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11月 第4期(总 第4期)

2023年11月20日

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

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：10 月，针对网友反映航班信息泄露威胁乘客个人信息及财产安全问题，民航局表示一直以来高度重视数据治理问题，已出台 7 部行业标准和 1 部信息通告规范民航数据治理。目前民航局正在编制相关文件，进一步加强重要数据保护。近年来，以航班故障取消为由针对乘客进行诈骗的新闻时有出现。此类事件的背后蕴含着乘客个人信息泄露的安全问题，需要公安机关、网信部门、行业主管部门、航空公司、第三方网络渠道代理公司等主体在各自职责义务范围内加强个人信息保护，严防乘客个人信息泄露，严厉打击诈骗等下游犯罪活动。

《密码法》颁布四周年研讨会暨《商用密码管理条例》高级研修班开班仪式成功举办，围绕“《密码法》颁布四周年回顾与展望”这一主题展开报告与研讨。

关键词：航空、个人信息泄露、密码法实施四周年

1. 民航局回应旅客信息泄露：正在编制相关文件，进一步加强重要数据保护

10 月 29 日消息，有网友近日呼吁严查旅客航班信息泄露及利用其诈骗问题，该网友通过人民网领导留言板反映：最近其和朋友们在某某地图App搜索航班信息并预订了机票，有三人接到诈骗电话，对方以航空公司客服的名义，以机械故障航班取消为由，让网友提供支付宝账号给予补偿，且能报出网友的姓名、电话、身份证、航班信息等。

该网友认为，一来假报航班取消信息干扰旅客行程，二来这种信息泄露问题极其严重，如有不明真相的旅客将会造成严重的财产损失。希望民航局协调公安部门严查第三方网络渠道代理公司的旅客信息泄露和利用航班信息诈骗问题。

中国民用航空局回应称：民航局高度重视数据治理工作，认真贯彻《网络安全法》《数据安全法》《个人信息保护法》等相关规定，先后出台“7+1”智慧民航数据治理系列规范（7 部行业标准、1 部信息通告），指导规范行业单位开展数据共享、数据服务、数据安全等工作。目前，为落实民航领域数据分类分级保护有关要求，民航局正在编制相关文件，进一步加强对重要数据的保护。（来源：中国交通新闻网）

2. 《密码法》颁布四周年研讨会暨《商用密码管理条例》高级研修班开班仪式成功举办

10 月 26 日，《密码法》颁布四周年研讨会暨《商用密码管理条例》高级研修班开班仪式成功举办。

本次研讨会由密码法治实践创新基地和中国信息安全法律大会专家委员会主办，西交苏州信息安全法学所和公安部第三研究所网络安全法律研究中心承办。会议围绕“《密码法》颁布四周年回顾与展望”这一主题展开报告与研讨。研讨会暨开班仪式由公安部第三研究所网络安全法律研究中心主任黄道丽主持。（来源： 苏州信息安全法学所）

境内前沿观察二：立法动向

导读：10 月，《未成年人网络保护条例》正式通过，自 2024 年 1 月 1 日起施行。这是我国出台的第一部专门性未成年人网络保护综合立法，重点就规范网络信息内容、保护个人信息、防治网络沉迷等作出规定。截至 2023 年 6 月，我国网民规模已达 10.79 亿，未成年网民规模突破 1.91 亿。《未成年人网络保护条例》的出台标志着我国未成年人网络保护法治建设进入新阶段。

中央网信办发布《全球人工智能治理倡议》，提出人工智能治理攸关全人类命运，是世界各国面临的共同课题，各国应秉持共同、综合、合作、可持续的安全观，坚持发展和安全并重的原则，通过对话与合作凝聚共识。

各省市持续发布政策文件，为数字经济发展提供制度保障。福建省、厦门市分别发布《福建省一体化公共数据体系建设方案》《厦门市公共数据授权运营管理暂行办法（征求意见稿）》，加强公共数据合法利用和安全管理。上海市人大常委会公布《上海市十六届人大常委会立法规划（2023-2027 年）》，涉及《上海市促进浦东新区数据流通交易若干规定》《上海市促进浦东新区跨境数据流通发展若干规定》等立法项目。

关键词：未成年人网络保护、人工智能、数据流通、公共数据、行政处罚裁量基准

（一）国家层面动向

1.《未成年人网络保护条例》公布，系我国第一部专门性未成年人网络保护综合立法

10 月 16 日，国务院总理李强签署第 766 号国务院令，公布《未成年人网络保护条例》，自 2024 年 1 月 1 日起施行。

条例是我国出台的第一部专门性未成年人网络保护综合立法。条例共七章六十条，重点规定以下内容：（1）健全未成年人网络保护体制机制。明确国家网信部门负责统筹协调未成年人网络保护工作，并依据职责做好未成年人网络保护工作。明确国家新闻出版、电影部门和国务院教育、电信、公安等有关部门依据各自职责做好未成年人网络保护工作；（2）促进未成年人网络素养。规定未成年人网络保护软件以及专门供未成年人使用的智能终端产品应当具有保护未成年人个人信息权益、预防未成年人沉迷网络等功能；（3）加强网络信息内容建设。明确网络产品和服务提供者发现危害或者可能影响未成年人身心健康信息的处置措施和报告义务。要求网络产品和服务提供者建立健全网络欺凌行为的预警预防、识别监测和处置机制；（4）保护未成年人个人信息。针对未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者，提出定期开展未成年人网络保护影响评估、提供未成年人模式或者未成年人专区、制定专门的平台规则等要求。（来源：中国政府网）

（二）部委层面动向

1. 中央网信办发布《全球人工智能治理倡议》

10 月 18 日，中央网信办发布《全球人工智能治理倡议》。倡议指出，人工智能治理攸关全人类命运，是世界各国面临的共同课题。在世界和平与发展面临多元挑战的背景下，各国应秉持共同、综合、合作、可持续的安全观，坚持发展和安全并重的原则，通过对话与合作凝聚共识，构建开放、公正、有效的治理机制，促进人工智能技术造福于人类，推动构建人类命运共同体。

倡议共计十一条，涉及发展理念、原则、安全保障、制度体系、伦理等诸多方面。其中，倡议提出发展人工智能应坚持“以人为本”理念，以人工智能助力可持续发展；面向他国提供人工智能产品和服务时，应尊重他国主权，严格遵守他国法律，接受他国法律管辖；发展人工智能应坚持“智能向善”的宗旨，各国尤其是大国对在军事领域研发和使用人工智能技术应采取慎重负责的态度；推动建立风险等级测试评估体系，实施敏捷治理，分类分级管理，快速有效响应。研发主体不断提高人工智能可解释性和可预测性，提升数据真实性和准确性，确保人工智能始终处于人类控制之下，打造可审核、可监督、可追溯、可信赖的人工智能技术。逐步建立健全法律和规章制度，保障人工智能研发和应用中的个人隐私与数据安全，反对窃取、篡改、泄露和其他非法收集利用个人信息的行为。（来源：中国网信网）

2. 工信部等六部门联合印发《算力基础设施高质量发展行动计划》

10 月 8 日，工信部、中央网信办、教育部等六部门联合印发《算力基础设施高质量发展行动计划》，旨在加强计算、网络、存储和应用协同创新，推进算力基础设施高质量发展，充分发挥算力对数字经济的驱动作用。

行动计划指出，要增强算力基础设施网络安全保障能力。严格落实网络安全法律法规要求，开展通信网络安全防护工作。要强化算力基础设施产业链供应链安全。加强产业链协同联动，逐步形成自主可控解决方案，鼓励算力基础设施采用安全可信的基础软硬件进行建设，保障供应链安全。

行动计划强调，要强化算力基础设施数据安全保护能力。加强数据分类分级保护，根据监管要求对重要和核心数据实行精准严格管理。制定数据全生命周期安全防护要求和操作规程，配套建设数据安全风险监测技术手段，加强数据安全风险的分析、研判、预警和处置能力。（来源：工信部）

3. 工信部发布《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》

10 月 9 日，工信部发布《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》。征求意见稿适用于工业和信息化领域重要数据、核心数据处理者对其数据处理活动的安全风险评估。

征求意见稿明确评估对象为数据处理活动中涉及的目的和场景、管理体系、人员能力、技术工具、风险来源、安全影响等要素，并按照以上要素细化具体评估内容。同时，征求意见稿明确评估期限、重新申报评估的

情形、可采取的评估方式，并对委托评估、评估协作、风险控制和评估报告报送等作出要求。

征求意见稿要求重要数据和核心数据处理者每年完成至少一次数据安全风险评估，并形成评估报告。数据安全风险评估结果有效期为一年，自评估报告首次出具之日起计算。重要数据和核心数据处理者可以自行或者委托具有工业和信息化数据安全工作经验的第三方评估机构开展评估。（来源：工信部）

4. 工信部发布《工业互联网安全分类分级管理办法（公开征求意见稿）》

10 月 24 日，工信部发布《工业互联网安全分类分级管理办法（公开征求意见稿）》。征求意见稿共五章二十一条，包括总则、企业分类分级、网络安全管理、支持与保障及附则。

征求意见稿规定，工业互联网企业应当按照工业互联网安全定级相关标准规范，结合企业规模、业务范围、应用工业互联网的程度、运营重要系统的程度、掌握重要数据的程度、对行业发展和产业链供应链安全的重要程度以及发生网络安全事件的影响后果等要素，开展自主定级。工业互联网企业级别由高到低分为三级、二级、一级。当企业定级要素发生较大变化，可能影响企业定级结果时，企业应当在发生变化的三个月内重新定级。同时具有联网工业企业、平台企业、标识解析企业中两种及以上属性的企业，应当按照不同类型分别定级。（来源：工信部）

5. 科技部等十部门联合印发《科技伦理审查办法（试行）》

10 月 8 日，科技部、教育部、工信部等十部门联合印发《科技伦理审查办法（试行）》。

审查办法指出，涉及以人为研究参与者的科技活动，审查重点在于生物样本的收集、储存、使用及处置合法合规，个人隐私数据、生物特征信息等信息处理符合个人信息保护的有关规定。所提供的知情同意书应当内容完整、风险告知客观充分、表述清晰易懂，获取个人知情同意的方式和过程合规恰当。

审查办法强调，涉及数据和算法的科技活动，审查重点在于数据的收集、存储、加工、使用等处理活动以及研究开发数据新技术等符合国家数据安全和个人信息保护等有关规定，数据安全风险监测及应急处理方案得当。（来源：科学技术部）

6. 国家密码管理局发布《电子政务电子认证服务管理办法（征求意见稿）》

10 月 17 日，国家密码管理局发布《电子政务电子认证服务管理办法（征求意见稿）》。征求意见稿共六章四十四条，包括总则、资质认定、行为规范、监督管理、法律责任和附则。

征求意见稿规定：（1）外商投资电子政务电子认证服务，影响或者可能影响国家安全的，应当依法进行外商投资安全审查。（2）电子政务电子认证服务机构应当每年至少进行一次电子政务电子认证服务合规性评估，对发现的问题及时整改，并及时向住所地省、自治区、直辖市密码管理部

门报送合规性评估报告。（3）发生重大安全风险和安全事件，重要系统、关键设备事故，关键岗位人员变动或重大法律诉讼情形之一的，电子政务电子认证服务机构应当自发生之日起15日内向住所地省、自治区、直辖市密码管理部门报告。（来源：国家密码管理局）

7. 证监会发布《证券期货业信息安全运营管理指南》

10月23日，证券监督管理委员会发布9项金融行业推荐性标准，其中包括JR/T 0295—2023《证券期货业信息安全运营管理指南》，自公布之日起施行。

指南提供了开展信息安全运营管理中安全管理、基础安全管理、信息资产管理、漏洞管理、开发安全管理、数据安全管理、集中监控与响应管理以及持续改进管理的指导思路及方法，并给出各管理域的度量指标以及行业最佳实践。指南适用于证券期货行业的核心机构（证券交易所、期货交易所、登记结算公司等）和经营机构（证券公司、期货公司、基金管理公司等）在完成基础的信息安全建设后开展的信息安全运营管理工作。（来源：证券监督管理委员会）

8. 全国信安标委发布《生成式人工智能服务安全基本要求（征求意见稿）》

10月11日，全国信安标委发布《生成式人工智能服务安全基本要求（征求意见稿）》，在语料安全、模型安全、安全措施、安全评估等方面给出生成式人工智能服务的基本要求。

征求意见稿要求，生成式人工智能服务提供者要保证语料来源安全、语料内容安全、语料标注安全等多方面安全。服务提供者不应使用未经主管部门备案的基础模型，此外要保证模型生成内容安全，即生成内容准确可靠，服务透明。

在安全措施方面，征求意见稿指出，生成式人工智能服务提供者应针对人工智能模型适用人群、场合、用途等加强安全措施。人工智能服务适用于未成年人的，应当允许监护人设定未成年人防沉迷措施，并通过密码保护。（来源：全国信安标委）

（三）地方层面动向

1. 上海市人民政府印发《上海市进一步推进新型基础设施建设行动方案（2023-2026 年）》

9 月 15 日，上海市人民政府印发《上海市进一步推进新型基础设施建设行动方案（2023-2026 年）》。

方案提出到 2026 年底，全市新型基础设施建设水平和服务能级迈上新台阶，人工智能、区块链、第五代移动通信（5G）、数字孪生等新技术更加广泛融入和改变城市生产生活，支撑国际数字之都建设的新型基础设施框架体系基本建成的目标。方案明确构建泛在互联的高水平网络基础设施、建设云网协同的高性能算力基础设施、建设数智融合的高质量数据基础设施、打造开放赋能的高能级创新基础设施以及打造便捷智敏的高效能终端基础设施五大主要任务。（来源：上海市人民政府）

2. 上海市委网信办发布《上海网站平台受理处置涉企网络侵权信息举报工作指引（试行版）》

10 月 19 日，上海市委网信办发布《上海网站平台受理处置涉企网络侵权信息举报工作指引（试行版）》。指引规定上海网站平台受理处置涉企网络侵权信息举报工作的工作机制要求、受理处置要求、试点工作要求，适用于上海网站平台开展涉企网络侵权信息举报工作。

指引从工作机制、受理处置、试点工作三个主要方面对网站平台作出要求。工作机制方面，要求健全规章制度，强化队伍建设，建立台账制度，接受检查监督；受理处置方面，要求建立举报专区，明确受理重点，明确受理范围，统一受理条件，明确处置重点，统一处置标准；试点工作方面，要求强化标签功能、加快办理时效、优化反馈机制、落实信息发布、设立投诉窗口、加强宣传推广。（来源：网信上海）

3. 上海市人大常委会公布立法规划，涉及多项数字经济发展立法项目

10 月 20 日，上海市人大常委会公布《上海市十六届人大常委会立法规划（2023-2027 年）》，共安排立法项目 165 件。

立法规划涉及多项数字经济发展立法项目，其中正式项目包括《上海市促进浦东新区数据流通交易若干规定》《上海市促进浦东新区健康医疗数据发展应用若干规定》，预备项目包括《上海市促进城市数字化转型条例》《上海市促进浦东新区跨境数据流通发展若干规定》《上海市促进浦

东新区智能算力产业发展若干规定》，调研项目包括《上海市促进电子商务发展规定》。（来源：上海人大）

4. 福建省印发《福建省一体化公共数据体系建设方案》

9 月 30 日，福建省人民政府办公厅印发《福建省一体化公共数据体系建设方案》。

建设方案指出要健全数据安全制度规范。建立健全公共数据分类分级保护、数据使用和安全审查等制度。健全数据安全工作责任机制，围绕数据全生命周期构建全方位、多层级的一体化公共数据安全管理体系。强化“管业务必须管业务数据、管业务数据必须管业务数据安全”理念，按照“谁管理、谁负责，谁使用、谁负责”的原则，明确数据流转全流程中各方权利义务和法律责任。

建设方案强调要强化数据安全运行管理。完善数据安全运维运营保障机制，明确各方权责，加强数据安全风险信息的获取、分析、研判、预警。建立健全数据安全运行监管机制，推动建立一体化数据安全监测预警体系，全面提升数据安全保障和风险防范能力。加强政务系统建设安全管理，确保数据安全。（来源：福建省人民政府）

5. 福建省厦门市发布《厦门市公共数据授权运营管理暂行办法（征求意见稿）》

10 月 10 日，福建省厦门市工业和信息化局、厦门市大数据管理局联合发布《厦门市公共数据授权运营管理暂行办法（征求意见稿）》，旨在从

授权方式、行为规范、数据安全与监督管理等方面规范厦门市公共数据授权运营。

授权方式方面，征求意见稿指出，公共数据融合开发平台应符合有关法律法规要求的网络安全等级保护标准和商用密码安全性评估要求，具备数据治理、脱敏脱密、数据应用合规审核等功能，确保全流程操作可追踪，数据可溯源。

行为规范方面，征求意见稿要求，涉及个人信息、商业秘密的公共数据须获得相关数据所指向的特定自然人、法人、非法人组织的授权同意后，按应用场景使用，相关授权记录应按有关法律、法规要求留存。

数据安全与监督管理方面，征求意见稿强调，一级开发主体应当履行公共数据安全管理职责，大数据主管部门应当会同有关部门建立健全监督机制，加强对公共数据融合开发平台运营、数据管理、开发利用等安全合规情况的监督检查，并督促整改落实。（来源：厦门市工业和信息化局）

6. 内蒙古自治区发布《内蒙古自治区电信领域数据安全管理实施细则（征求意见稿）》

10 月 8 日，内蒙古自治区通信管理局发布《内蒙古自治区电信领域数据安全管理实施细则（征求意见稿）》。征求意见稿共五章二十九条，涉及基础性数据安全保护要求、数据全生命周期安全保护要求等内容。

征求意见稿要求，电信领域重要和核心数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，负责牵头内部数据安全管理工作，明确数据处理关键岗位和岗位职责，要并配

备具备相应技能水平的专职人员，定期参与行业认可的数据安全考核与培训。（来源：内蒙古自治区通信管理局）

7. 内蒙古自治区印发《内蒙古自治区推动数字经济高质量发展工作方案（2023—2025 年）》

10 月 10 日，内蒙古自治区人民政府办公厅印发《内蒙古自治区推动数字经济高质量发展工作方案（2023—2025 年）》。

方案明确六项重点任务，包括优化产业空间布局、推动技术产品创新、构建良好数字经济产业生态、加快市场主体培育、加快数字基础设施建设以及强化发展要素支撑。

方案指出，要夯实安全底座、增强通信网络、数据中心等关键基础设施安全韧性，构建共建、共享、共用、共维的网络安全协同防护体系。完善制度规则，建立数据安全产品目录和技术清单，做好数据分类分级、资源目录管理、质量管理、流动风险监测等数据安全保障，强化行业数据安全治理能力。定期开展网络安全攻防演练，提升网络安全态势感知、主动防御、监测预警、安全防护能力。（来源：内蒙古自治区人民政府）

8. 北京市发布《北京市首席数据官制度试点工作方案》

10 月 20 日消息，北京市经信局近日发布《北京市首席数据官制度试点工作方案》，明确北京将在全市政府机关内全面推进首席数据官制度，建立健全数据汇聚、治理、共享、开放、应用和信息化统筹工作机制，创新数据共享开放和开发利用模式，提高数据治理和数据运营能力和水平。

工作方案选取了13家北京市级委办局、各区级政府和北京经济技术开发区作为试点单位，自行灵活设立首席数据官，职责范围包括推进数字政府建设、加强数据资源管理、提升指导监督能力、提高数字思维素养、促进人才队伍建设等。同时，工作方案还鼓励各区级政府选取有条件的下级单位开展试点工作，积极鼓励各类企业设立首席数据官。（来源：中国政府网）

9. 新疆维吾尔自治区公布《新疆维吾尔自治区网络安全管理行政处罚裁量权基准适用规定》

10月21日消息，新疆维吾尔自治区近日公布《新疆维吾尔自治区网络安全管理行政处罚裁量权基准适用规定》。

规定适用于在新疆维吾尔自治区域内对违反网络安全管理法律、法规或规章的行为实施行政处罚。网信部门、公安机关在职权范围内，根据法律、法规和规章的规定，综合考虑违法行为的事实、性质、情节、社会危害程度以及当事人主观过错等因素，决定是否给予行政处罚、给予行政处罚的种类和幅度的权限。网信部门依职权管辖本行政区域内的网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。公安机关依职权管辖本行政区域内危害公共信息网络的违法犯罪案件。

规定还包括《网络安全管理行政处罚裁量权基准》，明确《网络安全法》《数据安全法》《个人信息保护法》相关违法行为的处罚依据与裁量基准。（来源：新疆网警）

10. 山东省发布《关于印发支持推进全省数字经济高质量发展的若干措施的通知》

10 月 25 日，山东省大数据局发布《关于印发支持推进全省数字经济高质量发展的若干措施的通知》。

文件围绕强化工作统筹协调，保障数字经济持续发展；加大“三招三引”力度，促进数字经济快速发展；释放数据要素价值，激发数字经济创新发展；深化数字政府建设，引领数字经济高质量发展；加速数字社会建设，推动数字经济全面发展；夯实数字基础底座，支撑数字经济稳固发展等六个方面作出规定。（来源：山东省大数据局）

境内前沿观察三：治理实践

导读：10 月，国家数据局正式挂牌，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。公安部成立网络安全法律咨询委员会，旨在搭建多主体交流平台，构建共建、共治、共享的网络空间治理模式，推动网络空间法治建设。

江西南昌警方公布“夏季行动”成果，通报处置网络安全漏洞、网站攻击事件 213 起，发现并整改属地互联网企业问题隐患 317 处。甘肃警方公布侵犯公民个人信息类违法犯罪专项打击整治行动成果，检查企业单位 1034 家，查处行政案件 272 起；同时积极开展柔性执法，对于首次违法、危害后果轻微的 203 家企业单位采用责令整改、约谈等柔性执法方式进行提醒督促。

此外，国家网信办指导广东省网信办对“夸克”平台和“网易CC”直播平台相关负责人进行约谈；上海市网信办会同市公安局网安总队对新浪上海进行约谈；重庆市武隆区网信办在重庆市网信办指导下对属地某公司负责人进行约谈。上述治理实践中均涉及“约谈”这一行政指导行为。《网络安全法》《数据安全法》《个人信息保护法》规定有关部门在履行职责中，有权按照规定的权限和程序对有关组织、个人进行约谈，并要求其采取措施进行整改，消除隐患。

结合10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.建立人员安全意识教育培训及责任追究制度；2.采取信息系统防病毒、防网络攻击等技术措施；3.对存储的数据进行加密处理，办公电脑设置复杂的开机密码；4.对个人信息实行分类管理、采取加密及去标识化等技术措施；5.加强风险监测，发生安全事件时采取处置措施，并主动向有关部门报告。

关键词：国家数据局、网络安全法律咨询委员会、柔性执法、约谈、网络水军、安全漏洞

（一）公安机关治理实践

1. 公安部成立网络安全法律咨询委员会

10 月 10 日至 11 日，公安部在京召开网络安全法律咨询委员会成立大会暨网安法制专项研讨会。

会议指出，公安部成立网络安全法律咨询委员会是贯彻落实习近平法治思想的必然要求，是提升中国网络空间话语权的重要举措，是公安机关推进法治中国、平安中国建设的应有之义，是公安机关搭建的多主体交流平台，对构建共建、共治、共享的网络空间治理模式，推动网络空间法治建设具有重要意义。

会议强调，希望咨询委员会委员充分发挥主观能动性，积极参与，推动公安机关网络法治建设迈上更高台阶。一是加强网络安全法律研究，及时跟进网络领域发展趋势，跟踪研究国内外网络安全法律政策，为网络法治建设建言献策；二是严厉打击整治新型网络犯罪，针对网络安全新形势新特点，加强调查研究，研提针对性对策，为公安机关依法开展网络犯罪防治等工作提供有效支撑；三是防范新技术新应用安全风险，充分发挥专业优势，为互联网产业安全发展出谋划策，从法律、技术、管理等层面防范新技术新应用安全风险；四是强化网络综合治理，在本领域支持网络综合治理工作，为提高公安机关互联网安全监管工作质效、完善网络综合治理机制贡献智慧，打造共建、共治、共享的网络安全新格局。（来源：公安部网安局）

2. 江西南昌网警公布“夏季行动”成果：办理行政案件203起

10月16日，江西南昌网警公布“夏季行动”成果。

一是秉持“依法打击、生态打击”理念，积极开展“净网”专项行动，全力挖源头、打团伙、断链条，始终保持对涉网犯罪的凌厉攻势，切实保障人民群众生命财产安全。行动期间，全市侦办侵犯公民信息、黑客攻击等涉网案件183起，摧毁帮信等团伙23个，抓获犯罪嫌疑人230名，侦破某学院被非法侵入计算机系统获取个人信息案、利用苹果手机漏洞窃取公民个人信息案、伪造文凭案等一批经典案例，有效遏制涉网犯罪蔓延态势。

二是聚焦与企业群众生产生活紧密相关的网络谣言、网络水军、网络暴力等网络乱象，推动“打防宣治”整体发力，强化网络安全执法，压实网络平台安全主责，集中开展互联网销售危险化学品、APP违法违规收集使用个人信息等专项整治，针对网络直播短视频乱象推动“涤瑕治乱”专项行动。行动期间，全市共组织检查598家次，办理行政案件203起，约谈网络主播42人次。特别依托“百日打谣”专项行动，坚决防范打击造谣传谣违法犯罪，先后查处造谣案件6起，行政、刑事拘留5人，发送防谣手机短信600余万条，发现上报有害信息5890条。

三是联合市委网信办等单位，依托设在支队的全市信息通报中心、等级保护办公室两大枢纽，打造“基础排查、日常管理、执法检查、实时监测、态势感知、攻防检验、应急指挥”七维一体防控体系，常态做好全市关基设施、行业部门、网络平台的监督管理，联动举行“网络安全宣传周”活动，不断提升网络安全防护能力。行动以来，全市通报处置网络安全漏

洞、网站攻击事件213起，发现并整改属地互联网企业问题隐患317处，破获江西省首例无人机系统破解禁飞限飞限高程序案件，有效筑牢网络安全防线。（来源：南昌网警）

3. 甘肃警方重拳整治侵犯公民个人信息乱象：查处行政案件272起

10月18日消息，甘肃公安机关网安部门近日部署开展专项打击整治行动，重点围绕电信网点、房产中介、教培机构、售楼中心、快递门店等侵犯公民个人信息类违法犯罪活动易发多发领域，周密部署、主动出击，统一开展打击整治行动。

截止目前，已出动警力1736人次，检查企业单位1034家，破获刑事案件3起，查处行政案件272起，有力震慑遏制此类违法犯罪活动，同时全省网安部门在集群战役中秉持“优化营商环境服务企业发展”工作理念，以压实企业主体责任、消除问题隐患为根本目的，对于首次违法、危害后果轻微的203家企业单位，按照甘肃省公安机关行政处罚“两轻一免”清单和“裁量权基准”，采用责令整改、约谈等柔性执法方式提醒督促，取得良好的社会效果和法律效果。（来源：每日甘肃）

4. 因未履行网络安全保护义务，厦门市某培训机构被行政处罚

10月11日消息，因未履行网络安全保护义务，福建省厦门市公安局思明分局近日对某教培机构进行行政处罚。

2023年3月，厦门市民吴先生接到自称某教培机构工作人员的电话，对方称机构将关门停业，要为其办理学费清退。吴先生随后被对方拉进一个聊天群，并按照对方要求下载安装了某金融交易APP，后被诈骗上万元。

警方启动对该教培机构履行网络安全保护义务情况的监督检查，经查该机构未落实数据安全保护主体责任、未建立人员安全意识教育培训及责任追究制度、未采取信息系统防病毒防网络攻击等技术措施，存在未履行网络安全保护义务的违法行为。根据《网络安全法》第二十一条、第五十九条之规定给予该教培机构罚款一万元，直接负责的主管人员罚款五千元的行政处罚。（来源：公安部网安局）

5. 公安部网安局公布安徽警方查处的四起网络安全行政执法案例

10月14日，公安部网安局公布安徽警方查处的四起网络安全行政执法案例。

案例一：安徽滁州全椒网安部门在办理涉嫌侵犯公民个人信息案中发现，安徽某置业公司员工刘某非法向他人泄露该公司收集的小区业主信息。经查，该公司未履行网络安全保护、个人信息保护、数据安全保护义务。全椒县公安局根据《网络安全法》第六十四条第一款，《行政处罚法》第三十三条第一款、第三款之规定，对该公司予以警告，并处罚金，责令改正。另根据《数据安全法》第四十五条之规定，对该公司予以警告，并责令改正。

案例二：安徽滁州天长网安部门接到线索：有人利用手机卡开卡环节恶意注册、出售网络账号。经查，杨某在为他人办理业务过程中，利用在

移动营业厅的工作便利，用客户手机号码注册网上购物平台账户，将客户手机号、验证码发送给犯罪嫌疑人，非法牟利。天长市公安局根据《网络安全法》第五十九条第一款、第六十四条第二款之规定，对该中国移动该营业点予以警告并责令整改、没收违法所得并处罚金的处罚。

案例三：安徽滁州全椒县公安局网安大队依法对全椒县电竞酒店开展联合检查时发现，全椒一电竞酒店存在用户隐私数据泄露风险。经调查核实，该酒店未履行网络安全保护义务、未采取互联网安全保护技术措施。全椒县公安局根据《网络安全法》第五十九条之规定，对该电竞酒店责令限期改正，处以警告的行政处罚。

案例四：安徽滁州来安网安部门安全监督检查中发现，某材料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，导致网站管理系统遭到攻击，被挂与该企业无关的不良内容。来安县公安局根据《网络安全法》第五十九条第一款之规定，对该单位予以警告并责令改正。同时，公安机关要求责任单位严格履行网络安全保护义务、落实网络安全主体责任，建立完善网络安全各项制度、措施。（来源：公安部网安局）

6. 因个人信息保护不当，宁夏六家物业公司被予以行政处罚

10 月 15 日消息，因个人信息保护不当，宁夏六家物业公司近日被处以警告处罚并责令其限期改正。

宁夏回族自治区石嘴山市公安机关开展个人信息保护专项检查行动，检查发现六家物业公司办公电脑存储大量小区业主家庭住址、身份证号码、

联系方式等个人信息，存储数据未经加密处理，办公电脑未设开机密码，对个人信息未实行分类管理、未采取加密及去标识化等技术措施，业主个人信息被泄露的风险极大。

针对上述企业存储公民个人信息和不履行网络安全义务的违法行为，石嘴山市公安机关依据《个人信息保护法》第五十一条、第六十六条之规定，对其予以警告处罚并责令其限期改正。（来源：公安部网安局）

7. 上海警方成功打掉一非法控制计算机信息系统犯罪团伙

10 月 7 日消息，上海警方近日成功打掉一非法控制计算机信息系统犯罪团伙，该团伙在国内 1.2 万余台电商电脑种植木马程序，受害商家涉及全国多地。

本案中，2023 年 6 月，上海市公安局闵行分局接到本市一家知名平台报案，称入驻平台的多家电商反映他们的客服电脑疑似“中毒”。民警立即开展调查，发现多家电商客服的电脑内都存在隐蔽且自动运行的木马程序，能够窃取电脑数据并自动发送诈骗信息。

经调查，公安机关锁定了以陆某某为首的犯罪团伙，团伙成员冒充客户使用话术，以购买商品、服务为名添加电商客服微信，然后以需要定制商品为由向客服发送带有木马病毒的文件，诱骗客服在电脑端下载浏览，从而植入木马程序，收集信息。

目前该团伙陆某某等 3 名犯罪嫌疑人因涉嫌非法控制计算机信息系统罪已被检察机关依法批准逮捕，徐某某等 27 名犯罪嫌疑人因涉嫌非法控制计算机信息系统罪已被依法采取刑事强制措施。（来源：公安部网安局）

8. 安徽、广东警方公布多起打击“网络水军”案例

10 月 8 日，公安部网安局公布五起安徽警方打击“网络水军”案例，分别是：（1）安徽合肥警方成功打掉非法开展点赞、评论、直播间投诉、举报等业务网络水军犯罪团伙；（2）安徽淮北警方成功打掉提供负面舆情处理、有偿删帖等业务网络水军犯罪团伙；（3）安徽蚌埠警方成功打掉删评控评等业务网络水军犯罪团伙；（4）安徽宿州警方成功打掉为多家平台商铺提供刷量、刷虚假好评等网络水军业务犯罪团伙；（5）安徽阜阳警方侦破制造虚假流量，帮助直播占榜等网络水军犯罪团伙。

16 日，公安部网安局公布四起广东警方打击“网络水军”案例，分别是：（1）广州侦破利用AI软件炮制涉某政府部门虚假信息引流案；（2）佛山打掉 4 个刷单控评犯罪团伙；（3）中山打掉刷量控评团伙；（4）阳江打掉为短视频刷量控评团伙。据统计，广东警方近期开展的打击网络水军第二波次集群收网行动一举打掉犯罪团伙 43 个，查扣手机等电子设备 1400 余台，涉案金额 2.3 亿元。（来源：公安部网安局）

9. 公安部网安局公布一起非法获取计算机信息系统数据案件

10 月 25 日，公安部网安局公布一起非法获取计算机信息系统数据案件。

本案中，郑某、吴某、李某和罗某利用非法购买的手机卡和“猫池”不断注册新账号，再批量转卖给他人谋利。掌握线索后，重庆市江北区公安分局先后抓获 4 名犯罪嫌疑人，并在现场查获猫池设备 4 组、台式电脑 3 台、笔记本电脑 1 台、手机 5 台、电话卡千余张，4 人通过虚拟货币与买家交易结算，共计获利 15 万元左右。

4名犯罪嫌疑人因涉嫌非法获取计算机信息系统数据罪被江北警方采取刑事强制措施。目前该案件仍在进一步侦办中。（来源：公安部网安局）

（二）网信部门治理实践

1. 网信部门依法查处一批涉公共政策、社会民生领域造谣传谣账号

10月24日，国家互联网信息办公室发布消息称，近期，一些网络账号编造传播涉公共政策、社会民生等领域谣言信息，严重误导群众认知，造成不良社会影响。网信部门指导网站平台强化监测查证、开展排查整治，溯源关闭谣言首发账号，累计处置违法违规账号1781个。

同步通报部分典型案例，分别是（1）“苏锡常将设立经济特区”谣言；（2）“广州地铁遭恐怖袭击”谣言；（3）“上海成功申办2036年夏季奥运会”谣言；（4）“国家自然科学基金委员会成立‘试点社区’”谣言；（5）“中石油官员称1升汽油等于800毫升”谣言；（6）“中国工程院将创办大学”谣言；（7）“护照号码EL开头为失信人员”谣言；（8）“国庆后老年人可半价购买火车票”谣言。（来源：中国网信网）

2. 网信部门依法查处“夸克”“网易CC”破坏网络生态违法案件

10月30日消息，针对“夸克”平台和“网易CC”直播平台破坏网络生态问题，国家网信办近日指导广东省网信办依法约谈相关平台负责人，对

“夸克”平台实施50万元罚款处罚，责令“网易CC”暂停“舞蹈”版块信息更新7日，同时责令2家平台立即全面深入整改，严肃处理相关责任人。

经查，“夸克”平台未遵守相关管理要求，搜索结果呈现大量淫秽色情信息，并向用户推荐色情低俗关键词，违反《网络安全法》《网络信息内容生态治理规定》《互联网信息搜索服务管理规定》等有关规定，在平台信息内容安全审核管理方面存在严重漏洞，破坏网络生态，情节特别严重。“网易CC”直播平台多个账号主播在直播过程中存在言行低俗、打色情擦边球等问题。“网易CC”直播平台未对上述低俗直播进行有效整治，并在首屏“娱乐”频道“舞蹈”版块等重点环节呈现，反映其在网络信息内容安全管理责任上存在严重缺失，违反《网络安全法》《网络信息内容生态治理规定》等有关规定，破坏网络生态，性质恶劣，情节严重。（来源：中国网信网）

3. 上海部署启动“清朗浦江·生活服务类平台信息内容整治”专项行动工作

10月13日，上海网信办部署启动为期2个月的“清朗浦江·生活服务类平台信息内容整治”专项行动。属地大众点评、世纪佳缘、2345导航、携程、拼多多、soul、途虎养车、蔚来、抖音电商、前程无忧等60多家重点生活服务类平台参会，覆盖团购评价、婚恋交友、搜索引擎、影视点评、天气日历、旅游出行、网络购物、地图导航、本地生活、运动健康、实用工具、汽车服务、网络招聘等领域。

此次专项重点聚焦为线下违法活动引流、搜索环节呈现违法信息、发布违规营销信息、组织操纵刷分控评、重点环节推荐低俗不良信息、传播网络迷信信息、散布炫富拜金、暴饮暴食等不良导向信息等七个方面突出问题，要求各网站平台压实主体责任，紧盯跟帖评论、信息流推荐、直播、短视频、榜单弹窗、高风险产品等重点环节，排查风险漏洞，补齐短板弱项，规范信息内容发布，健全内容审核机制。（来源：网信上海）

4. 因发生勒索事件未履行主动报告义务等行为，江西南昌网信办对某企业进行处罚

10 月 8 日消息，江西省南昌市网信办近日接上级网信部门通报，南昌市南昌县某企业存在数据漏洞风险，疑似出现删库勒索事件。

经过立案调查、远程勘验、现场勘验、笔录问询等工作，南昌市网信办查明：（1）该企业运营的mongodb数据库存在未授权访问安全漏洞；（2）该企业未采取相应的技术措施和其他必要措施保障数据安全，其运营的数据库被黑客删库并勒索；（3）该企业未加强风险监测，发生删库勒索事件时未采取处置措施和履行主动报告义务。上述行为违反《数据安全法》第二十七条、第二十九条的规定。

南昌市网信办依据《数据安全法》第四十五条的规定，对该企业作出警告并处罚款五万元、对直接负责的主管人员作出罚款一万元的行政处罚。（来源：网信南昌）

5. 因存在未授权访问漏洞，浙江省网信办对杭州某科技公司罚款五万元

10 月 10 日消息，根据国家网信办移交的问题线索，浙江省网信办近日依法对杭州某科技公司未履行数据安全保护义务的问题进行立案调查。

经查实，该公司旗下某生活类APP相关数据库服务端口直接暴露在互联网环境中，存在未授权访问漏洞，未按要求履行数据安全保护义务，违反《数据安全法》第二十七条之规定。

浙江省网信办依据《数据安全法》《行政处罚法》等法律法规，对杭州某科技公司罚款五万元，对该公司直接负责人罚款一万元。（来源：网信浙江）

6. 因数据被窃并传输到境外，上海市网信办对某科技公司罚款八万元

10 月 11 日消息，上海市某科技公司近日因相关数据库存在未授权访问漏洞，部分数据被窃并传输到境外。事发后该公司未及时有效整改并擅自将涉事数据库一删了之，上海市网信办依据《数据安全法》对该科技公司及公司直接责任人员予以行政处罚。

经调查核实，该科技公司主要从事为保险类企业提供互联网通信服务。2022 年 10 月，公司安装配置了一台Elasticsearch数据库服务器，用于搜集多个应用系统的业务日志，并存储了包含用户姓名、身份证号码、手机号在内的大量个人信息。该公司未建立健全全流程数据安全管理制度，未采取相应的技术措施和其他必要措施保障数据安全，因数据库存在未授权

访问漏洞，造成部分数据泄漏被传输到境外IP。同时企业私自删除涉事数据库逃避责任、没有按照规定及时向网信部门报告，未有效履行数据安全保护义务。

针对以上违法情况，上海市网信办依据《数据安全法》第二十七条、第四十五条，对该科技公司责令改正，给予警告，并处人民币八万元罚款，对公司直接责任人员作出罚款人民币一万元的行政处罚。（来源：网信上海）

7. 上海市网信办联合上海市公安局网安总队约谈新浪上海

10 月 12 日消息，上海市网信办会同市公安局网安总队约谈新浪上海，宣讲《网络安全法》《互联网新闻信息服务管理规定》《网络信息内容生态治理规定》等法律法规。

约谈指出，相关不实信息误导社会公众，诱发谣言滋生，造成严重不良影响。新浪上海要认真学习互联网法律法规，切实履行管理责任，完善内部管理制度，对开设的话题以及发布转载的信息真实性承担主体责任，不得通过虚假话题、“蹭热点”“标题党”等方式传播炒作不实信息。（来源：网信上海）

8. 重庆市武隆区网信办就网络安全问题依法约谈某公司负责人

10 月 20 日，在重庆市网信办指导下，重庆市武隆区网信办依法对属地某公司负责人进行约谈。

该公司在短期内连续发生两起网络安全事件。根据《网络安全法》等法律法规，武隆区网信办在约谈中向该公司剖析接连发生安全事件的根源，阐明了可能导致的不良影响和后果，要求该公司充分认识到做好网络安全工作的重要性，提升网络安全意识，并提出要严格落实网络安全法律法规，切实抓好自查，开展安全培训，加大安全投入等要求。（来源：网信重庆）

9. 因未履行数据安全保护义务，北京市网信办对三家企业进行处罚

10 月 30 日消息，根据国家网信办移交的问题线索，北京市网信办近日依据《数据安全法》对属地三家企业涉嫌存在网络数据安全违法行为进行立案调查并作出行政处罚。

经查实，三家企业违反《数据安全法》第二十七条规定，未履行数据安全保护义务，部署的ElasticSearch数据库存在未授权访问漏洞，造成部分数据泄露。北京市网信办依据《数据安全法》第四十五条第一款规定，对三家企业分别作出责令改正，给予警告，并处 5 万元罚款，对直接主管人员和其他责任人员处以 1 万元罚款的行政处罚。（来源：网信北京）

（三）通信管理部门治理实践

1. 工信部及多省通信管理局通报或下架侵害用户权益 APP/SDK

（1）工信部

10 月 24 日，工信部通报 2023 年第 6 批，总第 32 批侵害用户权益行为的APP（SDK）。

通报指出，工信部持续开展APP侵害用户权益专项整治行动，近期组织第三方检测机构对群众关注的在线影音、网上购物等移动互联网应用程序（APP）及第三方软件开发工具包（SDK）进行检查，发现 22 款APP、SDK存在侵害用户权益行为。相关APP及SDK所涉问题包括：违规收集个人信息，违规使用个人信息，超范围收集个人信息，APP强制、频繁、过度索取权限，欺骗、误导强迫用户，SDK公示信息不完整等。

相关APP及SDK应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）广东

10 月 19 日，广东省通信管理局发布通报，下架 12 款侵害用户权益的APP。通报指出，9 月 15 日，广东省通信管理局向社会公开通报了 25 款存在侵害用户权益和安全隐患问题的APP，截至通报规定时限，经核查复检，尚有 12 款APP未按照要求完成整改反馈。为严肃处理违规行为，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。

（3）广东

10 月 19 日，广东省通信管理局公开通报两款未按要求完成整改APP。通报指出，广东省通信管理局近期共监测发现 64 款APP存在侵害用户权益和安全隐患问题，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“倍电小秘”“千帆直播”两款APP未完成整改。广东省通信管理局要求被通报的APP在 10 月 26 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。

（4）重庆

10 月 23 日，重庆市通信管理局发布《关于下架侵害用户权益APP的通报（2023 年第 4 批）》。通报指出，重庆市通信管理局前期对存在侵害用户权益行为的APP进行公开通报。截至目前仍有六款APP未按要求完成整改。现对六款问题APP进行下架，相关应用商店和平台应立即组织对应用软件和小程序进行下架处理。

六款APP所涉问题包括未明示个人信息处理规则、违规收集个人信息、隐私政策中未对处理的个人信息保存期限加以说明，未在隐私政策等公示文本中逐一列明APP所集成第三方SDK收集使用个人信息的目的、方式和范围。

（5）北京

10 月 31 日，北京市通信管理局通报 2023 年第九期问题APP。通报指出，北京市通信管理局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。截至目前，尚有九款APP未整改或整改不到位，此次予以公开通报。

此外，北京市通信管理局10月7日通报本市部分存在侵害用户权益行为的APP并要求整改。截至目前，仍有七款APP未整改或整改不到位，此次予以全网下架处置。（来源：工信部、地方通信管理局）

2. 上海市通信管理局通报2023年9月通信网络安全防护管理情况

10月27日，上海市通信管理局发布《关于通信网络安全防护管理情况的通报（2023年9月）》。

通报指出，前期，上海市通信管理局公开通报了15家存在未落实通信网络安全防护管理要求等违规行为的单位，并责令其限期整改。经复测核查，尚有5家单位未按照要求落实整改。依据《网络安全法》《公共互联网网络安全威胁监测与处置办法》等法律法规要求，上海市通信管理局对上述5家单位的相关通信网络系统采取停止互联网服务等措施。

同时，上海市通信管理局检查发现48家单位的53个定级系统存在未按期落实通信网络安全防护管理整改要求等问题。上述单位应当在2023年12月24日前（本通报发布之日起60日内）落实整改工作。逾期落实整改的，上海市通信管理局将依法依规组织开展处置和执法工作。（来源：上海通信圈）

（四）其他部门治理实践

1. 国家数据局正式揭牌

10 月 25 日，国家数据局在北京正式挂牌，中共中央政治局常委、国务院副总理丁薛祥出席仪式并揭牌。

丁薛祥强调，组建国家数据局是以习近平同志为核心的党中央从全局和战略高度作出的重大决策。要以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党中央和国务院关于数据工作的决策部署，统筹推进数字中国、数字经济、数字社会规划和建设，协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，全面赋能经济社会发展。要统筹发展和安全，充分发挥数据的基础资源作用和创新引擎作用，不断做强做优做大数字经济，促进数字经济和实体经济深度融合，为构建新发展格局、建设现代化经济体系、构筑国家竞争新优势提供有力支撑。

根据《党和国家机构改革方案》，国家数据局负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。（来源：中国政府网）

2. 因未严格落实消费者金融信息使用管理制度导致客户信息泄露，两金融机构被处罚

10 月 10 日，中国人民银行公布一起金融机构未严格落实消费者金融信息使用管理制度导致客户信息泄露案例。

2022年，人民银行发现A银行B分行和C银行D信用卡分中心存在个别员工涉嫌非法贩卖金融消费者账户信息的情形后，迅速对涉事银行启动立案调查。调查发现，A银行B分行和C银行D信用卡分中心未严格有效落实消费者金融信息保护相关法律法规和内控制度，业务系统权限设置不合理，导致涉案员工得以利用职务便利，在未经授权审批且没有合法、正当事由的情况下，通过银行主要业务系统私自查询、记录客户个人信息，并将相关信息对外贩卖。同时，涉事银行日常消费者金融信息保护排查、风险监测、教育培训工作不到位，在发生上述重大事件时亦未及时向当地金融监管部门报告。

人民银行相关分支机构依法对A银行B分行和C银行D信用卡分中心给予警告并处以罚款，对其中负有直接责任的管理人员给予个人处罚，责令相关银行积极落实整改并进行全面自查。（来源：国家金融监督管理总局）

3. 江苏省检察院发布一起针对网络游戏平台防沉迷系统的侵犯公民个人信息犯罪案件

10月17日，江苏省检察院发布一起针对网络游戏平台防沉迷系统的侵犯公民个人信息犯罪案件。

本案中，被告杨某某非法购买包括人脸头像在内的成套个人信息累计1.9万余条，而后根据各大游戏平台对人脸信息的认证要求，对静态照片进行不同程度的加工处理，帮助用户完成人脸识别认证，绕过网络游戏平台防沉迷系统监管。检察官认为杨某某虽然从1.9万余条筛选出需要的几百条用于出租牟利，但客观上1.9万余条个人信息属于侵犯公民个人信息罪

中“其他手段非法获取”的行为，应当以购买的信息条数认定为侵犯公民个人信息的条数。

法院采纳六合区检察院对被告人杨某某所指控犯罪事实和定性，依法判处杨某某拘役三个月，缓刑四个月，罚金人民币三千元，违法所得予以追缴。（来源：江苏检察在线）

4. 江苏无锡江阴市检察院办理一起黄牛入侵交管 12123 系统案

10 月 20 日消息，江苏无锡江阴市检察院近日办理一起破坏计算机信息系统案。

本案中，主犯杨某婷通过网络与其他二手车“黄牛”勾结，通过上线张某，非法侵入交管 12123 信息系统，为无法正常过户的“二手车”办理车主信息变更、补办行驶证、补办车辆牌照等业务。杨某婷共计进行相关非法操作 300 多次，向 9 名下线二手车“黄牛”收取共计 118210 元“手续费”。

杨某婷等 10 名二手车“黄牛”，因犯破坏计算机信息系统罪被判刑，其中主犯杨某婷被判 3 年 6 个月，其他 9 人被判缓刑，上线张某的案件另案办理。（来源：光明网）

境外前沿观察：月度速览十则

导读：10 月，俄罗斯《联邦信息保护法》修正案生效，对网站运营商和移动应用程序所有者规范使用算法技术提出要求。阿根廷发布新版《国家网络安全战略》，旨在加强国家关键基础设施安全保护、网络安全监管以及国际合作。英国《在线安全法》正式成为法律，采取零容忍态度进行儿童保护，规范社交媒体平台行为，为互联网用户提供保护措施。

美国发布《十大网络安全错误配置》，介绍大型组织中最常见的网络安全错误配置及处置建议。17 个网络安全机构联合发布《改变网络安全风险的平衡：软件安全设计原则和方法指南》，提出软件制造商应采取的四项安全防御措施。美国谷歌、亚马逊和 Cloudflare 公司共同抵御迄今为止互联网最大规模 DDoS 攻击，此次攻击每秒生成超过 3.98 亿个请求，规模为以往记录的 7 倍以上。

关键词：算法使用、在线安全、人工智能、网络安全错误配置、DDoS 攻击

1. 俄罗斯《联邦信息保护法》修正案生效

10 月 1 日，俄罗斯《联邦信息保护法》修正案生效。修正案要求，在使用算法技术向用户提供信息时，网站运营商和移动应用程序所有者应：（1）遵守法律与公民权益。尊重公民、组织的权利与合法利益以及俄罗斯联邦法律法规；（2）遵守以俄语发布的全流程规则。对这些规则的访问不应受用户注册或用户身份的限制，也不应以支付费用为条件；（3）保障网络用户的知情权。监督局建议在网站或移动应用程序上发布使用的算法技术相关信息。（来源：俄罗斯联邦通信、信息技术和大众媒体监督局）

2. 阿根廷发布新版《国家网络安全战略》

10 月 3 日，阿根廷发布新版《国家网络安全战略》。战略提出：（1）强化网络安全制度体系建设，完善网络安全法律法规；（2）加强国家关键基础设施安全保护，加强各主体信息交流与合作；（3）推进公共部门信息系统保护与恢复，确保国家信息与公民个人信息安全；（4）提升网络安全风险预防、检测和应对能力，有效打击网络犯罪；（5）强化网络安全意识、培训、教育和宣传，培育网络安全人才；（6）制定网络安全监管框架，确定网络安全评估标准；（7）加强网络安全国际合作，促进数字治理包容性与可持续性。（来源：阿根廷政府官网）

3. 美国 CISA 与 NSA 联合发布《十大网络安全错误配置》

10 月 5 日，美国网络安全和基础设施安全局(CISA)、国家安全局(NSA)联合发布《十大网络安全错误配置》，重点介绍大型组织中最常见的网络安全错误配置。十大最常见的网络安全错误配置包括：（1）未设置软件的默认配置；（2）网络用户与管理员权限分配不当；（3）内网监控不足；（4）缺乏网络分段；（5）补丁管理不足；（6）规避系统访问控制措施；（7）多因素身份验证配置错误；（8）网络共享和服务的访问控制列表不足；（9）网络凭证管理状况不佳；（10）代码执行设立限制。这些错误配置说明许多大型组织存在系统性安全漏洞，软件制造商应采用安全设计减轻网络防御者的负担。

文件鼓励网络防御者实施以下措施，降低恶意行为者利用已识别错误配置的风险，包括：（1）删除默认凭据并强化配置；（2）禁用未使用的服务并实施访问控制；（3）定期更新并自动修补、优先修补已知被利用的漏洞；（4）减少、限制、审核和监视管理账户和权限。（来源：美国网络安全和基础设施安全局官网）

4. 英国《在线安全法》正式成为法律

10 月 26 日，英国《在线安全法》正式成为法律。该法采取零容忍态度进行儿童保护，规定社交媒体平台应当：（1）快速删除非法内容或防范非法内容出现；（2）防止儿童访问有害和不适合年龄的内容；（3）实施年龄限制并采取年龄检查措施；（4）确保社交媒体平台对其受众儿童所构成

的风险更加透明；（5）为家长和孩子提供清晰易懂的方式以便在线反馈。同时，该法为互联网用户提供三层保护措施：包括：（1）确保互联网平台删除非法内容；（2）基于条款规定，社交媒体平台在用户注册时应向用户做出保护承诺；（3）为用户提供过滤掉其不想看到的内容的选项。（来源：英国政府官网）

5. 美国总统签署《关于安全、稳定和可信的人工智能行政令》

10 月 30 日，美国总统拜登签署《关于安全、稳定和可信的人工智能行政令》。行政令为人工智能安全和保障构建新标准，并在保护美国用户隐私、促进公平和公民权利、维护消费者和工人权益、促进创新竞争等方面做出规定。

行政令主要内容如下：（1）要求人工智能系统领域的龙头开发者与美国政府共享其安全测试结果和其他关键信息。要求正在开发对国家安全领域构成严重风险的基础模型公司，在训练模型时应通知联邦政府，并分享所有红队安全测试结果；（2）制定标准、工具和测试以帮助确保人工智能系统的安全性、保密性和可信任性。NIST 将制定严格标准，进行大量红队测试以确保在系统公开发布前的安全性。同时成立人工智能安全和保密委员会。能源部和国土安全部应处理人工智能系统对关键基础设施以及化学、生物、核能、网络安全等领域的风险威胁。（来源：美国白宫）

6. 以色列总统的 Telegram 账户遭到犯罪团伙入侵

10 月 5 日消息，以色列总统艾萨克•赫尔佐格的 Telegram 账户被黑客入侵。总统官邸表示，虽然没有确认谁访问该账户，但此次黑客攻击本质上是犯罪行为，与网络诈骗有关。初步调查显示，此次攻击并未发现任何数据被盗，且此次攻击可能为敌对国家或组织所为。目前违规行为已经关闭，账户已经恢复正常运营。但总统官邸及相关报道暂未提供有关在线诈骗以及如何导致账户被盗的详细信息，以色列内部安全部门辛贝特对此事件正展开进一步调查。（来源：The Times of Israel 网站）

7. 美国科技公司报告史上最大 DDoS 攻击

10 月 12 日消息，美国谷歌、亚马逊和 Cloudflare 公司近日共同抵御了迄今为止互联网最大规模的分布式拒绝服务（DDoS）攻击。谷歌表示，此次攻击每秒生成超过 3.98 亿个请求，规模为以往记录的 7 倍以上。一次仅两分钟的此类攻击便超过 2023 年 9 月维基百科的文章浏览量。此次攻击开始于 8 月下旬，由 HTTP/2（支撑万维网 HTTP 网络协议的较新版本）的漏洞导致，该漏洞使服务器特别容易受到恶意请求影响，因此各公司应立即要求提供关键互联网交付服务的组织采取补丁和其他缓解措施。（来源：usnews）

8. 全球网络安全机构联合发布《改变网络安全风险的平衡：软件安全设计原则和方法指南》

10 月 16 日，美国网络安全和基础设施安全局、加拿大网络安全中心等 17 个网络安全机构联合发布《改变网络安全风险的平衡：软件安全设计原则和方法指南》。指南建议软件制造商应：（1）采用安全信息技术开发和深度防御措施，防止恶意行为者破坏系统或未经授权访问敏感数据；（2）制定书面路线图，使其现有产品组合在安全能力方面有较大提升；（3）优先考虑产品安全性，保障产品功能安全运行，减小被攻击可能性；（4）对产品和平台采取整体安全战略，在产品开发设计的过程中进行战略投资。（来源：美国网络安全和基础设施安全局官网）

9. 卡巴斯基实验室发布高级持续性威胁研究报告，披露恶意软件 MATA

10 月 18 日，卡巴斯基实验室发布名为《更新的 MATA 攻击东欧工业公司》的报告，发现属于 MATA 集群的多个恶意软件样本，旨在窃取东欧国防工业和石油天然气行业数十个组织的数据。攻击者对 MATA 软件进行更新，新一代软件具有模块化结构，并能为攻击者提供服务器的连接协议，支持灵活的代理服务器链。攻击者向受害者发布鱼叉式网络钓鱼邮件，并在受害者点击链接并下载文件后施行感染，最终利用 Internet Explorer 中的 CVE-2021-26411 启动感染链。此外，攻击者使用多种技术来隐藏其活动，主要包括：将文件伪装成合法应用程序、使用应用程序之间的通信开放端

口、对文件和恶意软件的网络活动进行多级加密、在控制服务器的连接之间设置较长的等待时间等。（来源：Securelist 网站）

10. 美国人脸识别公司 Clearview AI 在英上诉成功，或免罚 750 万镑

10 月 19 日消息，美国人脸识别公司 Clearview AI 在英国赢得上诉，推翻英国 ICO 此前针对其发起的指控。Clearview AI 或因此免于支付 750 万英镑的罚款。

2022 年 7 月，ICO 宣布，Clearview AI 在未经用户同意的情况下非法收集和使用英国公民照片，未规定图像数据存储期限，还建立了超 200 亿张照片的数据库用于提供面部识别服务，向美国执法部门和国家安全机关出售身份匹配服务等,违反英国《2018 年数据保护法》。ICO 决定对 Clearview AI 处以 750 万英镑的罚款，要求删除其持有的英国公民图像数据。之后，Clearview AI 提起上诉。

针对此次上诉，法院认定 Clearview AI 的系统仅由英国以外的执法机构使用，而外国执法行为超出英国数据保护法管辖范围，ICO 对外国执法机构如何使用英国公民的数据没有管辖权，无法对其采取执法行动或处以罚款。目前 ICO 尚未确认是否会上诉，他们将在 28 天的时间内作出决定。（来源：隐私护卫队）

行业前沿观察一：2023 网络诚信建设专题

样本采集工作收官

导读：2023 网民网络安全感满意度调查活动第二阶段“网络诚信建设”专题样本采集工作于 11 日 7 日 24 时圆满收官，调查范围覆盖全国，数百支志愿队伍和十数万网民参加活动，是一次网络安全知识和网络诚信建设理念的普及和推广，对我国网络安全和网络诚信建设起到积极推进作用。

关键词：网络诚信建设专题，样本采集

1.2023 网络诚信建设专题样本采集收官

2023 网民网络安全感满意度调查活动第二阶段“网络诚信建设”专题样本采集工作于 11 日 7 日 24 时圆满收官，取得全国网民参与答题样本总量 191721 份的佳绩。调查范围覆盖全国，数百支志愿队伍和十数万网民参加活动，是一次网络安全知识和网络诚信建设理念的普及和推广，对我国网络安全和网络诚信建设起到积极推进作用。

支撑我国首个网络诚信发展年度报告

2022 年 8 月 29 日，在 2022 年中国网络文明大会网络诚信建设高峰论坛上首次发布了我国网络诚信发展年度报告——《中国网络诚信发展报告 2022》（以下简称《报告》）。

《报告》由中国网络社会组织联合会牵头编撰，全面反映 2021 年以来我国网络诚信建设取得的新进展新成就。支撑《报告》的大量数据，来自 2022 网民网络安全感满意度调查活动“网络诚信建设”专题。

《报告》从总体概况、履责情况、问题挑战、思考建议 4 个部分阐述年度网络诚信建设情况。《报告》显示，我国网络诚信建设呈现五大特点：规范力度明显加大、诚信机制加快健全、宣传教育深入人心、社会实践丰富多彩、失信惩戒成效明显，我国网络诚信建设整体状况持续向好。

专题调查活动继续弘扬志愿服务精神

“网络诚信建设”专题问卷调查是2023网民网络安全感满意度调查活动的重要组成部分。10月19日至11月7日，调查活动组委会再度携手网安联成员单位、调查活动发起单位及全国志愿服务站（队），开展“网络诚信建设”专题问卷调查，面向网民征集我国网络诚信建设意见建议，相关数据将用于编撰《中国网络诚信发展报告2024》（此报告将在“2024中国网络文明大会”上发布），为推进高质量网络诚信建设提供支撑。

本次专题调查活动范围覆盖全国全国31个省（自治区、直辖市）和新疆生产建设兵团、港澳台地区，数百支志愿服务团队参加，再次集中展现了志愿服务的力量，弘扬志愿服务精神。

调查报告发布值得期待

据组委会透露，本届专题调查活动结束后，下一阶段将进入紧张的调查数据整理分析和报告编撰阶段。最终依据专题调查活动数据生成的诚信建设报告，将在2023“安满周”期间正式发布。相关数据还将支撑《中国网络诚信发展报告2024》的编撰，助力推进我国高质量网络诚信建设。

另据组委会透露，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，“安满周”自2021年开始，今年已连续成功举办两届，已经成为业内颇具影响力的盛事。

2022年“安满周”全程共七天，分为“总报告发布”、“网安共建”、“网民满意”三个版块。“总报告发布”版块除全国总报告发布外，还包

括报告重要议题研讨、行业之声、圆桌会议，“网安共建”版块分为网安法治日、企业合规日、科技服务日、安全守护日四个主题日，“网民满意”版块分为网民权益日、网络文明日两个主题日。同期还召开了网安联调查数据应用研讨会、2022 网络志愿服务大会、2022 网络安全高峰论坛三场重要会议。除发布全国总报告外，还重磅发布了 12 个专题报告，175 个区域报告。

组委会表示，2023“安满周”体现“创新”的特点，正在紧张筹划过程中。本届“安满周”将以总报告发布会、12 个专题报告发布会、高端论坛、行业报告、区域报告集中发布，现场并穿插展览展示相关专题、机构和院校的科研成果和产品，以及普法宣传等科普知识，结合云上会场和展览，与全国各区域城市同频同步发布和展览，通过权威媒体、行业媒体和网络自媒体，传播今年网民对网络的安全感和满意度指数。

组委会秉承开放共享的精神，面向社会公开征集合作伙伴，关注网络空间安全的政府机构、研究机构、企事业单位，均有机会参与“安满周”活动（热线咨询电话：020—83713466） 。

在相关党政部门指导支持，国内一流科研院所，以及近百位专家学者的共同支持参与下，“安满周”成为具有网络安全行业生态影响力的创新平台，为提升广大网民安全感满意度，共绘国家网络安全同心圆贡献应有的力量。（来源：网安联）

行业前沿观察二：AI 安全治理

导读：人工智能（AI）技术发展迅猛，安全问题浮上水面，成为各界关注的热点话题。有观点认为，前沿 AI 是目前用于 ChatGPT 等生成式模型中的最复杂的技术形式，这些 AI 模型最重要的能力可能会造成严重甚至灾难性的伤害，无论是有意的还是无意的。

中国向世界发声：愿与各方一道就人工智能安全治理加强沟通交流，为推动形成普遍参与的国际机制和具有广泛共识的治理框架积极贡献智慧，切实落实全球发展倡议、全球安全倡议和全球文明倡议，促进人工智能技术更好造福于人类，共同构建人类命运共同体。

关键词：人工智能（AI），安全治理，人类命运共同体

1.中国发出全球人工智能治理最强音

在第三届“一带一路”国际合作高峰论坛上，习近平总书记宣布中方提出全球人工智能治理倡议，发出了引领全球人工智能治理的中国强音。

加强全球人工智能治理重要且紧迫

作为最具颠覆性的新兴技术之一，人工智能会不会打开“潘多拉魔盒”？ 会不会加剧“发展鸿沟”？人工智能军事应用应如何更好地规范？当前，国际社会迫切需要加强人工智能治理，推动人工智能朝着科技向善的方向发展。

中国工程院院士，ISC 名誉主席邬贺铨认为，人工智能等数字技术的应用本身既是安全防御的重点手段，也是安全保障的有力手段，需要将大数据、人工智能、互联网等技术融合，提升保障能力。数字安全需要从产业、技术、管理等多个维度提供保障的同时，也需要人才、法规的支撑。

中国工程院院士邬江兴指出，人工智能是引领新一轮产业变革的核心技术引擎，为各领域提供信息化、数字化、智能化的解决方案，正在引发经济结构重大变革，推动社会生产力的整体跃升。

面对生成式人工智能发展亟待解决的问题，中央网信办网络安全协调局副局长罗锋盈表示，要提升新技术新应用安全风险防范能力，如何将海量数据转换为真正能为大模型训练所用的数据是重点。此外，要善于把数据资源转换为数据优势，构建网络安全教育技术产业融合发展的良性生态。

网民网络安全感满意度调查组委会主任，公安部原一所、三所所长，中国计算机学会计算机安全专委会荣誉主任、研究员，本刊顾问专家严明认为，保证人工智能安全是一项复杂而设计面宽广的系统工程，迫切需要科技、法规、文化、社会等各个领域密切协同。

中国互联网协会研究中心副主任吴沈括表示，人工智能本身它的发展不单单是一个技术问题，它会深度改变我们的生活、生产方式以及未来发展的图景，包括我们的技术基础，经济发展的模式，乃至国家治理和国际关系。但需要注意的是，一方面部分国家和地区面对人工智能的快速发展，存在认知、能力以及治理的不足。另一方面部分国家利用技术优势推行技术霸凌、技术霸权，这种行径严重损害了其他国家和人民的发展利益。

人工智能安全治理中国路径和中国方案

中方正是在此背景下，提出全球人工智能治理倡议，围绕人工智能的发展、安全和治理三方面系统清晰阐述了中国路径和中国方案。

倡议强调面向他国提供人工智能产品和服务时，应尊重他国主权，严格遵守他国法律，接受他国法律管辖；发展人工智能应坚持“智能向善”的宗旨，各国尤其是大国对在军事领域研发和使用人工智能技术应该采取慎重负责的态度；发展人工智能应坚持相互尊重、平等互利的原则，反对利用技术垄断和单边强制措施制造发展壁垒，恶意阻断全球人工智能供应链等。

外交部军控司司长孙晓波指出，倡议坚持发展与安全并重的系统思维，反对以意识形态划线或构建排他性集团，恶意阻挠他国人工智能发展，引导人工智能朝着有利于人类文明进步的方向发展。倡议强调安全可控、隐私保护、公平和非歧视，集中反映了各方对人工智能安全的主要关切，也为相关国际讨论和规则制定提供了蓝本，反映出我们在人工智能领域成熟的治理经验。在当前全球人工智能治理的重要十字路口，倡议的提出将有力推动各方通过对话合作、凝聚共识，共同构建开放、公正、有效的治理机制。

相比一些国家构筑“小院高墙” 中方努力弥合“智能鸿沟”

倡议特别呼吁要增加发展中国家的代表性和发言权，开展面向发展中国家的国际合作与援助。这其实是对目前“智能鸿沟”不断扩大的一个回应，跟一些国家主张的“小院高墙”做法形成了鲜明对比。努力弥合“智能鸿沟”，并确保“智能红利”惠及各国，这是中方在人工智能治理问题上的立场，也是国际社会在制定相应标准规范时不容忽视的重要考量。

日前，联合国宣布成立“人工智能高级别咨询机构”，两名中国学者入选机构成员。对此，孙晓波表示，作为负责任的人工智能大国，中方支持在联合国框架下讨论人工智能治理，推动形成具有广泛共识的治理框架和标准规范。（来源：综合人民网、《经济参考报》等）

2. “AI 安全治理，不能没有中国”

当地时间 11 月 2 日，首届全球人工智能(AI)安全峰会落下帷幕。此次峰会由英国主办，于当地时间 1—2 日在英国布莱奇利园召开。全球政府官员和科技公司高管等近百名代表出席，就 AI 技术快速发展带来的风险与机遇展开讨论。中国代表团应英国政府邀请与会，受到高度重视和热烈欢迎。

世界关注 AI 安全

当地时间 11 月 2 日，首届全球人工智能(AI)安全峰会落下帷幕。此次峰会由英国主办，于当地时间 1—2 日在英国布莱奇利园召开。全球政府官员和科技公司高管等近百名代表出席，就 AI 技术快速发展带来的风险与机遇展开讨论。

英国《金融时报》旗下 Sifted 媒体网站报道称，这次峰会成功地将中美欧高级官员“聚集在同一张桌子上”，并得到了埃隆·马斯克等科技高管的参与支持。

首个全球性 AI 声明签署

在开幕式上，包括中国、美国、英国在内的 28 个国家及欧盟共同签署了《布莱奇利宣言》(以下简称《宣言》)，承诺以安全、以人为本、值得信赖和负责任的方式设计、开发、部署和使用 AI。

英国政府称，该协议旨在确定“共同关注的 AI 安全风险”，并制定“各国各自基于风险的政策”。

《宣言》警告说，前沿AI是目前用于ChatGPT等生成式模型中的最复杂的技术形式，这些AI模型最重要的能力可能会造成严重甚至灾难性的伤害，无论是有意的还是无意的。

英国科学、创新和技术大臣米歇尔·唐兰表示，该宣言的签署是一项“里程碑式的成就”，并且为峰会的讨论奠定了基础。

然而，有专家认为该宣言还不够深入。欧洲新闻电视台网站报道称，AI研究公司AMPLYFI首席执行官保罗·提瑟表示，将主要大国聚集在一起是一次成功，但必须迅速制定具体政策和问责机制。“模糊的术语给误解留下了空间”。

各国争相在监管方面有所作为

峰会上，各国阐述了各自在AI监管领域的具体进展。

英国称，并不急于通过新的AI法律来对本国AI进行监管，而是建议让AI技术公司更好地发现问题，并与立法机构分享他们的发现。

法国负责数字问题的副部长让·诺埃尔·巴罗特则表示，法国政府正在争取开源AI发展。开源是指模型开发者让公众开发、修改和迭代他们的模型。

巴罗特表示，我们不应该预先放弃开源，在前几代技术中可以看到，开源对于这些技术的透明度和治理都非常有用。它帮助确保竞争公平，并防止某些领域出现不利于创新的垄断。

美国商务部长吉娜·雷蒙多 1 日表示，美国将成立人工智能安全研究所，评估前沿 AI 模型已知和新出现的风险。

中方愿积极贡献智慧

中国代表团此次应英国政府邀请与会。中方代表表示，AI 治理攸关全人类命运，是世界各国面临的共同课题。

中方认为，在世界和平与发展面临多元挑战的背景下，各国应秉持共同、综合、合作、可持续的安全观，坚持发展和安全并重的原则，通过对话与合作凝聚共识，构建开放、公正、有效的治理机制，共同促进全球人工智能健康有序安全发展。

中方表示，愿与各方一道就人工智能安全治理加强沟通交流，为推动形成普遍参与的国际机制和具有广泛共识的治理框架积极贡献智慧，切实落实全球发展倡议、全球安全倡议和全球文明倡议，促进人工智能技术更好造福于人类，共同构建人类命运共同体。

美国消费者新闻与商业频道 2 日援引唐兰的话称，中国政府派官员出席本届 AI 安全峰会是一个非常重要的表态。

美国《财富》杂志 3 日报道称，会议结束后，英国首相里希·苏纳克与马斯克就 AI 展开了一场对话,并在马斯克旗下社交平台 X 上进行了直播。马斯克称赞苏纳克邀请中国参加峰会的决定“非常好”，并表示“应该感谢中国的出席”。

还有部分国家政府官员认为，中国参与此次峰会具有建设性意义。世界上一些最大的AI行业参与者都是中国公司，因此，有关AI安全性和透明度的高级别讨论，不能少了中国政府的参与。

Sifted网站援引欧盟委员会副主席维拉·朱罗瓦的话称，“他们(中国的AI企业)太庞大了，不容忽视”“我认为，他们(中方)在这里很重要。说实话，对于防范真正巨大的全球灾难性风险，我们需要中国的参与”。（来源：人民网）

3.世界互联网大会乌镇峰会与会人士聚焦人工智能治理

2023年世界互联网大会乌镇峰会期间，与会专家学者、企业代表等围绕人工智能发展与治理进行了交流探讨。

阿拉伯信息通信技术组织秘书长穆罕默德·本·阿莫认为，在这个飞速发展的世界，人工智能不仅是技术的进步，也是真正的变革，正在重塑人们生活、工作和交流的方式。

从线上到线下、从制造业到服务业，人工智能赋能千行百业，为经济社会高质量发展提供新动能。

与会人士认为，当前，人工智能已经成为全球治理的一个重要领域，需要各国携手共同应对其带来的风险。

“我想要强调人工智能领域全球合作的重要性。”穆罕默德·本·阿莫认为，未来，人工智能的发展应建立在良好合作之上。

今年10月，中国提出《全球人工智能治理倡议》，围绕人工智能发展、安全、治理三方面系统阐述了人工智能治理中国方案。

北京师范大学法学院博士生导师、中国互联网协会研究中心副主任吴沈括说，各方携手落实倡议，将有利于妥善应对科技发展带来的规则冲突、社会风险、伦理挑战。

世界互联网大会秘书长任贤良表示，国际社会应加强对话合作，不断弥合智能鸿沟和治理能力的差距，共同推动人工智能健康发展，促进人工智能技术造福于人类。（来源：新华网）

行业前沿观察三：数据安全

导读：10 月 25 日国家数据局在北京正式揭牌，成为数字中国建设进程中又一具有里程碑意义的事件。组建国家数据局，是以习近平同志为核心的党中央从全局和战略高度作出的重大决策。国家数据局正式运行，对于提高我国数字经济治理体系和治理能力现代化水平，统筹推进数字中国、数字经济、数字社会规划和建设，构建新发展格局、建设现代化经济体系、构筑国家竞争新优势，具有重大意义。

关键词：国家数据局，数据安全治理，数字经济

1. 国家数据挂牌亮相意义重大

2023 年 10 月 25 日，国家数据局正式挂牌。组建国家数据局，国家数据局的成立具有怎样的重要意义？又将给经济社会发展带来哪些新变化？

开启数字中国建设新局面

今年 3 月，中共中央、国务院印发的《党和国家机构改革方案》对外公布。根据方案，国家数据局负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。

中国工程院院士邬贺铨表示，数据与土地、资本、劳动力等传统生产要素不同，数据要素的开发与治理有很多需要深入研究的问题。根据党中央决策部署组建国家数据局，将有力促进数据要素技术创新、开发利用和有效治理，以数据强国支撑数字中国的建设。

2022 年底，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》发布，初步搭建了我国数据基础制度体系。成立国家数据局，有望推动数据基础制度建设进一步提速。

“数字经济时代面临数据确权、数据流通、数据安全等诸多新问题，这些问题归根结底源于体制机制的不完善、不合理，是典型的生产力与生产关系不匹配问题。”中国电子信息产业发展研究院院长张立认为，

在此背景下，国家数据局成立的首要任务即是建立数据基础制度，构建数字经济时代的规则体系，找到数据合规可信与数据价值实现之间的平衡点，有效破解激活数据新要素面临的一系列难题，从国家层面统筹协调数字中国、数字经济、数字社会的规划和建设。

夯实数字经济发展基础

“未来几十年，我们将经历一场由新一代信息技术驱动的深刻的经济社会变革，数字化转型已成为当今世界经济社会发展不可逆转之势。”中国科学院院士梅宏表示，为促进数字经济新形态的有序形成和健康发展，必须夯实数据要素市场、数字治理体系与数据技术体系“三大基石”。

首先，发展数字经济的关键是数据要素市场的培育与形成。梅宏表示，我国是首个将数据列为生产要素的国家，数据要素化尚处起步探索阶段，国际上亦无先例可循，数据要素化在资产地位、权属确权、流通交易、利益分配和安全隐私等方面还存在诸多障碍。其次，数字治理体系是数据要素市场健康有序及数字经济健康发展的保障，其中数据治理体系的建设是核心。再次，数据技术体系是数据要素化、数据治理和数字治理以及数字经济发展的技术支撑。“国家数据局挂牌成立，标志着我国数字经济发展新阶段的开始。期待在国家数据局的统筹规划与领导下，围绕‘三大基石’，夯实数字经济发展的基础，促进我国数字经济的有序健康和高水平发展。”梅宏说。

中国电子信息产业集团有限公司董事长曾毅认为，正式成立国家数据局，彰显了国家对数据的生产要素和资源属性的高度重视，有利于集中资源，破解目前数据流通利用中的难点，更好发挥数据要素在推动高质量发展、实现共同富裕中的基础性作用。

全面赋能经济社会发展

数据是数字经济发展的关键生产要素，是国家基础性战略性资源。我国数据资源富集，2022 年数据产量达 8.1ZB，位居全球第二位。

中国信息通信研究院院长余晓晖表示，数据具有乘数效应，能够创造规模经济和范围经济，提升配置效率和激励效率。当前，我国正处于数据资源迈向数据要素化配置阶段的重大变革期，应多措并举，推动构建“强资源、大市场、广应用、善治理”的数据要素发展新格局。一是布局数据基础设施，夯实底座；二是提升公共数据管理能力，引领发展；三是完善数据要素市场机制，补齐短板；四是规范数据要素市场主体，共建生态；五是构建数据要素治理体系，强化保障。

中国移动通信集团有限公司董事长杨杰认为，释放数据要素价值，是构筑数字经济竞争优势的必然选择。当前，数据正系统渗透至生产、生活、社会治理的各领域全环节，不断提升土地、劳动、资本等传统生产要素的配置效率，支撑社会资源的大规模整合、服务范围的高效拓展，实现供给和需求的更高水平动态平衡。要发挥我国海量数据资源的优势，切实用好数据，赋能新业态新模式创新。

“数据是21世纪全球经济发展的‘粮食’，谁掌握了数据，谁就拥有了世界，谁就掌握了未来。”北京交通大学信息管理理论与技术国际研究中心教授张向宏说，我们要统筹发展和安全、国内和国际，以数据为关键要素资源，以数据资源开发利用为主线，以数据基础设施为载体，不断做强做优做大我国数字经济，并全面赋能经济社会发展。（来源：经济日报）

2. 国家数据局局长刘烈宏：让数据安全“动”起来

11月10日国家数据局党组书记、局长刘烈宏在出席北京数据基础制度先行区启动活动上表示，国家数据局正在推进的重点工作之一，就是不断完善数据基础制度体系，充分发挥数据的基础资源作用和创新引擎作用，不断做强做优做大我国数字经济，为构建新发展格局、建设现代化经济体系、构筑国家竞争新优势提供有力支撑。

他提到，北京作为各类央企、国企和民营企业的总部聚集地，汇聚了国内优质的人才、技术、企业等资源，在数据资源类型、层级、规模方面具有得天独厚的优势。一直以来，北京市高度重视数字经济发展，正加快建设全球数字经济标杆城市，此次启动数据基础制度先行区建设，进一步体现了北京市委市政府对释放数据要素价值，培育数字经济的高度重视。希望北京市进一步发挥已有优势，在数据“三权”分置制度落地、数据流通交易、数据基础设施建设等领域持续探索、先行先试。

第一是探索数据“三权”分置落地，让数据放心“供”出来。数据资源持有权、数据加工使用权、数据产品经营权等分置机制是加快数据要素流通、释放数据要素价值的重要制度基础，需要进一步通过落地实践探索完善，希望北京市充分发挥数据要素基础制度先行区优势，探索界定数据来源、持有、加工等过程各参与方享有的合法权利，推进健全数据要素各参与方合法权益保护制度，助力中国特色数据产权制度体系实践落地。

第二是培育多层次数据流通交易体系，让更多数据“活”起来。数据流通交易体系是持续释放数据要素价值动力源，只有不断提高数据的价值创造能力才能激发更多主体积极性。国家数据局正研究起草相关指导文件，从顶层设计推动数据交易流通体系建设，希望北京市立足大数据交易所已有基础，探索完善公共数据、行业数据等的确权估值、登记结算、合规咨询等服务，培育发展数据生产、流通、应用等环节企业，构建数据交易流通生态体系。

第三是推动数据基础设施建设，让数据安全“动”起来。数据基础设施是让数据“供得出、流得动、用得好”的关键载体，让数据安全可信流通才能实现数据的高效利用。国家数据局正积极关注数据流通相关技术演进，希望北京市充分发挥人才、技术等优势，积极推进隐私计算、数据空间、区块链等数据流通技术研发和集成应用，布局建设数据基础设施，为数据可信、高效流通提供有力的基础支撑。

刘烈宏指出，当前数据基础制度建设正逐步完善，数据要素产业发展持续加速。国家数据局将持续关注北京市数据要素产业发展，支持先行区在数据要素相关领域积极探索，也期待北京市在数据要素领域取得新的成绩。（来源：新京报）

3. 数据安全进入资产安全阶段

以数据成为新型生产要素为标志，数据安全发展进入资产安全阶段。

数据本身安全阶段：以电子政务、电子商务、电子社区等业务应用的信息化发展为标志，承载业务信息的数据越来越多，数据本身的安全也成为信息安全关注的重点。数据本身安全阶段主要关注承载业务信息的数据本身安全，主要保障数据在传输、存储过程中的安全。保障对象主要为电子文档、数据库等数据。

数据资源安全阶段：以云计算和大数据等技术的发展为标志。如今，数据呈现大量汇聚、共享趋势，数据要素也从无序、散乱的非结构化数据转变为可分析、利用的结构化、半结构化的有序数据，逐渐实现数据的资源化。数据资源安全阶段主要关注数据资源的安全治理方面，需要保障大量数据汇聚、数据共享利用等场景中数据资源采集、传输、存储、共享、使用、销毁全生命周期安全，保障对象也由电子文件、数据库等传

统数据发展到具有数据量大（Volume）、数据种类多（Variety）、数据价值密度低（Value）、数据产生和处理速度快（Velocity）特征的大数据方面 。

数据资产安全阶段：以数据成为新型生产要素为标志。由中共中央、国务院对外发布的《关于构建数据基础制度更好发挥数据要素作用的意见》等政策，从国家层面为数据产权、流通交易、收益分配、安全治理等方面构建了数据基础制度，提出政策举措。数据要素的运营、交易需求愈发迫切。数据也完成由数据资源到数据资产的转变，数据安全目标开始聚焦到数据资产安全方面。数据资产安全阶段主要关注数据资产化后数据要素的开发利用、运营交易的安全性。保障对象主要为数据要素运营的物理网络设施、存储计算设施和数据应用设施等数据基础设施。

（来源：《信息安全与通信保密》杂志）

行业前沿观察四：各地协会动态

导读：安徽省网络安全协会成功换届，南宁协会将承办网安发展论坛，佛山协会职工技能大赛，清远协会网聚正能量，徐州协会赴苏州参加电子信息博览会等系列活动……各地协会积极开展活动，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：各地协会，动态

1. 安徽省网络安全协会成功举办第三次会员大会暨换届选举大会

11 月 5 日，安徽省网络安全协会成功举办第三次会员大会暨换届选举大会。

会议宣读了业务主管单位批准换届选举的文件，并审议通过了上届理事会的工作报告和财务收支审计情况报告。大会决定协会名称更改为“安徽省网络安全协会”，以更好地反映其宗旨和职责。大会同时还听取和审议了协会章程的修订说明、换届选举工作情况报告、理事选举办法等议题，并顺利选举产生了新一届理事会。随后召开的新一届理事会第一次会议选举产生了协会新一届领导机构，中国科学技术大学信息与智能学部副部长兼网络空间安全学院执行院长俞能海教授当选为协会会长。

安徽省民政厅社会组织管理局唐麟处长代表社会团体登记管理机关、安徽省公安厅网安总队李晓留总队长代表业务主管部门对新一届协会工作提出了要求和希望。（来源：安徽省网络安全协会）

2. 南宁市信息网络安全协会成功承办 2023（第二届）网络空间安全合作与发展论坛

为推动中国-东盟网络空间安全学术交流、人才培养以及产学研合作，南宁市信息网络安全协会继 2016 年成功举办“第一届中国-东盟网络空间安全高峰论坛”后，于今年延续举办第二届，并更名为“网络空间安全合作与发展论坛”。

据悉，该论坛由中国兵工学会的指导，中国兵工学会信息安全与对抗专业委员会、广西工业互联网产业协会等单位主办，南宁市信息网络安全协会等单位承办，定于2023年11月10日上午在南宁市科技馆（青秀区铜鼓岭路10号）科学会堂学术报告厅举办。

论坛主题为“凝聚网络空间安全学术智慧 赋能数字经济时代四链融合”，旨在推动网络空间安全学术交流、学科建设、技术应用、成果转化、商业模式创新，研判未来技术发展趋势，搭建“政产学研用资”互动交流共享平台。大会邀请了国内细分领域的学者专家和企业专家共话最新成果。（来源：南宁市信息网络安全协会）

3. 佛山市信息协会成功举办2023年佛山市职工职业技能大赛第三届开发者大赛

11月4日，由佛山市总工会主办，佛山市信息协会、佛山市CIO联盟承办的“2023年佛山市职工职业技能大赛第三届开发者大赛”成功落下帷幕。

此次大赛以“创新驱动·智赋无限”为主题，分为创新理念专题和成果应用专题两个专题，共有32名选手进行决赛的精彩角逐。参赛选手通过利用人工智能、大数据分析等先进技术，实现了生产流程优化、降低能耗和提高质量等目标，展示了制造业数字化转型的前沿成果。

佛山市信息协会、佛山市 CIO 联盟秘书长孙逊表示，佛山坚持制造业当家，聚焦优势产业集群，探索产业集群数字化智能化转型的新模式，推动“制造大市”向“制造强市”迈进，大赛通过激发制造业企业信息技术队伍建设的创新活力，开发各类技术解决方案，推动制造业的数字化、智能化转型。此次大赛不仅为企业职工提供了一个展示创新能力的平台，也为佛山市制造业高质量发展注入了新动力。（来源：佛山市信息协会）

4. 清远市网络文化协会承办 2023 年清远市网络文明大会

近日，“汇聚网络正能量 逐梦伟大新时代”2023 年清远市网络文明大会成功举行。大会设置主旨发言环节，宣读《共建网络文明行动承诺践诺书》，为 2023 清远市“五个十”网络正能量精品推选活动中的获奖单位颁奖，并邀请与会嘉宾以“网聚文明向善力量，共建美好精神家园”为题参与论坛探讨。

在主旨发言环节中，清远市委网信办领导、互联网企业代表、自媒体从业者和网络志愿者先后就如何共建网络文明，共享网上美好精神家园方面进行了主旨发言。

清远市网络文化协会代表宣读《共建网络文明行动承诺践诺书》，号召践行“坚持思想引领，把握正确方向”“ 坚持价值导向，建设清朗空间”

“坚持行业自律，践行社会责任”“ 坚持行为规范，提高文明素养”“坚持科技向善，助推创新发展”五大承诺。（来源：清远市网络文化协会）

5. 徐州网络公共安防技术协会赴苏州参加电子信息博览会

11 月 9 日至 11 日，由国台办和江苏省人民政府主办，由省商务厅、工业信息化厅、省台办和苏州市人民政府承办的第二十一届中国（苏州）电子信息博览会在苏州国际展览中心隆重举行。徐州网络公共安防技术协会理事长卜庆亚受邀带队前往参观考察。

本届电博会以“数字赋能 创新制造”为主题，契合两岸同胞促进数字技术与实体经济深度融合的共同愿望，包括开幕式、5 场主题论坛以及 1 场两岸智能装备产业对接会。展览面积 2 万平方米，展位 800 个，线下参展企业达 400 家，专业观众 10000 余人。台资企业占比 52%，并设置线上展区，为展商提供线上展览、在线直播、一对一线上商洽服务。

卜庆亚受邀出席开幕式，作为审定发布专家参加了《无线对讲通讯系统建设技术要求》团体标准审定发布会，出席了 2023 年全国巡展新品发布会暨“数字赋能 共铸智慧生活”高峰论坛，并与长三角安防地区协会领导一同参观了电博会展区。

期间，卜庆亚协同企业代表受邀赴苏州天融信网络安全技术有限公司、苏州楚天龙数字科技有限公司、苏州锐丰建声灯光音响器材工程安装有限

公司考察调研，就网络安全、大数据与云服务提供商以及促进数据经济发展繁荣等议题展开了探讨交流。（来源：徐州网络公共安防技术协会）

6. 甘肃省商用密码行业协会举办《密码法》进校园宣讲活动

10 月 24~25 日，由甘肃省国家密码管理局指导，甘肃省商用密码行业协会主办，西北师范大学、甘肃政法大学、兰州理工大学承办的《中华人民共和国密码法》进校园宣讲活动成功举办。活动以“增强密码安全意识，筑牢安全保密防线”为主题，甘肃商用密码行业协会会员单位、各高校师生共 500 余人参加活动。

甘肃省国家密码管理局副局长瞿凌杰出席了本次活动并致辞。她表示，密码技术作为保障网络与信息安全的核心技术和基础支撑，是国家的重要战略资源；希望通过此次活动，能够使大家充分认识到学习宣传贯彻《密码法》及相关法规的重要意义，多掌握密码方面的知识，自觉树立保密意识，在思想上构筑起一道密码安全的牢固防线，为民族复兴贡献自己的力量。同时，我省密码人才稀缺，也希望各高校紧抓国家大力支持密码事业发展和密码人才培养的良机，发挥自身优势，成立密码学科专业，培养优秀的密码人才，助力我省密码事业实现高质量发展。

协会设立西北师范大学、甘肃政法大学、兰州理工大学三个会场，邀请讲师围绕《密码法》《商用密码管理条例》《保密法》向广大师生

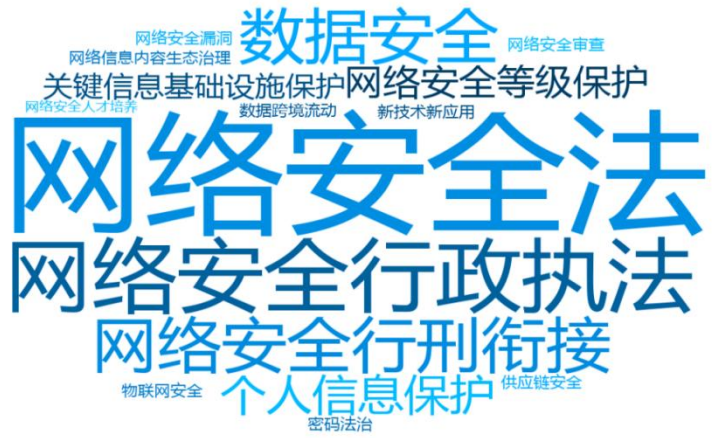
进行了专业解读；协会秘书处向三所高校密码学、网络安全、计算机应用等相关专业学生捐赠了助学基金；组织会员单位就商用密码行业的现状、发展趋势、就业市场前景等对同学们做了精彩分享，与各高校老师面对面深入交流了学科建设、实验室建设及教学、科研、就业等内容；同时组织密码相关企业在校园内摆放宣传展板、布置密码科普及招聘咨询台，提高了同学们的知识领域，扩大了同学们对密码产业、网络安全产业、数据安全产业的认知，辅导和指引了同学们的成长目标和就业方向。

此次活动将密码、保密宣传引入校园，不但拓展了密码科普宣传教育的范围，增强了同学们对密码安全、国家安全及保密安全的意识，同时也促进了产业单位与高校密码相关学科领域的进一步深入交流，加强了高校密码学科的建设和发展，为我省密码人才培养、密码产业的发展做出了积极贡献。（来源：甘肃省商用密码行业协会）

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

……