网安联
Wang An Lian

网络与数据安全治理前沿洞察

Frontiers of Regulatory Oversight in CyberSecurity and Data Governance

2023年12月第5期(总第5期)

2023年12月20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

顾 问：严 明 公安部第一、第三研究所 原所长、研究员

中国计算机学会计算机安全专业委员会 荣誉主任

指导专家：袁旭阳 北京网络行业协会 会长

总 编 辑：黄道丽 公安部第三研究所网络安全法律研究中心 主任

副总编辑：鲍 亮 公安部第三研究所网络安全技术研发中心 副主任

编委会主任：黄丽玲 北京网络空间安全协会 理事长

编委会副主任：（排名不分先后）

黎林烽 北京网络空间安全协会 副秘书长

朱方园 上海市信息安全行业协会 副秘书长

于永丰 辽宁省信息网络安全协会 秘书长

闫 东 辽宁省网络安全保障工作联盟 秘书长

孙甲子 黑龙江省网络安全协会 会长

吴晓文 安徽省计算机信息网络安全协会

刘长久 湖北网络安全协会 副秘书长

邓庭波 湖南省网络空间安全协会 秘书长

林勇忠 广东省网络空间安全协会 党支部书记

冯 伟 广西网络安全协会 秘书长

李春报 海南省网络安全和信息化信协会 常务副理事长

戴 勇 贵州省网络安全和信息化协会 常务副秘书长

孙大跃 陕西省信息网络安全协会 会长

卢建宙 甘肃省商用密码行业协会 会长

郑 方 甘肃烽侦网络安全研究院 院长

李学锋 新疆维吾尔自治区互联网协会 秘书长

胡俊涛 郑州市网络安全协会 秘书长

乔　奇 武汉市网络安全协会 副秘书长

樊建功 南昌市网络信息安全协会 会长

王胜军 南宁市信息网络安全协会 会长

邓开旭 成都信息网络安全协会 副秘书长

陈建设 贵阳市信息网络协会 秘书长

杨建东 昆明市网络安全协会 秘书长

沈　泓 宁波市计算机信息网络安全协会 秘书长

卜庆亚 徐州网络安全协会 理事长

孙　逊 佛山市信息协会 秘书长

谢照光 惠州市计算机信息网络安全协 会长

孔德剑 曲靖市网络安全协会 会长

贾辉民 榆林市网络安全协会 会长

编委会委员：（排名不分先后）

黄汝锡 广东关键信息基础设施保护中心 党支部专职副书记

王　嫣 上海市信息网络安全管理协会 部长

林小博 北京安网联认证服务中心 主任

贺　锋 广东中证声像资料司法鉴定所 主任

成珍苑 网安联认证中心 副主任

黎明瑶 广东新兴国家网络安全和信息化发展研究院 研究员

陈菊珍 广东计安信息网络培训中心

潘少芝 揭阳网络空间安全协会 秘书长

编辑部主任：梁思雨

编　辑　部：何治乐 胡文华 王彩玉 王明一 胡柯洋

黎林烽 薛　波 孙翊伦　林 晴 徐瑞雪

发行部主任：周贵招

发　行　部：林永健 张 彦 高梓源

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：11 月，2023 年世界互联网大会乌镇峰会成功举办。国家主席习近平向峰会开幕式发表视频致辞，提出三大倡导，倡导发展优先，构建更加普惠繁荣的网络空间；倡导安危与共，构建更加和平安全的网络空间；倡导文明互鉴，构建更加平等包容的网络空间。

峰会正式发布《中国互联网发展报告 2023》和《世界互联网发展报告 2023》。报告指出，一年来，全球网络安全威胁升级，各国积极布局增强网络安全能力；网络空间法治化趋势明显，多国不断推出细分领域立法；网络空间碎片化程度加剧，生成式人工智能等新技术治理引发全球关注。与此同时，我国网络安全保障体系和能力建设力度加大，数据安全治理基础不断夯实；网络法治化程度不断提高，未成年人网络保护等重点领域网络立法取得突破。

中国工商银行在美全资子公司遭遇勒索软件攻击，部分系统中断。目前已经切断并隔离受影响系统，正在推进恢复工作，工银金融表示未对中国工商银行其他系统产生影响。韩国国家情报院将韩国外交部此前遭遇的网络攻击事件归咎于我国有关部门，我国外交部发言人表示中方一贯坚决反对并打击所有形式的网络攻击。

关键词：三大倡导、网络空间命运共同体、中国工商银行、网络攻击

1. 习近平主席提出三大倡导，推动构建网络空间命运共同体迈向新阶段

11 月 8 日，国家主席习近平向 2023 年世界互联网大会乌镇峰会开幕式发表视频致辞，提出“三大倡导”，为携手推动构建网络空间命运共同体提供重要指引。

一是倡导发展优先，构建更加普惠繁荣的网络空间。深化数字领域国际交流合作，加速科技成果转化。加快信息化服务普及，缩小数字鸿沟，在互联网发展中保障和改善民生，让更多国家和人民共享互联网发展成果。

二是倡导安危与共，构建更加和平安全的网络空间。尊重网络主权，尊重各国的互联网发展道路和治理模式。遵守网络空间国际规则，不搞网络霸权。不搞网络空间阵营对抗和军备竞赛。深化网络安全务实合作，有力打击网络违法犯罪行为，加强数据安全和个人信息保护。妥善应对科技发展带来的规则冲突、社会风险、伦理挑战。中方愿同各方携手落实《全球人工智能治理倡议》，促进人工智能安全发展。

三是倡导文明互鉴，构建更加平等包容的网络空间。加强网上交流对话，促进各国人民相知相亲，推动不同文明包容共生，更好弘扬全人类共同价值。加强网络文明建设，促进优质网络文化产品生产传播，充分展示人类优秀文明成果，积极推动文明传承发展，共同建设网上精神家园。（来源：中国网信网）

2. 《中国互联网发展报告2023》和《世界互联网发展报告2023》蓝皮书发布

11月8日,《中国互联网发展报告2023》和《世界互联网发展报告2023》蓝皮书在2023年世界互联网大会乌镇峰会上正式发布。

《中国互联网发展报告2023》重点展示了一年来中国互联网发展的新情况、新进展、新成效。一年来，数字基础设施“大动脉”作用凸显，5G、IPv6规模部署、算力总规模等多项指标居全球前列；数字经济发展势头强劲，成为稳增长促转型的重要引擎；数据管理体制更加完善，数据基础制度和数据资源体系加快构建；数字政务协同治理效能普遍提升，数字公共服务普惠便捷，“数字为民”成效彰显；网络综合治理体系基本建成，网络生态持续向好，网络空间正能量充沛、主旋律高昂；数字文化产业发展、产品丰富，人民群众精神文化生活多姿多彩；网络安全保障体系和能力建设力度加大，数据安全治理基础不断夯实；中国对人工智能治理的实践探索走在世界前列，为世界提供了中国方案；网络法治化程度不断提高，未成年人网络保护等重点领域网络立法取得突破；网络空间国际交流合作深化拓展，积极搭建国际交流平台，有力推动构建网络空间命运共同体。

《世界互联网发展报告2023》显示，一年来，信息基础设施建设持续推进，逐渐成为大国关注焦点；信息技术创新引领社会变革，人工智能、量子计算等新兴技术进入发展快车道，全球技术合作遭冲击破坏；数字经济成为发展强劲引擎，在全球经济总量中的比重不断增加，多国强化顶层设计和布局；政府数字化转型步伐加快，一体化在线政务服务成趋势；新

技术赋能媒体融合，全球数字娱乐产业发展前景广阔；网络安全威胁升级，各国积极布局增强网络安全能力；网络空间法治化趋势明显，多国不断推出细分领域立法；网络空间碎片化程度加剧，生成式人工智能等新技术治理引发全球关注。（来源：中国网信网）

3. 中国工商银行在美子公司遭勒索软件攻击

11 月 8 日，中国工商银行在美全资子公司--工银金融服务有限责任公司在其官网发布公告称公司遭到勒索软件攻击，导致部分系统中断。工银金融表示，发现攻击后立即切断并隔离了受影响系统，已展开彻底调查并向执法部门报告，正在专业信息安全专家团队的支持下推进恢复工作。工银金融称，中国工商银行及其他国内外附属机构的系统未受此次事件影响，中国工商银行纽约分行也未受影响。（来源：观察者网）

4. 韩国国家情报院将网络攻击事件归咎于中国，外交部回应

11 月 9 日，韩国外交部表示 2022 年 1 月韩国外交部网络系统遭不明黑客攻击。据媒体报道，韩国国家情报院认为相关攻击可能来自中国有关部门。对此，外交部发言人汪文斌在例行记者会上表示：中方一贯坚决反对并打击所有形式的网络攻击。网络安全是各国面临的共同挑战，各方应通过对话合作共同维护网络安全，而不应在没有事实依据的情况下抹黑他国。（来源：中国新闻网）

境内前沿观察二：政策立法动向

导读：11 月，我国积极参与网络空间国际交流与合作，首次提出《国际科技合作倡议》。我国与美英等 28 个国家联合签署首个全球性人工智能声明《布莱切利宣言》，呼吁通过国际合作共同应对人工智能安全风险。

公安部、工信部、国家市场监督管理总局分别发布《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》《网络交易执法协查暂行办法（征求意见稿）》，对联合惩戒、行政处罚裁量基准、执法协查作出规定。这表明在网络安全法治体系基本建成的当下，细化犯罪打击、行政执法各个环节的具体要求，为各部门执法提供规范性指引成为全面推进严格规范公正文明执法、提升法律实施效能的重点关注。

数据仍是地方立法的核心关切，聚焦发挥数据要素价值、探索数据基础制度、推动数据应用、促进数据交易等方面。同时，汽车数据安全及车联网行业发展受到关注。浙江省五部门联合印发《浙江省汽车数据处理管理规定》，江苏省人大常委会通过《关于促进车联网和智能网联汽车发展的决定》，系促进车联网和智能网联汽车发展的全国首部省级地方性法规。此外，广东省人大常委会通过《广东省政务服务数字化条例》，系全国首部政务服务数字化条例。

关键词：全球性人工智能声明、联合惩戒、行政处罚裁量基准、数据要素、汽车数据处理、车联网、政务服务数字化

（一）国家层面动向

1. 中国等 28 国及欧盟签署《布莱切利宣言》，首个全球性人工智能声明

11 月 1 日，首届全球人工智能安全峰会在英国布莱切利庄园召开。中国、美国、英国等 28 个国家代表及欧盟出席并联合签订《布莱切利宣言》。该宣言是全球第一份针对人工智能这一快速新兴技术的国际性声明，旨在关注对未来强大人工智能模型构成人类生存威胁的担忧，以及对人工智能当前增强有害或偏见信息的担忧。

宣言指出，国际社会应认识到开发和使用人工智能需要解决人权保护、透明度和可解释性、公平性、监管与问责制、安全、数字歧视、生成式欺骗性内容、隐私和数据保护等问题。其中，通用人工智能模型可能存在特殊安全问题，故意滥用或意外脱离人类控制问题可能会产生重大风险，尤其应注意网络安全和生物技术等领域的安全风险。同时，人工智能带来的许多风险需要通过国际合作解决。

针对国际合作，宣言提出，通过现有的国际论坛和其他相关组织支持所有人的利益，促进合作，以应对人工智能带来的广泛风险。各国应采取创新且适度的治理和监管方法，以最大限度实现收益提升与人工智能风险降低的平衡。同时，所有参与者都可以在保障人工智能安全方面发挥作用，国家、国际论坛和其他组织需要共同努力。（来源：环球网、英国政府官网）

2. 中国首次提出《国际科技合作倡议》

11 月 7 日，中国在首届“一带一路”科技交流大会上首次提出《国际科技合作倡议》，倡导并践行开放、公平、公正、非歧视的国际科技合作理念，坚持“科学无国界、惠及全人类”，携手构建全球科技共同体。

倡议主要包括以下六方面内容：（1）坚持崇尚科学。坚持科研诚信，尊重科研伦理，塑造科技向善理念，完善全球科技治理。加强知识产权保护，加强对新兴技术发展的包容与审慎管理；（2）坚持创新发展。加强全球科技创新协作，共建全球创新网络，促进新兴技术推广应用，加强企业间创新和技术合作，为世界经济复苏和发展注入新动能。各国应携手推动数字时代互联互通，加快全球绿色低碳转型，实现全人类可持续发展；（3）坚持开放合作。坚决反对限制或阻碍科技合作、损害国际社会共同利益；（4）坚持平等包容。坚决反对将科技合作政治化、工具化、武器化，反对以国家安全为借口实施科技霸权霸凌；（5）坚持团结协作；（6）坚持普惠共赢。要坚持真正的多边主义，探索互利共赢的全球科技创新合作新模式，促进科技创新成果互惠互享。（来源：外交部）

（二）部委层面动向

1. 公安部发布《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》

11 月 13 日，公安部发布《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》。征求意见稿共十九条，主要包括惩戒原则、惩戒对

象、惩戒措施、分级惩戒、惩戒程序、申诉核查六方面内容，遵循依法认定、过惩相当、动态管理原则，将个人和单位纳入惩戒对象的范围，规定金融、电信网络、信用惩戒的具体措施，根据惩戒对象违法行为分级适用惩戒，规范审核认定、惩戒期限和告知等程序，明确申诉、受理、核查、反馈和解除的程序和时限。

征求意见稿坚持依法认定、预防为主，严格按照《反电信网络诈骗法》确定惩戒对象范围和认定标准，列举了依法被实施惩戒的具体行为，区分了设区的市级以上公安机关和省级以上公安机关审核认定惩戒对象的范围，切实强化警示教育，以实现预防犯罪的效果。（来源：公安部）

2. 工信部发布《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》

11 月 23 日，工信部发布《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》。征求意见稿由正文及附件裁量基准组成。其中，正文共五章二十六条，裁量基准共十四项。

征求意见稿明确工业和信息化领域数据安全行政处罚由违法行为发生地的行政处罚机关管辖。数据安全违法行为发生地包括实施违法行为的住所地、实际经营地、工商注册地（工商注册地与实际经营地不一致的，应按实际经营地），网络接入地，取得电信和互联网信息服务相关许可（备案）所在地，网站建立者、管理者、使用者所在地，计算机等终端设备所在地，数据集中存储地、交易地、出境活动所在地等。

征求意见稿明确不履行数据安全保护义务、向境外非法提供数据、不配合监管三类违法行为触发条件；围绕数据级别和数量、损害持续时间、直接经济损失、影响范围等因素，将数据安全违法行为的危害程度划分为“较轻”“较重”“严重”等情节。同时，征求意见稿规定不予处罚、从轻或减轻处罚、从重处罚的适用情形。（来源：工信部）

3. 财政部、国家网信办发布《会计师事务所数据安全管理暂行办法（征求意见稿）》

11 月 2 日，财政部、国家网信办发布《会计师事务所数据安全管理暂行办法（征求意见稿）》，规范会计师事务所数据安全管理。

征求意见稿要求会计师事务所对数据区分核心数据、重要数据、一般数据进行分级分类管理，对数据传输、数据加密、数据备份等事项作出具体规定，对数据管理技术手段、数据存储方式、日志管理等提出具体要求。同时对跨境审计监管中涉及的数据出境事项作出规范。同时，征求意见稿明确会计师事务所应当建立完善的网络管理治理架构，建立健全内部网络管理制度体系，按照业务活动规模及复杂程度配置具备相关职业技能水平的网络管理技术人员，确保合理的网络资源投入和资金投入。（来源：财政部）

4. 文化和旅游部办公厅印发《互联网上网服务行业上云行动工作方案》

11 月 1 日，文化和旅游部办公厅印发《互联网上网服务行业上云行动工作方案》。

方案分为总体要求、主要任务、组织实施三方面内容，明确要推进云服务试点工作，在前期试点工作基础上，不断巩固和扩大上网服务行业云服务试点，积极探索上网服务行业云服务发展方法路径、市场机制，培育云服务发展生态。打造上云创新场所，鼓励各地积极探索上网服务场所云服务发展新模式，打造一批降本增效强、环境品质优、用户体验好、数字化转型成效明显的上网服务行业云服务创新场所——上云创新场所，发挥典型示范和创新引领作用，探索云服务向多元场景应用推广，支持云服务标准建设。（来源：文化和旅游部）

5. 国家市场监督管理总局发布《网络交易执法协查暂行办法（征求意见稿）》

11 月 14 日，国家市场监督管理总局发布《网络交易执法协查暂行办法（征求意见稿）》。

征求意见稿规定，执法协查工作应当遵循合法、合理、高效原则，向平台调取的信息应当遵循“必要且适当”原则，不得超出履行法定职责所必需的范围和限度。平台经营者应当在收到市场监督管理部门限期提供信息通知书之日起十五个工作日内完成协查工作并复函。如协查事项较复杂需延期完成的，平台经营者应当在期限届满前告知提出协查要求的市场监

督管理部门，并说明延期理由、延期期限，延期期限最长不得超过十五个工作日。紧急情况需要加急办理的，市场监督管理部门可以与平台经营者先行沟通情况后履行相应程序，必要时可以请求平台经营者住所地市场监督管理部门协助。（来源：国家市场监督管理总局）

6. 三项网络安全国家标准发布

11 月 27 日，国家市场监督管理总局、国家标准化管理委员会发布中华人民共和国国家标准公告（2023 年第 13 号），全国信安标委归口的三项国家标准正式发布，将于 2024 年 6 月 1 日起实施。

三项国家标准分别是《信息安全技术 网络安全应急能力评估准则》（GB/T 43269-2023）、《信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求》（GB/T 43435-2023）以及《信息安全技术 移动智能终端预置应用软件基本安全要求》（GB/T 43445-2023）。（来源：国家标准化管理委员会）

7. 全国信安标委发布《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》

11 月 1 日，全国信安标委发布《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》。征求意见稿规定粤港澳大湾区跨境处理个人信息应遵循的基本原则和保护要求，为实施粤港澳大湾区个人信息保护认证提供认证依据，也为大湾区个人信息处理者规范个人信息跨境处理活动提供参考。

征求意见稿规定，个人信息处理者跨境处理个人信息，应满足以下要求：（1）制定个人信息跨境安全管理制度和操作规程，采取相应的加密、去标识化等安全技术措施，防范跨境个人信息遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；（2）对个人信息跨境处理活动进行日志记录，个人信息跨境处理日志至少保存 3 年；（3）识别数据跨境处理中涉及的个人信息，形成个人信息跨境处理目录，并及时更新；（4）对被授权跨境访问或查阅个人信息的人员，建立最小授权的访问控制策略，使其只能访问或查阅职责所需的最小必要的个人信息和数据操作权限；（5）承诺接受认证机构对个人信息跨境处理活动的持续监督、包括答复询问、配合检查、服从采取的措施或做出的决定等，并提供已采取必要行动的书面证明。（来源：全国信安标委）

（三）地方层面动向

1. 浙江省五部门联合印发《浙江省汽车数据处理管理规定》

11 月 4 日，浙江省委网信办、省发展改革委、省经信厅、省公安厅、省交通运输厅联合印发《浙江省汽车数据处理管理规定》。规定共计二十六条，旨在进一步规范浙江省汽车数据处理活动，促进汽车数据合理开发利用和汽车行业健康有序发展。

规定明确汽车数据处理者应当：（1）处理汽车数据具有明确、合理的目的，处理的汽车数据类型应与实现产品或服务的业务功能直接关联，同时应遵守对重要数据处理的相关规定；（2）与行业组织、教育和科研机构、

有关专业机构等在数据安全风险评估、防范、处置等方面开展协作，组织数据安全教育培训，落实数据安全管理责任；（3）开展重要数据处理活动应当按照规定开展风险评并向省网信部门和有关部门报送风险评估报告，并在每年十二月十五日前向省网信部门和有关部门报送年度汽车数据安全管理情况。（来源：网信浙江）

2. 浙江省杭州市人大常委会发布《杭州市数字贸易促进条例（草案）》

11 月 8 日，浙江省杭州市人大常委会发布《杭州市数字贸易促进条例（草案）》。草案共计七章四十二条，包括业态模式、主体培育、数字营商环境、开放与合作等内容。

草案规定市人民政府应当依法组织设立数据交易所，推动建设多层次数据要素交易市场，探索建设数据交易国际板。数据交易所应当建立规范、透明、安全可控、可追溯的数据交易环境。鼓励数据交易主体应用区块链、数据安全沙盒、隐私计算等技术探索建立多元化数据流通模式。数字贸易市场主体不得利用算法、数据资源、平台等优势实施垄断和不正当竞争行为。数字贸易市场主体应当依法保护消费者合法权益和个人信息安全。（来源：杭州人大）

3. 湖北省发改委发布《湖北省数据交易管理暂行办法（征求意见稿）》

11 月 7 日，湖北省发展和改革委员会发布《湖北省数据交易管理暂行办法（征求意见稿）》。征求意见稿共计八章三十九条，包括数据交易场所、主体、标的、流程、交易安全等内容。

征求意见稿规定，数据交易场所应当建立全流程数据安全管理制度，设立数据安全负责人和管理机构，组织开展安全教育培训，建立数据交易安全基础设施，采取相应的技术措施和其他必要措施，保障数据安全。数据交易场所应当制定数据安全事件应急预案，定期组织应急演练，提升数据安全事件应对能力。发现泄露、篡改、损毁等数据安全事件，或者数据安全风险明显加大时，数据交易场所应当立即采取补救措施，及时告知数据供需双方，并向有关部门报告。（来源：湖北省发展和改革委员会）

4. 北京数据基础制度先行区启动运行

11 月 10 日，北京数据基础制度先行区启动运行，北京市经济和信息化局发布《北京数据基础制度先行区创建方案》。

方案明确数据先行区总体目标，到 2030 年，北京汇聚高价值数据资产总量达到 100PB，数据交易额达到 100 亿元，数据产业规模超过 1000 亿元。北京将打造“2+5+N”的数据先行区基础设施技术架构：基础设施层包含智能算力基础设施和国家区块链网络枢纽；业务中台层包括数据资产登记平台、数据资产评估平台、数据资产托管平台、数据交易节点、数字资产管

理平台等；数据应用层涵盖金融数据、政务数据、“三医”数据、自动驾驶数据、航运贸易数据、文旅数据等数据专区与应用。（来源：新华社）

5. 国务院批复《支持北京深化国家服务业扩大开放综合示范区建设工作方案》：探索形成既能便利数据流动又能保障安全的机制

11 月 18 日，国务院批复《支持北京深化国家服务业扩大开放综合示范区建设工作方案》。

工作方案明确，推动数据资源开发利用。支持北京积极创建数据基础制度先行区，推动建立健全数据产权制度、数据要素流通和交易制度、数据要素收益分配制度、数据要素治理制度。制定数据交易标准合同指引，出台数据交易负面清单和谨慎清单。在国家数据跨境传输安全管理制度框架下，开展数据出境安全评估、个人信息出境标准合同备案、个人信息保护认证工作，探索形成既能便利数据流动又能保障安全的机制。支持设立跨国机构数据流通服务窗口，以合规服务方式优先实现集团内数据安全合规跨境传输。探索制定自动驾驶、生物基因等行业数据分类分级指南和重要数据目录，以重点领域企业数据出境需求为牵引，明确重要数据识别认定标准，做好数据安全保护支撑。（来源：中国政府网）

6. 北京市十六届人大常委会立法规划发布：涉及《北京市重要信息基础设施网络安全管理条例》等立法项目

11 月 24 日，北京市十六届人大常委会发布《北京市十六届人大常委会立法规划》。规划共确定 82 个具体项目，根据现实紧迫性和项目成熟度分

为两类：一类项目即任期内完成制定、修改的法规，有 42 项；二类项目即任期内调研起草，条件成熟时制定、修改的法规，有 40 项。从领域看，完善首都功能方面有 20 项，推动经济高质量发展方面有 15 项，保障和改善民生方面有 23 项，加强城市治理方面有 19 项，推进京津冀协同发展方面有 5 项。

其中，包含《北京市智能网联汽车管理条例》《北京市未成年人保护条例（修改）》《北京市网络视听节目管理条例》《北京市重要信息基础设施网络安全管理条例》等立法项目。（来源：北京人大）

7. 广东省深圳市卫生健康委员会印发《深圳市卫生健康数据管理办法》

11 月 16 日，广东省深圳市卫生健康委员会印发《深圳市卫生健康数据管理办法》。办法共七章四十九条，包括数据收集、传输和存储，数据使用、加工和删除，数据共享和开放，安全和监管等内容。

办法规定责任单位收集、存储卫生健康数据的要求，明确责任单位应当对数据传输、存储采取的安全防护措施，要求医疗卫生机构按照要求在本机构信息系统中为实名就医的个人建立身份标识唯一、基本数据项一致的居民电子健康档案，记录为其提供的健康服务信息，并将数据录入或者上传至卫生健康信息化平台，实现居民电子健康档案联网管理，使用电子病历系统的医疗卫生机构还应当将患者的电子病历数据上传至卫生健康信息化平台实现联网管理。在使用、加工卫生健康数据时应制定相关管理制

度，包括合规性审查、数据访问控制、脱密脱敏、采取相应安全措施等。（来源：深圳市卫生健康委员会）

8. 广东省人大常委会审议通过《广东省政务服务数字化条例》

11月23日，广东省人大常委会审议通过《广东省政务服务数字化条例》，2024年1月1日起施行。该条例是全国首部政务服务数字化条例。

条例要求，县级以上人民政府政务服务数据管理机构和政务服务机构应当依照法律、法规的规定和国家标准要求，建立健全政务服务数据安全管理制度，落实数据安全保护责任，采取技术措施和其他必要措施保障政务服务平台运营和数据安全。委托服务商建设、运营、维护政务服务平台的，应当监督服务商履行数据安全保护义务。政务服务机构需要通过生物识别技术核验服务对象身份的，应当具有明确、合理的目的和充分的必要性，取得服务对象的单独同意，并采取严格的数据保护措施。（来源：广东省人大常委会）

9. 广东省广州市印发《关于更好发挥数据要素作用推动广州高质量发展的实施意见》

11月28日，中共广州市委全面深化改革委员会印发《关于更好发挥数据要素作用推动广州高质量发展的实施意见》。

创新性规定方面，实施意见将：（1）探索通过民事商事合同、行政协议约定和资产登记等方式明确数据产权，推动数据产权“三权分置”机制在广州落地；（2）构建结构合理和运行顺畅的数据要素市场体系，推进以

政府指导价格形成机制为主的一级数据要素市场建设，完善以市场竞争价格形成机制为主的二级数据要素市场建设，支持打造国家级数据交易场所，培育多元化数据流通生态；（3）创新公共数据运营模式，培育公平竞争、多方参与、收益共享的公共数据开发利用生态，更好调动市场主体参与公共数据开发利用的积极性；（4）推动数据资产入表，探索构建数据要素价值评估与统计核算规则，并研究政府在数据要素收益分配中的引导调节作用，促进全社会共享数据红利。（来源：广州市人民政府）

10. 江苏省人大常委会通过《关于促进车联网和智能网联汽车发展的决定》

11 月 29 日，江苏省十四届人大常委会第六次会议审议通过《关于促进车联网和智能网联汽车发展的决定》，2024 年 1 月 1 日起施行。作为促进车联网和智能网联汽车发展的全国首部省级地方性法规，该决定针对新业态新问题进行创制性立法，为江苏相关产业继续走在全国前列提供法治保障。

决定共十九条，重点强化政府部门的引导推动责任。要求省政府应加强领导，制定车联网和智能网联汽车发展政策；省工业和信息化部门负责组织协调、统筹实施和监测评估，有关部门各负其责促发展。安全方面，决定要求相关企业建立网络安全管理制度；落实数据分类分级保护，依法将在我国境内运营中收集和产生的重要数据和个人信息存储在境内，因业务需要确需向境外提供的，应当按照国家有关规定办理相关手续；鼓励有

关企业、机构依法开展车联网和智能网联汽车的网络安全和数据安全认证、检测、风险评估等服务。（来源：中国人大网、江苏人大发布）

11. 江西省人大常委会通过《江西省数据应用条例》

11 月 30 日，江西省第十四届人大常委会第五次会议审议通过《江西省数据应用条例》，2024 年 3 月 1 日起施行。条例共七章五十二条，主要从数据资源、数据要素市场、发展应用、促进措施等方面做出规定。

条例明确数据资源的处理原则。处理涉及个人信息的数据应当具有明确、合理的目的，遵循最小必要和合理期限原则，采取对个人权益影响最小的方式，并遵守法律、法规规定的个人信息处理规则，履行个人信息处理者的法定义务。数据处理者是数据安全保护的责任主体。数据存在多个处理者的，各数据处理者承担相应的安全保护责任。数据处理者因合并、分立、收购等变更的，由变更后的数据处理者承担数据安全保护责任。（来源：江西省人民政府）

境内前沿观察三：治理实践

导读：11 月，公安部通报全国公安机关全力打击黑客类违法犯罪举措及总体成效情况。通报指出，2022 年以来，全国公安机关共侦破黑客类犯罪案件 2430 起。目前黑客类犯罪中与广大网民和企业日常生产生活密切相关的犯罪手法，主要有勒索病毒攻击、网络钓鱼攻击、弱口令攻击、流量攻击、物联网设备入侵五种。

数据治理方面，国家数据局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×”行动。数据出境治理取得新进展，海南航空控股股份有限公司成为海南首家通过数据出境安全评估的企业，国际航空运输协会成为首批通过数据出境安全评估的外国航空机构之一。伟创力技术（长沙）有限公司提交的两份个人信息出境标准合同通过湖南省互联网信息办公室组织的备案审核，成为湖南省首家通过订立标准合同实现个人信息合规出境的企业。

广东、北京、杭州等地法院发布个人信息保护案件相关审理情况或典型案例。其中，北京市互联网法院表示受理的个人信息保护案件以互联网企业为主要被诉主体，涉诉个人信息类型和侵权形态较为多样。

结合 11 月公布的行政案件中的违法行为，企业在开展合规工作时应注意以下方面：1. 如实开展网络安全等级保护定级、备案、等级测评；2. 履行国际联网备案职责；3. 建立健全全流程数据安全管理制度；4. 组织开展

数据安全教育培训；5.采取技术措施和其他必要措施保障数据安全；6.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。

关键词：黑客类违法犯罪、虚假撤销等保备案、数据出境、数据要素X、个人信息保护案件

（一）公安机关治理实践

1. 公安部公布依法惩治网络暴力违法犯罪10起典型案例

11月28日，公安部网安局发布消息称，近年来，网络暴力违法犯罪频发，致使部分当事人“社会性死亡”甚至精神失常、自杀，严重扰乱网络秩序、破坏网络生态，造成恶劣社会影响。公安机关网安部门对此高度重视，始终保持“零容忍”态度，立足自身职能，依法侦办查处一大批在信息网络上肆意侮辱谩骂、造谣诽谤、侵犯隐私等网络暴力违法犯罪案件。

同期公布依法惩治网络暴力违法犯罪10起典型案例，分别是（1）江苏公安机关侦破章某雇佣“网络水军”网暴他人案；（2）四川公安机关侦破陈某某犯罪团伙侮辱他人案；（3）浙江公安机关侦破张某等人诽谤案；（4）江苏公安机关侦破季某某通过网暴手段吸粉引流案；（5）广西公安机关侦破王某某犯罪团伙寻衅滋事案；（6）江西公安机关侦破胡某甲寻衅滋事案；（7）山东公安机关侦破宋某某犯罪团伙非法利用信息网络案；（8）山西公安机关侦破郭某某寻衅滋事案；（9）广东公安机关查处雷某某侮辱他人案；（10）湖南公安机关查处李某某侮辱他人案。（来源：公安部网安局）

2. 公安部通报打击黑客类违法犯罪举措成效：2022 年以来侦破黑客类犯罪案件 2430 起

11 月 30 日，公安部通报全国公安机关持续开展“净网”系列专项行动，全力打击黑客类违法犯罪举措及总体成效情况。通报指出，2022 年以来，全国公安机关共侦破黑客类犯罪案件 2430 起、抓获犯罪嫌疑人 7092 名。

从公安机关近年侦办的案件来看，目前黑客犯罪有以下趋势特点：一是成为涉网犯罪的“技术引擎”。黑客案件破案数连续三年上涨，年均增幅达 27.7%，犯罪分子除直接入侵、破坏计算机信息系统外，还通过窃取数据、篡改网站、劫持流量等方式，为电信诈骗、网络赌博、网络色情、网络水军等违法犯罪活动提供技术支持、物料信息和推广引流服务；二是侵害领域从网上延伸到网下；三是作案手法伴随技术发展越发多样。随着人工智能、区块链、物联网等新技术、新业态、新应用的发展变化，黑客犯罪分子的作案手法也在不断升级；四是技术门槛不断降低，低龄化特征显著；五是黑客犯罪的社会危害性日益严重。

通报指出，目前黑客类犯罪中与广大网民和企业日常生产生活密切相关的犯罪手法，主要有勒索病毒攻击、网络钓鱼攻击、弱口令攻击、流量攻击、物联网设备入侵五种。

通报指出，日常网络和数据安全监管方面，公安机关主要开展四方面常态化工作：一是开展执法监督检查。持续推动落实国家网络安全等级保护制度和关键信息基础设施安全保护制度，全面增强重要行业部门的网络和数据安全意识，有力提升重要信息系统安全保护能力，有效防范黑客攻

击犯罪，确保国家网络和数据安全；二是加大网络和数据安全行政执法力度。针对关键信息基础设施运营者、重要行业部门等单位，坚持问题导向，创新方式方法开展行政执法，及时排查风险、堵塞漏洞、消除隐患、补齐短板，压紧压实网络运营者、数据处理者的安全责任。2023 年第三季度，公安机关共办理网络和数据安全行政案件 1.4 万起，其中，网络运营者不履行网络安全保护义务的案件占 86%；三是开展一案双查。针对黑客攻击犯罪，公安机关在侦查调查的同时，均同步启动“一案双查”机制，分析案事件成因，依据《网络安全法》《数据安全法》《个人信息保护法》等法律法规，对问题单位违法违规行为开展调查，依法开展约谈、责令改正、警告、罚款、吊销证照、暂停业务、停业整顿等执法活动，切实压紧压实网络和数据安全保护责任；四是加强警示教育。（来源：公安部网安局）

3. 浙江温州网警查处某大药房“内鬼”侵犯公民个人信息案

11 月 10 日消息，浙江温州公安网安部门近日查处一起某大药房“内鬼”侵犯公民个人信息案。

温州网安部门在日常工作中发现有人在暗网上售卖温州某大药房销售数据。通过侦查发现，该大药房数据分析师利用工作便利将大量交易数据导出并售卖。温州网安依法对该数据分析师采取刑事强制措施，并启动“一案双查”工作机制。经进一步侦查发现，该大药房因未建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施保障数据安全，最终导致大量敏感数据泄露。

该大药房数据分析师因违反《刑法》第二百五十三条之一之规定，涉嫌侵犯公民个人信息罪被温州公安机关依法刑事拘留，现案件还在进一步办理中。同时，温州公安机关依据《数据安全法》第二十七条、第四十五条，对该药房处罚款 110 万元，对该大药房直接负责的主管人员处罚款 10 万元。（来源：公安部网安局）

4. 山东济南网警破获一起侵犯公民个人信息案

11 月 21 日消息，山东省济南市公安局网安支队近日成功破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 13 名，涉案金额 200 余万元。

济南网警在工作中发现，本地多名新生儿父母曾接到“上门摄影”电话推销，疑似个人信息泄漏。经查，确定推销电话来自山东某文化有限公司，其主营业务为新生儿摄影。该公司法人席某倩于 2021 年 5 月联系在济南某单位工作的好友张某某、周某，意图通过非法渠道获取更多客户资源。与席某倩达成共识后，张、周二人利用职务之便潜入单位系统，查询获取到部分孕妇和新生儿信息，并以每条 5 元的价格出售给席某倩。

查明真相后，专案组将上述 3 人以及山东某文化有限公司共同经营人张某江抓获，同时查获纸质版新生儿信息 2000 余条，电子版 6 万余条。席某某非法获利 51 万余元，张某某非法获利 24 万余元，周某非法获利 12 万余元。专案组加紧取证勘验，梳理其他曾为该公司提供各类公民个人信息的家政、月嫂、孕教等上线机构 6 家，席某倩转手倒卖新生儿个人信息的保险、产康等下线机构 2 家，又先后抓获犯罪嫌疑人 9 名。

以上案件中涉事单位系统监管缺位，存在安全漏洞。济南网警开展“一案双查”，根据《数据安全法》对该系统主管单位处以行政警告并责令整改，对其开发运维企业处以行政警告、罚款5万元并责令整改，对企业驻点的直接责任人崔某健处以行政警告、罚款1万元。（来源：公安部网安局）

5. 广东广州花都网警公布三起网络安全行政执法典型案例

11月22日，广东省广州市公安局花都区分局发布三起“净网2023”专项行动网络安全行政执法典型案例。

案例一：2023年11月3日，接广州市网络与信息安全信息通报中心通报，花都区某贸易有限公司财务系统页面出现违法信息，花都区分局网警大队民警接到通报后，立即启动应急响应机制，妥善处置并立即开展相关检查工作。经现场核查，发现该公司未按规定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，导致系统被黑客入侵并被篡改，加入违法信息，违反《网络安全法》第二十一条。花都区分局根据《网络安全法》第五十九条第一款，对该公司给予罚款两万元，对直接负责人罚款五千元的行政处罚。

案例二：2023年5月19日，花都网警在工作中发现，广州某教育科技有限公司的某百科系统于2021年4月完成三级等保备案，后于2022年12月撤销等保备案。经过核查，发现该公司系统撤销备案后仍在继续运行使用，且未重新定级备案，存在虚假撤销的行为，违反《广东省计算机信息

系统安全保护条例》第十四条。花都区分局根据《广东省计算机信息系统安全保护条例》第四十二条，对该公司给予警告并责令其限期完成整改。

案例三：2023 年 10 月 19 日，花都网警在工作中发现，花都区某货源网站未履行网络安全保护义务，未按规定履行网络国际联网备案手续，违反《计算机信息网络国际联网安全保护管理办法》第十二条。花都区分局根据《计算机信息网络国际联网安全保护管理办法》第二十三条，给予该网站负责人警告，并责令其限期完成整改。（来源：广州日报）

6. 四川成都网警破获一起编造传播证券市场网络谣言案

11 月 22 日消息，四川成都网警近日破获一起编造传播证券市场网络谣言案。

成都网警在工作中发现，有不法人员利用境外新闻媒体的局部页面，编造我国证券市场融资融券等政策的不实信息。随后，该信息以图片的形式在境内网站、论坛和微博、微信等社交网络上大量传播，严重扰乱证券市场稳定运行，严重误导投资者和社会公众，严重破坏网络舆论环境。

四川网安部门与证券监管部门开展侦察工作，成功抓获嫌疑人王某。经查，王某出于主观臆断和寻求精神刺激，通过篡改境外新闻媒体的局部页面，对外发布自己编造的我国证券市场融资融券等政策的不实信息。王某的行为违反《证券法》第五十六条和《治安管理处罚法》第二十五条第一项，公安机关和证券监管部门依法依规予以处理。（来源：公安部网安局）

7. 四川凉山网警打掉一虚拟助农“水军”团队

11 月 3 日消息，四川凉山网警近期打掉一个孵化网红以“卖惨”虚拟助农的“水军”团队。

四川凉山公安机关工作中发现，网红“凉山曲布”“赵灵儿”“凉山孟阳”“凉山阿泽”等人在网络水军的帮衬下，在直播带货过程中虚假宣传，涉案数额巨大，涉嫌犯罪。

经查，成都某“助农”传媒有限公司和某网络科技公司在凉山物色多名网红苗子，通过设计剧本、话术，专门挑选当地无人居住的生产用房、破壁残垣等素材作为直播背景，打造“大凉山原生态”人设，在短视频平台发布“偶遇”“蹭饭”“助农”等情节短视频，并通过“水军”对相关账号进行涨粉、推流，孵化多个百万粉丝网红账号。之后，该团伙通过开设网店和直播带货，打着“助农”“优质原生态”等旗号，假冒“大凉山特色农产品”商标，从成都、云南、南京等外地低价购入蜂蜜、核桃等农副产品，以次充好，以假充真，在全国范围内销售，涉案金额超千万。

凉山警方开展收网行动，共抓获犯罪嫌疑人 51 人，捣毁涉嫌虚假宣传的网络传媒公司 5 个，打掉“XX代刷”等水军团伙 3 个、刷单平台 1 个、技术支撑公司 3 个，查获网络推手账号数万个，缴获作案手机电脑若干，扣押假冒商品成品 5000 余瓶、外包装 5 万余件、生产设备 3 套，冻结赃款 500 万余元，涉案资金流水达 1.5 亿余元。（来源：公安部网安局）

8. 广东网警开展打击“网络水军”第三波次集群收网，涉案金额5.1亿元人民币

11月6日消息，根据公安部“净网2023”专项行动工作部署，广东网警于9月15日至9月27日组织发起打击“网络水军”第三波次集群收网行动，打掉犯罪团伙16个，抓获嫌疑人154人，其中刑事拘留79人，涉案金额5.1亿元人民币。

同期公布五起典型案例，分别是：（1）广州网安打掉刷单控评团伙；（2）深圳网安侦破通过恶意信访敲诈勒索网上店铺案；（3）佛山网安打掉刷单控评团伙；（4）惠州网安打掉刷单控评团伙；（5）湛江网安侦破冒用记者利用自建网站发布虚假信息敲诈牟利案。（来源：公安部网安局）

9. 上海普陀网警破获一起非法获取计算机信息系统数据案

11月21日消息，上海普陀警方近期在纵深推进净网2023、砺剑2023等专项工作中破获一起非法获取计算机信息系统数据案。

今年5月，普陀分局网安支队接到某提供导航服务的公司报案称，发现有人利用技术手段盗取公司服务器内全国的导航地图信息数据，并在论坛中售卖，导致公司直接经济损失约21万元。经侦查，普陀分局网安支队锁定就职于一家数据科技公司的犯罪嫌疑人张某齐，发现张某齐售卖的“盗版”数据均来自其所就职公司的数据库。该公司自2021年7月起从事大数据分析业务，主要根据客户需求出具分析报告，并提供营销分析、运营分析、产品分析等服务。经进一步侦查发现，在该公司实际控制人张某某的

指使下，公司技术负责人吕某昌和技术员张某齐编写爬虫程序，对目标平台的数据进行非法爬取，通过分析“盗版”数据出具分析报告以非法牟利。

6月底，警方将张某某、吕某昌、张某齐等3名犯罪嫌疑人抓获。7月21日，警方赴外省抓获犯罪嫌疑人丘某平。经审讯，张某齐交代，其因工作需要，通过论坛搭识网络工程师丘某平，并在丘某平处购买了相关技术服务。两人在未经授权的情况下，非法盗取平台数据2000余万条。此外，张某齐为进一步非法牟利，私自将非法爬取的“盗版”数据于论坛售卖。

目前，犯罪嫌疑人张某某、吕某昌、张某齐、丘某平因涉嫌非法获取计算机信息系统数据罪被警方依法采取取保候审的刑事强制措施。（来源：警民直通车上海）

（二）网信部门治理实践

1. 中央网信办开展“清朗·网络戾气整治”专项行动

11月10日,中央网信办决定即日起在全国范围内启动为期1个月的“清朗·网络戾气整治”专项行动。

专项行动围绕社交、短视频、直播等重点平台类型，坚决打击以下问题：（1）“网络厕所”“开盒挂人”行为；（2）借社会热点事件恶意诋毁、造谣攻击；（3）污名化特定群体、煽动地域对立；（4）斗狠PK等低俗不良直播行为；（5）有组织地恶意辱骂举报他人；（6）编造网络黑话、恶意造梗；（7）煽动网上极端情绪。（来源：网信中国）

2. 浙江网信通报10月执法处置情况：开展行政检查、行政指导57家次

11月3日，浙江省互联网信息办公室发布10月执法处置通报。通报指出，2023年10月，浙江网信重点围绕护航杭州亚运会和亚残运会，切实加强网络执法力度，严处网上违法违规行为，积极营造良好网络环境。

浙江网信依法依规约谈网站账号38个，责令整改网站平台168家，注销网站备案26家，下架APP5款，开展行政检查、行政指导57家次。网信部门及属地重点平台总计受理处置网民举报3.3万件，对30家无备案或虚假备案的网站移交省通信管理局作进一步处置。（来源：网信浙江）

3. 浙江网信通报一批侵犯个人信息合法权益的违法违规App

11月28日，浙江省互联网信息办公室通报一批侵犯个人信息合法权益的违法违规App。通报称，浙江省网信办近日依法查处违法违规App156款，存在未公开收集使用规则、未明示收集使用个人信息的目的方式和范围、未经用户同意收集使用个人信息、违反必要原则收集等问题，责令限期15日完成整改。相关App开发者应严格参照问题清单进行整改，并将整改报告加盖公章发送至指定电子邮箱。（来源：网信浙江）

4. 重庆网信发布通知，要求报送数据出境需求

11月14日，重庆市互联网信息办公室发布关于报送数据出境需求的通知，明确报送重点对象、报送数据范围以及报送方式等内容。

通知指出，所在地为重庆市的外资企业，以及跨境金融、跨境物流、跨境电商等可能存在数据出境情况的机构，将在境内收集和产生的数据传输、存储至境外（含港澳台地区）的，或数据存储在境内但境外机构、组织、个人可以查询、调取、下载、导出的，应向重庆市网信办报送数据出境需求。（来源：网信重庆）

5. 海南首家企业通过数据出境安全评估

11 月 17 日，海南省委网信办发布消息称，海南航空控股股份有限公司近日通过国家网信办数据出境安全评估，出境数据项为海外订座业务相关数据项和海外离岗业务相关数据项。

海南航空控股股份有限公司在提交安全评估申报后，海南网信办积极对接，协助企业梳理数据出境场景和指导其完善申报材料，经海南网信办完备性审查后提交国家网信办评估，最终获批通过。（来源：网信海南）

6. 湖南首家企业通过个人信息出境标准合同备案

11 月 17 日，湖南省互联网信息办公室发布消息称，伟创力技术（长沙）有限公司提交的两份个人信息出境标准合同通过湖南省互联网信息办公室组织的备案审核，是湖南省首家通过订立标准合同实现个人信息合规出境的企业。（来源：网信湖南）

7. 国际航协财务结算数据安全评估项目通过国家网信办评估

11 月 28 日消息，国际航空运输协会成为首批通过国家互联网信息办公室数据出境安全评估的外国航空机构之一，出境数据为北亚区财务结算与分销业务相关数据。（来源：国际航协）

8. 各地开展 2023 年度汽车数据安全管理情况报送工作

11 月，北京、天津、江苏、浙江、江西、山西等省（市）依据《汽车数据安全管理若干规定（试行）》的相关规定，发布《2023 年度汽车数据安全管理情况报送通知》。

通知明确报送对象、报送内容、报送时限以及报送方式等，应报送内容包括 2023 年度汽车数据安全管理情况报告、风险评估报告、汽车数据处理者情况汇总表；报送时限为即日起至 2023 年 12 月 15 日。（来源：地方网信部门）

（三）通信管理部门治理实践

1. 工信部等四部委决定开展智能网联汽车准入和上路通行试点工作

11 月 17 日，工信部、公安部、住房和城乡建设部、交通运输部发布通知，决定开展智能网联汽车准入和上路通行试点工作。

试点工作分为试点申报、试点实施、试点暂停与退出、评估调整四个环节。通知指出，试点期间，车辆发生道路交通安全违法行为和交通事故

涉嫌安全隐患，试点汽车生产企业或使用主体有未履行安全责任和网络安全、数据安全、无线电安全保护义务等情形，应当暂停试点并整改。

通知同步发布《智能网联汽车准入和上路通行试点实施指南（试行）》及《智能网联汽车准入和上路通行试点申报方案（模板）》。其中，指南要求企业建立智能网联汽车产品与供应商相关的风险识别和管理能力，明确供方产品和服务的网络安全评价标准、验证规范等，具备管理企业与合同供应商、服务提供商、企业内部组织之间安全依赖关系的能力等。建立智能网联汽车产品数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。（来源：工信部）

2. 工信部及多地通信管理局通报问题 APP/SDK

（1）工信部

11月，工信部通报2023年第7批、第8批侵害用户权益行为的APP(SDK)。通报称，工信部近期组织第三方检测机构对群众关注的实用工具、在线影音、网络游戏等APP及SDK进行检查。分别发现13款、22款APP、SDK存在违规收集个人信息、强制频繁过度索取权限、欺骗误导强迫用户以及超范围收集个人信息等侵害用户权益行为。上述APP及SDK应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）安徽省

11月9日，安徽省通信管理局通报2023年第7批侵害用户权益的APP。安徽省通信管理局近期对省内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问题，2023年10月10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。截至目前，尚有17款APP未完成问题整改，相关APP企业应在2023年11月15日前落实整改要求。逾期不整改的，将依法依规组织开展相关处置工作。

（3）浙江省

11月21日，浙江省通信管理局通报2023年第9批侵害用户权益行为的APP。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、网络社区等类型APP进行检查，发现部分APP存在违规收集个人信息、强制频繁过度索取权限、强制用户使用定向推送功能等问题，书面要求违规APP开发运营者限期整改。截至目前，尚有14款APP未按要求完成整改。上述APP开发运营者应在11月29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。

（4）广东省

11月23日，广东省通信管理局公开通报19款未按要求完成整改APP。通报称，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，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19款APP未完成整改。被通报的APP应在11月29日前完成整改及反馈工作。逾期不整改的，将依法依规采取下一步处置措施。

同日，广东省通信管理局还发布关于下架4款侵害用户权益APP的通报。通报称，截至通报规定时限，经核查复检，尚有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。

（5）上海市

11 月 28 日，上海市通信管理局通报 2023 年第四批侵害用户权益行为的APP。上海市通信管理局近期组织第三方检测机构对本市APP侵害用户权益行为开展检查。经检测发现 59 款APP（含小程序）存在“违规收集个人信息”“超范围收集个人信息”等相关问题。截至目前，尚有 19 款APP未完成整改，相关APP应在 12 月 5 日前落实整改工作。逾期不整改的，将依法依规组织开展处置工作。（来源：工信部、地方通信管理局）

（四）其他部门治理实践

1. 国家数据局将研究实施“数据要素 X”行动

11 月 25 日，国家数据局局长刘烈宏在 2023 全球数商大会上表示，国家数据局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×”行动，从供需两端发力，在智能制造、商贸流通、交通物流、金融服务、医疗健康等若干重点领域，加强场景需求牵引、打通流通障碍、提升供给质量，推动数据要素与其他要素相结合，催生新产业、新业态、新模式、新应用、新治理。

数据要素乘数效应的具体表现为：一是以协同实现全局优化，提升产业运行效率，增强产业核心竞争力；二是以复用扩展生产可能性边界，释

放数据新价值，拓展经济增长新空间；三是以融合推动量变产生质变，催生新应用、新业态，培育经济发展新动能。（来源：中国政府网）

2. 最高人民检察院发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023 年）》

11 月 30 日，最高人民检察院发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023）》。报告指出，检察机关起诉电信网络诈骗犯罪案件同比呈明显上升趋势。随着打击治理特别是境外抓捕力度加大，2023 年 1 月至 10 月，全国检察机关共起诉电信网络诈骗犯罪 3.4 万余人，同比上升近 52%。

报告指出，起诉帮助信息网络犯罪活动罪案件仍高位运行，但上涨幅度逐步放缓。主要原因是，一方面，反电信网络诈骗法对于出租、出售银行卡的行为设置了前置行政处罚，实践中对于行为人系初犯且犯罪情节轻微的，检察机关依法作出相对不起诉决定后，反向移送给行政执法机关予以行政处罚；另一方面，随着打击和风控力度加大，单纯出租、出售银行卡的情形逐渐减少，转而代之的是要求在“卖卡”同时提供“刷脸”转账验证等帮助，这类行为往往符合掩饰、隐瞒犯罪所得、犯罪所得收益罪的犯罪构成。

检察机关打击治理主要举措方面，报告指出，检察机关围绕信息流，深挖案件线索，加大对侵犯公民个人信息尤其是非法获取人脸、声纹等敏感信息、利用AI等前沿技术伪造人脸、声纹以及获取其他信息犯罪的打击力度。认真贯彻落实反电信网络诈骗法赋予的公益诉讼职责，围绕重点行

业个人信息保护、“两卡”管理、企业反诈义务履行等方面，积极开展公益诉讼检察工作。2023年以来，针对电信、金融、互联网等行业未依法落实反电信网络诈骗义务的违法情形，立案办理公益诉讼案件160余件。（来源：最高人民检察院）

3. 广东省高级人民法院发布个人信息保护典型案例

10月31日，广东省高级人民法院发布七起个人信息保护典型案例，涉及违规收集处理信息、算法运行错误侵权、非法采集人脸图像等侵害个人信息权益的行为。

相关案例分别是：（1）互联网平台收集和处理个人信息的标准认定——王某与某计算机公司个人信息保护纠纷案；（2）算法运行错误导致个人信息不实的责任主体认定——梁某等与某科技公司网络侵权责任纠纷案；（3）未经同意发送商业短信侵害个人信息权益——王某与某信息公司网络侵权责任纠纷案；（4）个人信息认定标准“可识别性”的适用——田某与某物业公司隐私权、个人信息保护纠纷案；（5）未经同意采集人脸图像作为证据的效力认定——某科技公司与某房地产公司商品房委托代理销售合同纠纷案；（6）大规模个人信息侵权中不特定损害的判定——广州市越秀区人民检察院与郑某等个人信息保护公益诉讼案；（7）危害公共利益的个人信息侵权行为的司法认定——东莞市人民检察院与赵某侵犯公民个人信息民事公益诉讼案。（来源：广东法院网）

4. 北京互联网法院通报个人信息保护案件审理情况

11 月 1 日，北京互联网法院通报个人信息保护案件审理情况。2018 年 9 月至今，北京市互联网法院共受理 58 件涉及个人信息保护的案件，以互联网企业为主要被诉主体，涉诉个人信息类型和侵权形态较为多样。

调研发现，个人信息保护案件涉诉信息类型较为丰富，既包括法律法规列明的手机号、身份证号、行踪信息等，也包含大量法律未明确列举的信息，例如视频浏览记录、职业信息、交易信息、位置信息等，还包括敏感个人信息，如人脸信息。与此同时，引发个人信息纠纷的场景涉及众多数字经济领域，例如，金融企业信息泄露引发电信诈骗风险，在线教育APP强制收集个人信息用于用户画像，电商平台频繁拨打用户电话等。另外，有企业将用户信息制作成数据包，开发数据产品向他人提供，引发侵权风险；有企业存在线下收集、线上处理、线下线上多主体混合处理、关联企业共同处理等行为，反映出涉诉个人信息处理活动呈现多主体多形态交融的态势。此外，一系列新类型个人信息纠纷进入诉讼，如死者个人信息处理、提供查阅复制信息等。新闻通报会同步通报 8 起个人信息保护典型案例。（来源：北京互联网法院）

5. 北京高院发布《侵犯公民个人信息犯罪审判白皮书》

11 月 15 日，北京高院发布《侵犯公民个人信息犯罪审判白皮书》，对近 5 年来全市法院审结的侵犯公民个人信息罪案件进行分析。白皮书显示，侵犯公民个人信息犯罪案件数量呈波动状态，今年有所攀升。自 2018 年以来，北京法院审结侵犯公民个人信息罪一、二审案件共计 229 件。与 2018

年相比，2019 年全市法院侵犯公民个人信息罪收、结案数量有所上升，后开始下降，2020 年和 2022 年下降幅度尤为明显。从 2023 年的收案情况来看，案件数量出现反弹，反映出侵犯公民个人信息犯罪多发的态势。

侵犯公民个人信息犯罪呈现出以下基本特点：涉案公民个人信息类型中有关人身、财产安全的信息占比突出；涉案信息要素中手机号码、身份证件占比最大；涉案公民个人信息的数量规模日渐庞大；五成案件的被告人有较为固定的工作单位或职业；侵犯公民个人信息的犯罪手段越发隐蔽；侵犯公民个人信息犯罪与其他违法犯罪活动相关联等。（来源：京法网事）

6. 杭州互联网法院发布十大典型司法建议，涉及个人信息保护、人工智能换脸等

11 月 7 日，杭州互联网法院召开司法建议工作新闻发布会，发布十大典型司法建议。此次发布的典型司法建议，涉及个人信息保护、算法模型优化升级、人工智能换脸、平台内自治规则统一等领域，且被建议单位均及时反馈整改。部分司法建议是：（1）杭网法建〔2023〕2 号——关于强化快递包裹个人信息保护的司法建议；（2）杭网法建〔2023〕7 号——关于推动完善平台算法治理机制的司法建议；（3）杭网法建〔2022〕2 号——关于对应用人脸替换技术产品应添加显著标识的司法建议。

其中，杭网法建〔2022〕2 号——关于对应用人脸替换技术产品应添加显著标识的司法建议中，杭州互联网法院在案件审理中发现，某科技公司开发、运营的APP，应用了人脸替换信息技术，为他人提供对图像、视频内容中人脸等生物特征进行生成或者编辑的服务，存在违法、违规的情况，

可能危及公民合法权益，遂发出司法建议。要求该科技公司立刻予以整改，对使用了人脸替换技术的产品，应添加显著标识予以明示。（来源：杭州互联网法院）

7. 国家卫生健康委强化医疗健康数据保护

11 月 7 日，国家卫生健康委召开新闻发布会，介绍全国医疗机构信息互通共享三年攻坚行动相关情况。

针对信息互通共享和个人隐私之间的边界问题，国家卫生健康委规划司表示，长期以来，卫健委高度重视数据和个人信息的安全风险问题，坚持发展与安全并重。在开展攻坚行动过程中，重点的精力放在如何进一步强化网络和数据安全上，强化医疗健康数据保护“防泄露”，要求各级卫生健康行政部门要建立完善的符合医疗健康信息互通共享场景的网络与信息安全相关管理制度。医疗机构要加强数据安全管理，依法依规对数据的产生、传输、存储、使用、共享、销毁等实行全生命周期安全管理，提高数据安全防护能力和个人隐私的保护力度。运用加密二维码技术，通过授权访问机制，来保护患者隐私，加强医疗健康数据管理“防滥用”。（来源：健康中国）

8. 上海市消保委与连锁经营协会联合印发《上海市商超购物个人信息保护合规指引》

11 月 6 日，上海市消费者权益保护委员会和上海连锁经营协会联合印发《上海市商超购物个人信息保护合规指引》，适用于注册地或者消费行为地在上海的各类商超。

指引明确：（1）APP或小程序使用微信、支付宝等一键登录获取昵称、头像或手机号码等信息，或需要获取精准位置以提供附近门店服务的，应当征得消费者明确同意，不得以消费者拒绝授权为由停止提供服务或限制使用功能；（2）商超经营者应当遵循“最小、必要”原则，不得以任何形式和理由强制、诱导消费者关注微信公众号、注册会员、索取非必要个人信息和权限，不得频繁弹窗索取权限或申请消费者同意，干扰消费者正常使用功能；（3）未经消费者同意、请求，或消费者明确表示拒绝的，商超经营者不得将消费者个人信息共享至第三方使用或推送个性化商业营销信息。推送商业营销信息应当提供退订或拒绝选项，个性化推荐服务应当提供简易的关闭操作流程。（来源：网信上海）

9. 因生产数据安全管控不足，华美银行被罚 60 万元

11 月 13 日，国家金融监督管理总局上海监管局行政处罚信息公开表（沪金罚决字〔2023〕28 号、29 号）显示，华美银行（中国）有限公司生产环境安全管控不足、生产数据安全管控不足。时任华美中国信息科技部主管仲蔚负直接管理责任。

依据《银行业监督管理法》第四十六条，国家金融监督管理总局上海监管局责令华美银行（中国）有限公司整改，并处罚款60万元；依据《银行业监督管理法》第四十八条，对华美中国信息科技部主管仲蔚处以警告。（来源：国家金融监督管理总局）

10. 因使用气象仪使数据外泄至境外，浙江舟山普陀区综合行政执法局对张某罚款5000元

11月16日消息，浙江舟山市普陀区综合行政执法局近日查处一起气象数据信息外泄案件。

根据舟山市气象局提供的违法线索，舟山市普陀区综合行政执法局调查发现，居民张某为配合家中智能家居使用而网购了某款无线气象仪，将气象仪放置于院落内并接入互联网，人在外时可以通过手机APP实时查看院内天气信息。执法人员经过咨询相关部门、查看手机APP用户协议及有关数据资料，确定该款产品的确会将气象仪收集的数据信息（包括温度、湿度、风向、风速、气压、雨量、日照等）通过互联网传输至境外。

张某网购的该款无线气象仪，在未联网的情况下不会外传数据信息，一旦联网，就会将数据信息传输至境外服务器。鉴于张某检查发现后，立即停止了违法行为，且认错态度良好，情节轻微。普陀区综合行政执法局依法对其作出警告并处罚款5000元的处罚决定。（来源：环球网）

境外前沿观察：月度速览十则

导读：11 月，美国网络安全和基础设施安全局发布《缓解指南：医疗保健和公共卫生行业》，用以应对医疗保健和公共卫生行业面临的网络安全威胁。澳大利亚网络和基础设施安全中心发布《关键基础设施年度风险评估报告》，建议实施关键基础设施风险管理计划。

加拿大国库委员会宣布禁止在政府配发的设备上使用中国移动互联网应用程序微信和俄罗斯杀毒软件卡巴斯基。加拿大首席信息官表示，两款软件对隐私和安全构成不可接受的风险，尽管如此，目前尚没有证据表明政府信息已遭到泄露。中方对此坚决反对，指出加拿大政府在没有任何真实证据的情况下，出台针对中国企业的禁令是典型的泛化国家安全概念。

新西兰发布《2022/2023 年度网络威胁报告》，指出新西兰在 2022 年 7 月 1 日至 2023 年 6 月 30 日之间共发生 316 起网络安全事件，其中外国资助的活动占事件总数的 23%。同时，各国披露多起网络攻击事件。丹麦关键基础设施遭遇最大规模网络攻击，22 家能源基础设施公司受到影响。波音公司和美国软件公司 MeridianLink 遭到勒索软件攻击。印度发生大规模数据泄露事件，涉及约 8.15 亿公民数据。

关键词：关键信息基础设施安全、加拿大微信禁令、网络安全事件、勒索攻击防治、公民数据泄露

1. 美国 FBI 发布私营行业通知，对勒索攻击提出防治对策

11 月 7 日，美国联邦调查局（FBI）发布私营行业通知，详细介绍勒索攻击作案手段并提出防治对策。FBI 表示勒索软件通过木马恶意软件启动初始入侵，经远程代理访问侦察最佳入侵时间并实施入侵，网络犯罪分子会基于前期侦察阶段获取的非公开信息池选择勒索对象，诱使受害者支付赎金。FBI 提出离线备份关键数据、在所有主机上安装并定期更新防病毒或应对恶意攻击的软件、仅使用安全的网络、用户登录采用双因素身份验证等防治对策。FBI 不鼓励向犯罪分子支付赎金，支付赎金会对更多勒索组织形成激励，也可能资助其他非法活动，支付赎金也并不能保证受害者文件得以恢复。（来源：美国 FBI、CISA）

2. 美国 CISA 发布《缓解指南：医疗保健和公共卫生行业》

11 月 17 日，美国网络安全和基础设施安全局（CISA）发布《缓解指南：医疗保健和公共卫生行业》，旨在应对医疗保健和公共卫生行业网络安全威胁。指南主要涉及三个方面：（1）资产安全管理。建议组织实施并派专员维护资产清单，列出组织所有资产并记录其属性；（2）身份管理和设备安全。包括正确配置并保护电子邮件系统、实施多因素认证、保护敏感信息安全等；（3）漏洞、补丁和配置管理。通过资产清单、漏洞扫描工具和风险管理策略，对漏洞进行评估、排序、修复。（来源：美国 CISA）

3. 澳大利亚 CISC 发布《关键基础设施年度风险评估报告》，将外国干涉和间谍活动确定为主要威胁

10 月 31 日，澳大利亚网络和基础设施安全中心（CISC）发布《关键基础设施年度风险评估报告》，指出澳大利亚关键基础设施面临的多方挑战，包括：（1）外国干涉和间谍活动。这是澳大利亚国家安全面临的首要威胁，外国势力和间谍组织窃取敏感信息和研究成果，可能会威胁澳大利亚主权安全和长期发展；（2）恐怖主义。虽然恐怖主义威胁程度有所下降，但仍有可能发生针对关键基础设施的攻击，造成社会恐慌和经济损失；（3）误传和假消息。通过社交媒体和其他渠道传播虚假或误导性信息，可能会破坏公众对关键基础设施的信任和支持，激化社会分歧和冲突；（4）人员风险。具有内部访问权限的人员可能会因为恶意、疏忽或无意识的行为，导致关键基础设施数据泄露、系统破坏或服务中断，或者被外国情报机构招募或利用；（5）海底电缆、卫星等灰色地带攻击、关键零件和软件供应链、自然灾害等风险。为此，报告建议澳大利亚政府通过实施关键基础设施风险管理计划、加强网络安全和物理安全、提高供应链透明度和韧性等措施强化风险抵御能力。（来源：澳大利亚 CISC）

4. 新西兰 NCSC 发布《2022/2023 年度网络威胁报告》

11 月 2 日，新西兰国家网络安全中心（NCSC）发布《2022/2023 年度网络威胁报告》，分析新西兰面临的网络威胁形势。

报告指出，新西兰在2022年7月1日至2023年6月30日之间共发生316起网络安全事件，其中90起为出于犯罪或经济动机的事件，占总数的28%，外国资助的活动占事件总数的23%。报告总结常见网络威胁并提出应对策略，包括：（1）常见漏洞。恶意网络行为者会定期扫描并利用最新的漏洞。各组织应识别和了解常见漏洞，对已知漏洞快速实施补丁，并在安装补丁之前检查是否已经发生危害；（2）虚拟专用网和线上远程办公。恶意网络行为者通过社交欺骗或创建特权账户获取虚拟专用网凭证。各组织应采用条件访问等零信任方法的工具和技术，以及基于身份识别的网络代理；（3）禁用安全工具。恶意网络行为者试图通过“防御规避”技术扩展其网络访问权限，通过禁用内置安全控制或删除活动日志以隐藏其踪迹。各组织应强制使用多因素身份验证，将禁用安全工具视作高度可疑行为。（来源：新西兰NCSC）

5. 加拿大禁止在政府设备上使用微信和卡巴斯基

10月30日，加拿大国库委员会宣布禁止在政府配发的设备上使用中国移动互联网应用程序微信和俄罗斯杀毒软件卡巴斯基。加拿大首席信息官认定，两款软件对隐私和安全构成不可接受的风险。在移动设备上，两款软件的数据收集方式使其可以大量访问设备的内容。但首席信息官也表示，尽管加拿大政府声称这些风险是“明显”的，但目前没有证据表明政府信息已遭到泄露。

10 月 31 日，中国外交部发言人汪文斌在例行记者会上表示，加拿大政府在没有任何真实证据的情况下，打着维护数据安全的幌子，出台针对中国企业的禁令是典型的泛化国家安全概念、滥用国家力量、无理打压特定国家企业行为，中方对此坚决反对。（来源：加拿大政府、中国外交部）

6. 印度 8.15 亿公民数据被泄露，或成为印度最大数据泄露事件

10 月 31 日，美国网络安全公司 Resecurity 报告称 8.15 亿印度人的个人信息，包括姓名、电话号码、护照号码、身份证号码、年龄、性别、地址、地区等在暗网上被出售。这可能是印度目前最大数据泄露事件。据悉，被泄露的数据可能来自印度医学研究委员会中的公民 Covid-19 测试记录。（来源：Deccan Herald 官网）

7. OpenAI 确认 ChatGPT 遭遇分布式拒绝服务攻击

11 月 8 日，OpenAI 发布《关于 ChatGPT 及其 API 发生重大中断的报告》，表示发现 ChatGPT 受到分布式拒绝服务攻击，黑客利用大量设备向目标服务器发送访问请求，导致服务器过载崩溃。由于分布式拒绝服务攻击，ChatGPT 及其 API 出现周期性中断，大量用户无法正常使用。OpenAI 在发现问题后立即采取修复措施，包括增加服务器容量、调整流量分配、阻止恶意请求等。11 月 9 日，OpenAI 宣布服务状态已恢复正常。同时，OpenAI 还推出定制版 GPT 的全新版本，让用户可以对机器人的身份、语言特征等进行深度定制，还可以建立企业自有知识库。（来源：OpenAI 官网）

8. 波音公司拒绝支付赎金，勒索软件 LockBit 直接公布 43GB 文件

11 月 10 日，因波音公司拒绝支付赎金，勒索软件 LockBit 团伙直接公布波音公司 43GB 数据文件，其中包括信息技术管理软件的配置备份、监控和审计工具日志以及可能来自此前波音公司披露的 Citrix Bleed 漏洞相关设备的备份。尽管波音确认此次网络攻击，但公司并未提供有关事件的细节以及黑客侵入网络的方式。（来源：Bleepingcomputer 官网）

9. 丹麦关键基础设施遭遇有史以来最大规模网络攻击

11 月 13 日，由丹麦关键基础设施运营商支持的非营利性网络安全组织 SektorCERT 发布《针对丹麦关键基础设施的网络攻击》，披露丹麦关键基础设施在 2023 年 5 月遭遇的迄今为止最大规模的网络攻击。

报告指出，攻击者于 5 月 11 日发起首次攻击，5 月 22 日发起第二轮攻击，SektorCERT 组织于第二轮攻击当天察觉安全问题。攻击者利用丹麦关键基础设施运营商使用的 Zyxel 防火墙中的零日漏洞，成功破坏 22 家能源基础设施公司。Zyxel 在发现漏洞后立刻发布安全更新补丁并敦促其客户尽快安装。攻击者利用该漏洞，向易受攻击的设备发送特制数据包，在未经身份验证的情况下，直接在设备上执行具有根权限的命令。（来源：SektorCERT 官网）

10. 因受害者无视安全事件,勒索攻击组织向美国证券交易委员会提出投诉

11 月 17 日，勒索组织 ALPHV/BlackCat 向美国证券交易委员会提出投诉，指控金融软件服务商 MeridianLink 未遵守网络攻击披露规则。这是首次由勒索者向监管机构提出的投诉行为。

此前，勒索组织 ALPHV/BlackCat 已将软件公司 MeridianLink 列入其数据泄露名单，并威胁其在 24 小时内支付赎金，否则将泄露被盗数据。而 MeridianLink 对此次勒索置之不理，因此勒索组织向美国证券交易委员会发起投诉。MeridianLink 表示其高度重视保护客户和合作伙伴信息，发现安全事件后立即采取行动，并聘请第三方专家团队调查该事件。根据现有调查，MeridianLink 并未发现任何未经授权访问其生产平台的证据，目前调查仍在进行。（来源：Bleepingcomputer 官网）

行业前沿观察一：2023 安满周筹备中

导读：网民网络安全感满意度调查活动是目前国内调查范围最广、参与人数最多的全国公益网络安全社会调查；安满周作为网民网络安满度调查活动的重要组成部分与成果体现，在业内乃至全社会影响较大，有力地推进全社会网络空间安全意识建设，推动行业健康发展。2023 网络调查样本采集工作圆满结束后，目前数据分析、报告编撰和安满周筹备工作，正紧锣密鼓地进行中。

关键词：2023 调查活动，样本采集，安满周

1.安满周各项筹备工作紧锣密鼓进行中，数据挖掘值得期待

2023 网民网络安全感满意度调查活动样本采集工作圆满收官后，数据分析、报告编撰和安满周筹备工作紧锣密鼓进行中。

据组委会透露，2023 安满周将与往年有较大的创新，一是表现形式是线上与线下相结合，本次安满周将以线下活动为主，举办地点除主报告发布在北京外，其他报告发布地点将拓展到全国，调查活动开展较好、牵头编撰报告的地点将优先获得举办权限；二是报告发布和论坛相结合，内容层次更丰富，据介绍，本次安满周除发布一个主报告和其他分报告外，还将发布网民网络安全感满意度年度指数，以及网络安全感满意度趋势预测、行业发展分析等重磅内容，集中体现数据挖掘和数据分析的力量；组委会免费开放数据共享，以最大程度发挥数据的功效，造福全社会。有能力和意愿的机构或个人可联系组委会，沟通商洽相关数据共享开发事宜；三是继续弘扬志愿服务精神，安满周开幕式、闭幕式将对 2023 调查活动样本采集优秀志愿团队和个人进行表彰，安满周期间还将召开志愿者大会。

同时，组委会秉承开放的原则和宗旨，2023 安满周一如既往地面向全社会征集合作伙伴，除往年合作的机构组织之外，将有各行各业的新的合作伙伴加入，为安满周增加新鲜血液。由历年积累的海量的调查数据进行的数据挖掘和数据分析，产生的有价值的研究报告，将深度推进行业发展，推进全社会网络空间安全事业发展。（来源：网安联）

2. 腾讯公司到访北京网络空间安全协会洽谈“安满周”合作事宜

12 月 6 日，腾讯科技有限公司安全管理部副总经理何兴煌、数字舆情部总监戎飞腾、企鹅有调负责人邹晓婷、企鹅有调研究员仇业涵一行到访北京网络空间安全协会，洽谈商议“安满周”合作相关事宜。北京网络空间安全协会副理事长林勇忠热情接待。

何兴煌副总经理表示，网民网络安全感满意度调查活动是目前国内调查范围最广、参与人数最多的全国公益网络安全社会调查；安满周作为网民网络安满度调查活动的重要组成部分与成果体现，在业内乃至全社会影响较大，有力地推进全社会网络空间安全意识建设，推动行业健康发展。腾讯公司历来在建立规范运行体系和营造自律行业氛围方面，坚持责任担当。2022 年的“安满周”活动，腾讯成功承担了两个专题报告，取得良好效果，希望今年继续合作，在组委会统一安排下，撰写、发布相关专题报告，及承办相关分论坛。

腾讯舆情专家戎飞腾表示，2022 年腾讯承担了“未成年人网络安全保护”和“网暴”两个专题报告内容撰写，今年希望向组委会申请撰写《数字经济发展和网络安全挑战专题报告》，并承办相关分论坛。企鹅有调负责人邹晓婷作为 2022 年度专题报告的负责人，希望更多了解 2023 专题报告研究框架，以便尽快开展相关的工作。

林勇忠副理事长对腾讯公司的来访以及腾讯 2022 年积极参与“安满周”相关活动表示感谢。林副理事长表示，2023 年的“安满周”以线下为主，希望参与各方从打品牌的角度，精心准备科学组织，在组委会统筹安排下，做大做精做强“安满周”，唤起社会各界对网络空间安全的重视与关注。

林副理事长强调，希望“安满周”报告发布不是为了发布而发布，而是要发现问题、指出问题并且给出解决方案，为政府部门、社会各界提供建设性意见，群策群力建言献策，影响社会各方力量共同推进网络空间安全事业发展。

双方还就“安满周”活动日程安排、举办地点、志愿服务常态化等事项进行了沟通磋商。（来源：网安联）

3. 网络调查活动志愿服务走向常态化

调查活动样本采集圆满收官后，志愿服务进入常态化环节。调查活动组委会常务副主任兼秘书长、北京网络空间安全协会理事长黄丽玲表示，全国的志愿者队伍是一个充满正能量，有着公益心，非常可亲可敬可爱的群体，与网安联多年来坚持做公益活动的初心使命目标宗旨是高度一致的。今年是调查活动第二个五年的开局之年，在网安联志愿服务队的引领下，大家激情踊跃，干劲十足，网安联全国志愿服务体系目前已经初具规模。

黄理事长表示，在样本采集等阶段性工作结束后，下一阶段网安联志愿服务的重点要转到常态化上来，希望网安联志愿服务队要深入研究志愿服务的特点，创新思路和做法，常态化开展网络空间安全志愿服务，打通网络空间安全“最后一公里”。

黄理事长指出，常态化开展网络空间安全志愿服务要注意克服急功近利和急躁心态，要深入研究志愿服务的现实需求，整合资源，争取各地主管部门的支持，最大效能开展各项工作。（来源：网安联）

行业前沿观察二：行业竞争加剧，人才需求旺盛

导读：今年以来，我国经济顶住了国外风险挑战和国内多重因素交织叠加带来的下行压力，消费较快恢复，投资持续增长，内需贡献稳步提升。网络空间安全行业保持持续增长态势，凸显行业竞争加剧态势。目前网络空间安全人才缺乏整体规划，实战人才缺乏，人才评价需求旺盛。

关键词：网络空间安全，人才评价

1. 网络空间竞争加剧，网络安全人才评价需求旺盛

今年以来，我国经济顶住了国外风险挑战和国内多重因素交织叠加带来的下行压力，消费较快恢复，投资持续增长，内需贡献稳步提升。三季度，最终消费支出拉动经济增长 4.6 个百分点，对经济增长贡献率达 94.8%，比二季度提高 10.3 个百分点；资本形成总额对经济增长的贡献率是 22.3%，拉动国内生产总值增长 1.1 个百分点。相关指标持续回暖，折射内需潜力持续释放。网络空间安全行业发展态势良好，行业竞争加剧，凸显人才供需企待破局。

网络安全人才发展缺乏规划。随着全球信息化进程的推进，众多国家已经认识到网络安全的重要性，并纷纷制定国家网络安全战略。然而，相较于美国等发达国家在网络安全人才培养方面的系统性和层次性，我国在这方面起步较晚。尽管我国已经发布了一些网络安全战略规划文件，强调了人才培养的重要性，但总体上来说，仍缺乏网络安全人才培养的整体规划和顶层设计。相比之下，美国已具备领先的网络人才战略和体系，并发布了《国家网络人才和教育战略》，旨在推动政府、企业、学校和其他组织在人才培养和发展领域的改革，以适应当前和未来的网络人才需求，将对国际网络安全产生深远影响，同时，也给我国的网络安全人才培养战略带来了挑战。

网络安全攻防实战人才不足。据《网络安全人才实战能力白皮书》调查数据显示，“到 2027 年，我国网络安全人员缺口将达 327 万，而高校人才培养规模为 3 万 / 年，许多行业面临着网络安全人才缺失的困境”。此

外，由于高校缺乏实战环境，过于注重理论知识传授而轻视实践能力培养，所培养的网络安全人才往往无法迅速融入实际工作，高达92%的企业认为自己缺乏网络安全实战人才。攻防实战人才必须具备在实际业务环境中，利用网络安全技术和工具进行安全监督和解析、危险度评估或风险评估与衡量、渗透测试事件研判等业务能力，这对网络安全攻防实战人才的培养路径提出了高标准、高要求。

网络安全人才评价需求旺盛。目前我国网络安全人才评价缺乏全国性统一标准，各地目前社会性商业培训认证占据较大市场份额，人社部门主导的职称评审各地发展不平衡，而且存在主导部门不同的差异，目前普遍存在的现象是由网信部门牵头开展的职称评审和公安部门牵头开展的职称评审两大主流渠道。而且除广东等省市开展了人才评价工作外，还有十多个省市没开展该项工作。从人才发展规划和行业发展的角度来看，网络安全人才评价需求旺盛。（来源：国家信息中心）

2. 新技术引发网络安全新风险

近年来，随着人工智能（AI）、区块链、大数据等新技术不断涌现，引发网络安全新风险，主要表现为一下几个方面：

新场景引发新挑战。随着互联网应用的普及，网络安全技术的应用场景也越来越广泛。在线支付、在线购物、在线教育等都离不开网络安全技术，随之而来的网络安全风险也不断激增。一是网络黑客、电信网络诈骗

等犯罪问题频发。根据公安部公布的最新数据，2022 年全国共破获电信网络诈骗案件 46.4 万起，同比上升 5%。随着科技的进步，互联网为人们的工作生活带来便利的同时，网络诈骗手法也不断翻新，封装 APP、群发邮件“引流”、AI 语音视频造假诈骗等花招层出不穷。据公安部门统计，高发电信网络诈骗案件发案占比近 80%。

虚拟货币存在网络安全风险。虚拟货币的网络安全风险主要源于其网络特性。一方面，虚拟货币存在网络漏洞和后门程序等安全风险，黑客利用这些漏洞可以窃取用户信息，进而盗取用户的虚拟货币资产。另一方面，在线交易平台的安全性、个人信息的保护程度不够等都是影响虚拟货币安全的重要因素。有些在线交易平台缺乏安全保障，导致用户在交易过程中遭受虚拟货币被盗的风险。

网络技术犯罪持续高发。随着网络技术的飞速发展，网络技术犯罪已成为一个不容忽视的问题。近年来，网络技术犯罪持续高发，带来了重大经济损失和数据安全风险。一是勒索软件攻击愈演愈烈。勒索软件是一种流行的网络攻击工具，通过加密用户文件等方式进行勒索。近年来几乎所有国家的政府、金融、医疗、交通等行业均受到影响。2022 年，勒索软件活跃程度再度飙升，攻击事件数量同比增长 13%，超过以往五年的总和。各大勒索攻击团伙不断改进攻击手法和模式，使得新一代勒索软件攻击更加复杂、更有针对性，呈现出勒索软件智能化、多重勒索常态化等趋势。以多重勒索为例，新型勒索软件攻击从单端的支付赎金即可恢复被加密的数据，逐渐演变成窃取商业信息、非法销售数据、DDoS 攻击等勒索方式结合

的新模式。Lapsus$黑客组织通过多重勒索已攻击了微软、英伟达、优步等多家知名企业，一旦受害者拒绝支付赎金，该组织就会将窃取的数据发布到网上组织非法售卖。二是软件供应链数据泄露事件频发。随着软件产业快速发展，软件供应链也愈加复杂，极易触发一系列安全问题，网络安全整体防护难度越来越大。据 IBM 发布《2022 年数据泄露成本报告》显示，五分之一的数据泄露事件是由软件供应链受陷造成，识别并遏制供应链事件所耗费的平均总时长要比全球数据泄露事件长 26 天。供应链攻陷事件的总成本是 446 万美元，比数据泄露事件的全球平均总成本高 2.5%，且后者已达到史上最高水平，比过去两年高出近 13%。据相关网络安全公司报告显示，2022 年针对软件供应商的网络攻击同比增长 146%，其中 62%的数据泄露归因于供应链安全漏洞。

网络战形势错综复杂。我国面临的网络战、封锁战、舆论战形势日益严峻。一是网络代码已经被武器化。网络攻击手段和网络攻击主体的特征明显，敌对势力利用其掌控的强大网络技术对我国连接的国际互联网实施有组织、集团化的网络断网、网域除名等，对我国政府部门、高校、重点企事业单位的网络系统进行精准的网络攻击及窃密。2022 年 9 月，美国国家安全局 NSA 对我国西北工业大学网络长时间入侵攻击，窃取关键敏感数据，对我国的国家安全造成了严重的危害。二是社交媒体被政治化、“武器化”。敌对势力利用网络漏洞实施攻击和制造散布虚假信息，利用其影响力制造发动网络舆论战，造成网络舆论信息真假难辨，从而迷惑蛊惑网民，影响民众的思想和准确分析判断，制造对立，引发社会矛盾。同时，

网络空间的军事化趋势加剧，威胁越来越大，数字外交、网络外交成为维护数字利益的政治手段。面对网络风险和挑战，加强网络安全和维护国家安全十分迫切和重要。

核心技术自主可控能力不够强。自主可控是确保网络安全的必要条件。目前，我国在网信领域（如芯片和基础软件等方面）仍存在一些短板。芯片方面，其短板在于制造工艺、装备、材料、设计工具等方面。以AI芯片为例，我国起步晚，在算法方面缺乏原始创新，目前仍依赖进口。基础软件方面，操作系统大部分依赖Windows，国产操作系统很少；大型工业基础软件，如集成电路涉及软件基本上是进口，自主研发的较少。我国亟需“扬长处，补短板”，努力突破“卡脖子”问题，提升自主可控能力，保障网络安全。（来源：国家信息中心）

行业前沿观察三：各地协会动态

导读：黑龙江省网络安全协会牵头2023年全国网络安全行业职业技能大赛（黑龙江赛区）正式启动，重庆信息安全产业技术创新联盟成功举办2023数据安全治理与发展研讨会，甘肃省首届密码知识技能大赛圆满收官，湖北顺利完成2023年第三期网络与信息安全管理员（四级）职业技能等级认定考试，宁波市计算机信息网络安全协会金融行业工作委员会成功举办金融行业网络安全交流研讨会，肇庆市计算机学会、肇庆市信息协会等14家企业机构协办“青春筑梦正当时 科教强市谱新篇”科普进校园活动，辽宁省网络安全保障工作联盟协办的铁岭市网络安全和信息化领域专家库成立暨网络安全工作座谈会顺利召开动……各地协会活跃在网络空间安全事业建设第一线，推进我国网络空间安全事业稳步向前。

关键词：协会，活动，网络安全

1.2023年全国网络安全行业职业技能大赛（黑龙江赛区）重磅启动

为深入贯彻落实党的二十大精神和省第十三次党代会精神,创新网络安全人才发现、培养、激励、管理等机制,服务网络空间治理工作,有效提升全省互联网企业、联网单位、电子数据取证企业网络安全责任意识和网络安全相关行业从业人员技能水平,由黑龙江省公安厅、省人力资源和社会保障厅、省总工会共同举办的2023年全国网络安全行业职业技能大赛（黑龙江赛区）于12月正式启动。

竞赛由理论知识考试和技能操作考核两部分组成。其中理论知识占30%，技能操作占70%。根据《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规以及人力资源社会保障部公布的网络安全管理员、网络信息审核员（互联网信息审核员）、数据安全管理员、电子数据取证分析师职业技能标准要求，结合企业及行业实际情况，适当增加新知识、新技术、新设备、新技能的相关内容。

全省网络安全行业职业技能大赛设置网络安全管理员、网络信息审核员、数据安全管理员和电子数据取证分析师等四个竞赛项目，均为单人赛项。

参赛人员均需以法人单位职工身份统一在竞赛全国统一官网（http://www.inspc.org.cn）进行线上报名，参赛的独立法人单位需设置一名单位管理员，每位选手只限报名参赛一个项目，各参赛单位的参赛选手人数不受限制。报名时间于2023年12月12日24时截止。

初赛阶段的理论知识、技能操作竞赛内容参照各比赛工种发布的技术文件，统一采用全国大赛组委会题库，在全国统一官网（http://www.inspc.org.cn）上进行。

初赛时间为2023年12月14日9:00-11:30。每个项目评选出5名选手进入全省决赛。获得初赛每个项目前5名的选手参加现场决赛。决赛时间为2023年12月19日13:30-16:30，地点为黑龙江省哈尔滨市（具体地点另行通知）。每个项目确定2名选手进入全国决赛。

全国决赛由公安部第三研究所、上海市公安局、上海市人力资源社会保障局、上海市总工会共同承办，拟于12月下旬在上海市举办线下赛，具体时间、地点由全国组委会另行通知。（来源：黑龙江省网络安全协会）

2. 重庆：成功举办2023数据安全治理与发展研讨会

12月13日，2023数据安全治理与发展研讨会成功举办。本次研讨会由重庆信息安全产业技术创新联盟、重庆人文科技学院主办，重庆市合川区网络安全学会承办，重庆信息安全产业知识产权联盟、重庆市信息安全产学研联合体、网安加社区协办。

重庆市经信委原二级巡视员刘伟、重庆人文科技学院计算机工程学院副院长金维宏分别发表了致辞。

刘伟表示，数据已经成为信息社会的核心资源和支撑，需要各方加强数据安全治理与发展的研究与实践。

金维宏提出，只有通过深入研究和广泛合作，才能共同建立一个可靠、安全、创新的数据环境。

研讨会上，西南大学副教授林已杰进行了《数据安全治理思考与探索——以高校为例》的主题演讲，分享了教育行业数据安全现状、高校数据安全治理规划等方面的内容。

重庆市合川区妇幼保健院党委副书记兼合川区网络安全学会副会长吴健进行了《医疗健康数据安全治理与实践》的主题演讲，指出医疗健康大数据的现状与安全风险，并分享了数据安全治理与实践在医疗健康领域的趋势与运用。

西部智联数字科技（重庆）有限公司售前经理蒋刚进行了《智能网联汽车信息安全建设实践》的主题演讲，分析了智能网联汽车企业面临的信息安全挑战并给出了实际解决方案。

开源网安（深圳）技术有限公司副总经理王颉进行了《从软件供应链安全视角看数据安全保障》的主题演讲，从数字化转型中的数据安全风险、软件供应链安全现状、软件供应链安全保障实践等方面进行了深度阐述。

北京启明星辰信息安全技术有限公司西南大区技术总监朱毅进行了《打造能源数字化转型中的数据安全防护能力》的主题演讲，指出能源数字化转型中存在的问题与风险，并分享了自己的思考与实践案例。

会后，大家积极进行了交流，碰撞出诸多思维火花。

与传统的网络安全不同，数字化时代的数据安全一定与数字化业务逻辑有更多的交互与融入，数据需要做安全治理、分类分级，对于大数据的“流转”要进行分级安全管控和防护，以保障数据的安全可控流转。在数据安全体系化的建设中，需要系统化的思维与建设框架，由国家、行业和企业多方共同协作落地完成，共同保障各类数据共享应用场景安全，数据安全已经成为支撑数字经济的“底板工程”。

本次数据安全治理与发展研讨会聚焦了高校和行业专家，聚焦于数据安全的新思考、新挑战，探讨在各行业不同的业务场景下，在数据发展方向如何达到发展与安全的平衡，该如何开拓从体系化框架到建设实践之路。（来源：重庆信息安全产业技术创新联盟）

3. 甘肃省首届密码知识技能大赛圆满收官

12 月 2 日，由甘肃省国家密码管理局、兰州市国家密码管理局指导，甘肃省商用密码行业协会、西北师范大学主办，甘肃烽侦网络安全研究院提供技术支持的甘肃省首届密码知识技能大赛圆满收官。

本次竞赛以团体比赛为主、面向甘肃省内普通高等院校，吸引了来自省内 9 所高校的 30 支队伍 90 余名师生参加，通过知识竞赛与技能竞赛两部分的激烈角逐，分别颁发了一个特等奖、2 个一等奖、3 个二等奖、5 个三等奖。

此次大赛是甘肃省内举办的首届密码知识技能大赛，以此次比赛为契机，一是能够发掘密码人才，为省内高校师生提供密码技能展示的平台，激活更多年轻学子学密码的热情，让更多人才投身到密码事业的浪潮中；二是能够提高密码安全意识，在全省内深入普及密码法、密码安全教育，营造了知密码、懂密码、用密码的浓厚氛围；三是能够切磋密码技术，通过研究和交流密码技能，强化高校学生创新意识和实践能力，助力密码人才的成长和进步。（来源：甘肃省商用密码行业协会）

4. 湖北：2023 年第三期网络与信息安全管理员（四级）职业技能等级认定考试顺利完成

12 月 16 日，湖北省信息网络安全协会成功举办了第三期网络与信息安全管理员（四级）职业技能等级认定考试。此次考试涵盖了众多业内专业人士，以及对此领域充满热情的初学者。

此次考试的范围广泛且深入，涵盖了网络与信息安全管理的各个方面，包括但不限于安全策略制定、安全设备配置、安全软件编写，以及在各种环境下的实际操作。经过严谨的评审和测试，考试的组织和实施均获得了圆满成功。

这场考试不仅是一次知识和技能的检验，更是一次对网络与信息安全领域从业者责任和使命的确认。通过这次考试，我们看到了湖北省内网络与信息安全领域从业者们的专业素养和职业精神，他们以实际行动守护着网络空间的安全，为湖北省乃至全国的信息网络安全贡献着力量。

这次考试的成功举办，不仅是对协会工作的肯定，也为湖北省乃至全国的信息安全领域注入了一股新的活力。它不仅推动了信息安全领域的发展，也为广大从业人员提供了一个展示自我、提升技能的舞台。

展望未来，湖北省信息网络安全协会将继续致力于提升信息安全领域的职业技能等级认定工作，为湖北省乃至全国的信息安全事业做出更大的贡献。我们期待着更多的专业人士加入到这个行列中来，共同为信息安全领域的发展添砖加瓦。（来源：湖北省信息网络安全协会）

5. 浙江宁波：金融行业网络安全交流研讨会成功召开

12 月 14 日，宁波市计算机信息网络安全协会金融行业工作委员会举办了金融行业网络安全交流研讨会，会议在兴业银行宁波分行拉开帷幕。兴业银行宁波分行副行长俞裕捷热情欢迎了各位嘉宾，出席本次会议的有宁波市公安局网安支队副支队长倪彦波、宁波市计算机信息网络安全协会会长刘柏嵩、协会金融行业工作委员会主任朱朝晖以及部分金融行业科技处负责人等精英。

活动伊始，与会人员参观了兴业银行行史馆和数据中心，深度了解了兴业银行在信息化建设的先进设施。接下来，兴业银行、中信银行等业界代表展开了技术交流和经验分享。同时，宁波市公安局网安支队三大队周劭文教导员对当前的网络安全形势进行了通报，为与会者通报了清晰的行业背景和当前面临的挑战，并提出了安全建议。

宁波市公安局网安支队副支队长倪彦波的讲话将研讨会推向了高潮，倪支对我市金融单位在网络安全方面取得的显著成就给予充分肯定，并对他们在网络安全领域做出的卓越贡献表示了感谢，同时提出了具有远见的期望。他寄望未来各方能够深化合作，共同迎接不断严峻的网络安全挑战，确保金融系统的长期稳健运行。

本次会议不仅突显了技术交流与经验分享的重要性，更为金融行业网络安全的构建提供了宝贵契机。通过深入研讨，各方在应对网络安全威胁的共同努力中迈出了坚实的一步。研讨会的成功召开对于推动宁波市金融行业网络安全水平的提升具有极其重要的意义。（来源：宁波市计算机信息网络安全协会）

6. 广东四会：“青春筑梦正当时 科教强市谱新篇”科普进校园活动

为弘扬科学精神，普及科学知识，进一步营造热爱科学、鼓励创新、敢于实践的良好校园氛围，12 月 7 日，由广东省四会市科学技术协会和四会市教育局主办、四会市四会中学（东城校区）承办，四会市市场监督管理局、肇庆市计算机学会、肇庆市信息协会等 14 家企业机构协办的“青春筑梦正当时 科教强市谱新篇”科普进校园活动在四会中学（东城校区）开展，为全校 1800 名师生送去丰富多彩的科普大餐，更为同日如火如荼举行的校园体艺节增添一抹科技亮色。

在科普展示区，来自肇庆市科协的“科普大篷车”为同学们带来了一场视觉、听觉、触觉的全方位科普盛宴。展品包括了尖端放电、电影

原理、风力发电等共10项，同学们围在展区交流思考、动手尝试，亲身感受科技的魅力，充分满足了好奇心。

在青少年竞赛区，学生们聚精会神地参观青少年科技创新大赛的参赛展品，来自四会市青少年科技教育协会的志愿者邀请同学们沉浸式体验青少年科技实践能力挑战赛项目木牛流马、青少年机器人竞赛项目红色之旅、OM无所不能、 无人机足球，不仅为师生提供了互相学习和交流的平台，更激发了四会市青少年在科技领域的创意和潜力。

本次活动还设置了AI下棋机器人、3D打印展示、睿抗机器人互动、自然科学展览、眼健康移动科普、食品安全科普等共8个科普项目展示区。好玩、有趣的科普展示让学生们在轻松愉悦的互动体验中学习到科学知识，通过观察、互动和思考了解科学的真谛。

这次科普进校园活动的成功开展，不仅为同学们提供了近距离接触科学、感受科学的机会，还增强了他们的创新思维和动手实践能力，激发孩子们对科学的兴趣和热爱，为未来的科技创新和发展奠定了坚实的基础。下一步，学会将继续配合政府部门，充分利用科普资源，继续开展科普进校园活动，拓宽青少年科技视野，增进青少年动手能力，助力科技梦想开花结果。（来源：肇庆市计算机学会）

7.辽宁铁岭：网络安全和信息化领域专家库成立

12月8日，由铁岭市委网信办主办，辽宁省网络安全保障工作联盟协办的铁岭市网络安全和信息化领域专家库成立暨网络安全工作座

谈会在铁岭顺利召开。铁岭市网络安全和信息化领域专家库专家、市直关键信息基础设施单位网络安全技术负责人、以及联盟技术支撑单位有关网络安全专家50余人参加。铁岭市委网信办分管日常工作的副主任高迅出席会议并发表讲话。

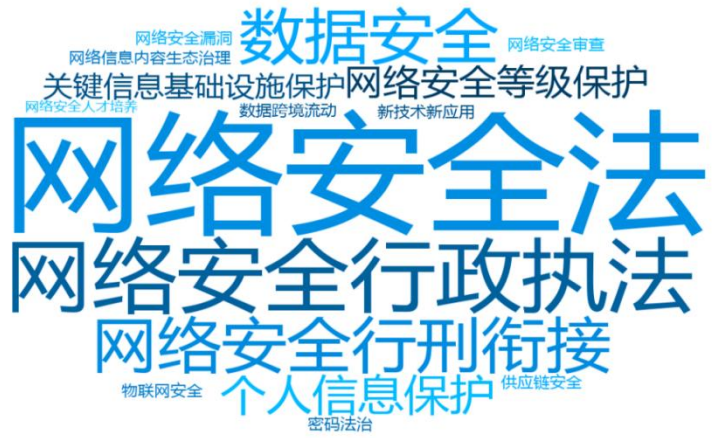
铁岭市网络安全和信息化领域专家库由30名来自不同领域的网络专家组成，成立后将配合网信办开展网络安全检查、网络安全应急处突、信息化项目评估等工作，并提供网络安全技术支持，推动全市网络安全工作再上新台阶，为铁岭市实施全面振兴新突破三年行动提供可靠的网络安全保障。

在座谈环节，与会专家围绕“发挥网络安全专家智库作用，支撑网络安全工作”，“加强关键信息基础设施网络安全保障能力，降低网络安全风险”，以及“发挥网络安全行业组织的桥梁纽带作用，促进行业健康发展”等方面内容进行广泛交流，并对提出的问题进行答疑解惑。

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

……