据安全技能竞赛，由来自全国近100支参赛队伍共280选手从报名参赛的2000名选手中脱颖而出，在本届大赛创设的数据安全实战和数据安全评估两大赛道中激烈角逐，最终经裁判组审核确认，分别决出团队一等奖3项、二等奖5项、三等奖8项。

新疆参赛选手在本届“强基杯”竞赛中获得好成绩：其中，中国移动通信集团新疆有限公司李黔、程纪、崔启龙（天山卫士二队）获首届“强基杯”数据安全技能竞赛全国总决赛数据安全评估赛道一等奖（团队奖）；中国电信股份有限公司新疆分公司李冬、韩冰、张越（我爱吃西红柿队）获首届“强基杯”数据安全技能竞赛全国总决赛数据安全实战赛道二等奖（团队奖）；李黔（中国移动通信集团新疆有限公司）获首届“强基杯”数据安全技能竞赛全国总决赛“数据安全评估精英”称号（个人奖）；李冬（中国电信股份有限公司新疆分公司）获首届“强

基杯”数据安全技能竞赛全国总决赛“数据安全技术能手”称号（个人奖）。希望受表彰的团队和单位，继续发扬成绩，再接再厉，为推动数据安全人才培养和选拔持续贡献力量。　　（来源：新疆互联网协会）

10. 广西：2023 年南宁市全民科学素质竞赛圆满落幕

日前，2023 年南宁市全民科学素质竞赛决赛在南宁师范大学（明秀校区）举行，50 名决赛者用时 90 分钟答 100 道题进行比拼，最终决出特等奖 1 名，一等奖 4 名，二等奖 6 名，三等奖 9 名。南宁市科学才俊和科学知识达人由此产生，此次竞赛圆满落幕。

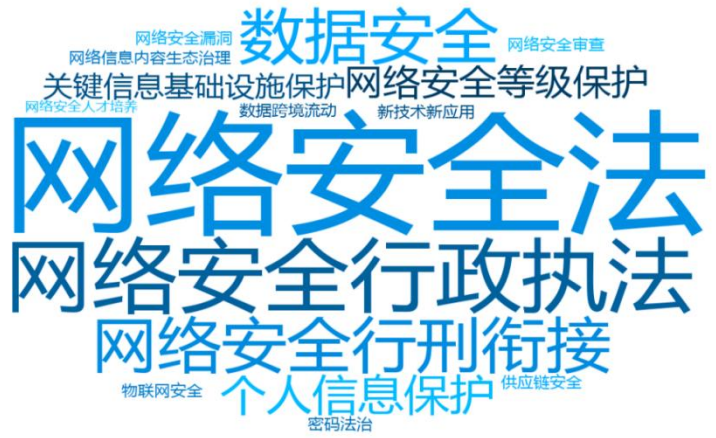
本次竞赛活动于 11 月 4 日拉开帷幕，设初赛、复赛、决赛三个阶段，持续近一个月，旨在普及科学知识、传播科学思想、弘扬科学精神，促进科学意识、创新理念深入人心，持续优化科学素质建设体系，增强南宁市基层科普服务能力。

此次竞赛活动，激发了南宁市公众参与科普知识学习和科普活动的主动性、积极性，为开展类似活动积累了经验。下一步，市科协将继续做好科学普及的各项工作，助力南宁市全民科学素质持续提升，不断开创南宁科普工作新局面。　　（来源：南宁市信息网络安全协会）

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

……