网安联
Wang An Lian

网络与数据安全治理前沿洞察

Frontiers of Regulatory Oversight in Cyber Security and Data Governance

2023年9月第2期（总第2期）

2023年8月31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

刘玮颉 广州网络空间安全协会 副秘书长

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

程　谦 河源市网络空间安全协会 秘书长

孔德剑 曲靖市网络安全协会 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：安全态势

导读：8 月，武汉地震监测中心遭网络攻击事件有新进展，联合调查组在受害单位调查发现符合美国情报机构特征的后门恶意软件，攻击者旨在窃取地震监测相关数据，而且具有明显的军事侦察目的。

此外，杭州马拉松官网报名页面崩溃，显示大量报名者真实姓名、手机号码、身份证件号码等个人信息，报名系统紧急关闭后于次日重新开放。

关键词：境外网络攻击、个人信息泄露

1. 武汉地震监测中心被网攻“幕后黑手”已锁定

8 月 14 日，《环球时报》记者获悉，针对武汉市应急管理局地震监测中心遭遇网络攻击一事，国家计算机病毒应急处理中心和 360 公司组成的联合调查组已取得新进展，在受害单位的网络中发现技术非常复杂的后门恶意软件，符合美国情报机构特征，具有很强的隐蔽性，并且通过恶意软件的功能和受影响的系统判断，攻击者的目的是窃取地震监测相关数据，而且具有明显的军事侦察目的。

下一步有关机构将向外界公开披露美国政府一直处于高度保密的某全球侦察系统，其对我国和世界各国国家安全和世界的和平安全都构成严重安全威胁。（来源：环球网）

2. 杭州马拉松官网报名页面崩溃泄露大量个人信息

8 月 28 日消息，杭州马拉松官网报名页面崩溃，显示大量报名者真实姓名、手机号码、身份证件号码等个人信息，当日，杭州马拉松官网紧急关闭报名入口，暂停报名。

报名参加马拉松的选手表示在官网登录自己的账号报名，却跳出来另一位参赛者的个人信息，包括姓名、身份证号、性别、出生日期、服装尺码等等。另有网友也在社交媒体表示，登录自己的账号查询是否成功报名，却显示他人信息，包括姓名、身份证号、家庭住址、手机号等。8 月 29 日，杭州马拉松工作人员表示网站现已重新开放。（来源：数据安全域）

境内前沿观察二：立法动向

导读：8月，国家网信办发布《个人信息保护合规审计管理办法（征求意见稿）》，要求处理超过100万人个人信息的个人信息处理者每年至少开展一次个人信息保护合规审计，其他个人信息处理者每两年至少开展一次个人信息保护合规审计。工信部发布通知，要求在中国境内从事互联网信息服务的APP主办者履行备案手续。通知发布前开展业务的APP应当在2024年3月底前向其住所所在地省级通信管理局履行备案手续。2024年4月至6月底，电信主管部门将组织对APP备案情况开展监督检查，对仍未履行备案手续的APP依法进行处置。

成都市、宁夏回族自治区相继发布政策文件，推动人工智能产业创新发展的同时强调人工智能安全保障。北京市卫健委发布《北京市互联网诊疗监管实施办法（试行）（征求意见稿）》，指出人工智能软件等不得冒用、替代医师本人提供诊疗服务，严禁使用人工智能等自动生成处方。

关键词：个人信息保护合规审计、APP备案、行政执法电子数据取证、生成式人工智能服务内容标识、人工智能创新发展

（一）国家层面动向

1. 国务院发布《关于进一步优化外商投资环境 加大吸引外商投资力度的意见》：探索便利化的数据跨境流动安全管理机制

8 月 13 日，国务院发布《关于进一步优化外商投资环境 加大吸引外商投资力度的意见》，从持续加强外商投资保护、提高投资运营便利化水平等方面有效吸引和利用外商投资。

意见强调，要提高投资运营便利化水平，探索便利化的数据跨境流动安全管理机制。落实网络安全法、数据安全法、个人信息保护法等要求，为符合条件的外商投资企业建立绿色通道，高效开展重要数据和个人信息出境安全评估，促进数据安全有序自由流动。支持北京、天津、上海、粤港澳大湾区等地在实施数据出境安全评估、个人信息保护认证、个人信息出境标准合同备案等制度过程中，试点探索形成可自由流动的一般数据清单，建设服务平台，提供数据跨境流动合规服务。（来源：中国政府网）

2. 国家网信办发布《移动互联网未成年人模式建设指南（征求意见稿）》

8 月 2 日，国家网信办发布《移动互联网未成年人模式建设指南（征求意见稿）》，将“青少年模式”全面升级为“未成年人模式”，推动模式覆盖范围由 APP 扩大到移动智能终端、应用商店。

征求意见稿强调，未成年人模式应具备自动切换功能。在移动智能终端一键启动未成年人模式后，应用程序、应用程序分发平台应自动切换到未成年人模式界面；在移动智能终端退出未成年人模式后，应用程序、应用程序分发平台应自动切换到普通模式界面。征求意见稿要求，移动智能终端应为不同年龄段的未成年人用户提供差异化使用时长管理服务。当超过每日使用时限，移动智能终端应自动关闭除特定必要应用程序和家长自定义豁免的应用程序之外的其他应用程序。（来源：中国网信网）

3. 国家网信办发布《个人信息保护合规审计管理办法（征求意见稿）》

8 月 3 日，国家网信办发布《个人信息保护合规审计管理办法（征求意见稿）》。征求意见稿指出，个人信息处理者开展合规审计的情形分为两种：一是自行定期开展审计。处理超过 100 万人个人信息的个人信息处理者应当每年至少开展一次个人信息保护合规审计，其他个人信息处理者应当每两年至少开展一次个人信息保护合规审计。个人信息处理者自行定期开展审计的，可根据实际情况，由本组织内部机构或委托专业机构开展。

二是应监管要求审计。履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应监管要求开展审计的，应在收到通知后按要求选定专业

机构进行审计，且强制外部审计应当在90个工作日内完成。（来源：中国网信网）

4. 国家网信办发布《人脸识别技术应用安全管理规定（试行）（征求意见稿）》

8月8日，国家网信办发布《人脸识别技术应用安全管理规定（试行）（征求意见稿）》，系统解答公众广泛关注的人脸识别技术滥用等诸多问题，对相关组织或个人如何规范使用人脸识别技术提出具体安全要求。

征求意见稿明确“最小使用原则”，即只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可使用人脸识别技术处理人脸信息。实现相同目的或者达到同等业务要求，存在其他非生物特征识别技术方案的，应当优先选择非生物特征识别技术方案。

征求意见稿还明确“最小存储原则”，即除法定条件或者取得个人单独同意外，人脸识别技术使用者不得保存人脸原始图像、图片、视频，经过匿名化处理的人脸信息除外。面向社会公众提供人脸识别技术服务的，相关技术系统应当符合网络安全等级保护第三级以上保护要求，并采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。属于关键信息基础设施的，还应当符合关键信息基础设施安全保护的相关要求。（来源：中国网信网）

5. 工信部发布《关于开展移动互联网应用程序备案工作的通知》

8月4日,工信部发布《关于开展移动互联网应用程序备案工作的通知》,要求在中国境内从事互联网信息服务的APP主办者，应当依照《反电信网络诈骗法》《互联网信息服务管理办法》等规定履行备案手续，未履行备案手续的，不得从事APP互联网信息服务。工信部对全国APP备案工作进行监督指导，省、自治区、直辖市通信管理局负责实施监督APP备案管理工作。

通知指出，APP主办者在填写有关备案材料并实名核验后，由其网络接入服务提供者或应用分发平台通过“国家互联网基础资源管理系统”（即ICP/IP地址/域名信息备案管理系统），向APP主办者住所所在地通信管理局在线提交备案申请，APP主办者无需到通信管理局窗口排队办理。

通知要求，2023年9月至2024年3月底，通知发布前开展业务的APP向其住所所在地省级通信管理局履行备案手续。2024年4月至2024年6月底，电信主管部门将组织对APP备案情况开展监督检查，对仍未履行备案手续的APP依法进行处置。通知发布后拟开展业务的APP，应先履行备案手续后再开展业务。（来源：工信部）

6. 财政部印发《企业数据资源相关会计处理暂行规定》

8月1日，财政部印发《企业数据资源相关会计处理暂行规定》，从适用范围、数据资源会计处理适用的准则、列示和披露要求等方面推动企业数据资源资产入表。暂行规定适用于符合企业会计准则规定、可确认为相

关资产的数据资源，以及不满足资产确认条件而未予确认的数据资源的相关会计处理。后续随着数据资源相关理论和实务的发展，可及时跟进调整。

暂行规定要求企业应当根据重要性原则并结合实际情况增设报表子项目，通过表格方式细化披露，并规定企业可根据实际情况自愿披露数据资源（含未作为无形资产或存货确认的数据资源）的应用场景或业务模式、原始数据类型来源、加工维护和安全保护情况、涉及的重大交易事项、相关权利失效和受限等相关信息，引导企业主动加强数据资源相关信息披露。（来源：财政部）

7. 市场监管总局发布《市场监督管理行政执法电子数据取证暂行规定（征求意见稿）》

8 月 22 日，市场监管总局发布《市场监督管理行政执法电子数据取证暂行规定（征求意见稿）》，主要适用于市场监督管理部门及其执法人员在行政执法过程中对电子数据的收集提取、查封扣押、检查分析、证据存储等情形。

征求意见稿明确电子数据的定义及种类，对收集提取电子数据的主体、工具及笔录要素等做出规定，明确查封、扣押原始存储介质的情形、要求、程序及笔录要素，同时对原始介质进行检查分析的适用情形、人员要求及注意事项等进行规定。（来源：市场监管总局）

8. 全国信安标委发布《信息安全技术 大数据服务安全能力要求》等四项国家标准

8 月 11 日，全国信安标委发布四项网络安全国家标准，分别是：（1）GB/T 35274-2023《信息安全技术 大数据服务安全能力要求》；（2）GB/T 42884-2023《信息安全技术 移动互联网应用程序(App)生命周期安全管理指南》；（3）GB/T 42888-2023《信息安全技术 机器学习算法安全评估规范》；（4）GB/Z 42885-2023《信息安全技术 网络安全信息共享指南》（来源：全国信安标委）

9. 全国信安标委发布《网络安全标准实践指南——生成式人工智能服务内容标识方法》

8 月 25 日，全国信安标委发布《网络安全标准实践指南——生成式人工智能服务内容标识方法》，围绕文本、图片、音频、视频四类生成内容，给出生成式人工智能服务内容标识的实践指引。

实践指南明确，对生成式人工智能服务进行内容标识分为显式水印标识与隐式水印标识两种。在人工智能生成内容的显示区域中，应在显示区域下方或使用者输入信息区域下方持续显示提示文字，或在显示区域的背景均匀添加包含提示文字的显式水印标识。提示文字应至少包含“由人工智能生成”或“由 AI 生成”等信息。

实践指南要求，由人工智能生成图片、视频时，应采用在画面中添加提示文字的方式进行标识。由人工智能生成图片、音频、视频时，应在生

成内容中添加隐式水印标识。由人工智能生成的图片、音频、视频以文件形式输出时，应在文件元数据中添加扩展字段进行标识。由自然人提供服务转为由人工智能提供服务，容易引起使用者混淆时，应通过提示文字或提示语音的方式进行标识。（来源：全国信安标委）

（二）地方层面动向

1. 上海市印发《立足数字经济新赛道 推动数据要素产业创新发展行动方案（2023-2025 年）》

7 月 24 日，上海市人民政府办公厅印发《立足数字经济新赛道 推动数据要素产业创新发展行动方案（2023-2025 年）》，提出数据要素产业创新发展的八大方向二十三项措施。行动方案强调，要强化数据安全保障。建立数据分类分级保护制度，制定重要数据目录，严格实施个人信息保护。建立数据安全监测预警和应急处置机制，提升安全事件处置智能化和自动化水平。（来源：上海市人民政府）

2. 成都市印发《成都市加快大模型创新应用推进人工智能产业高质量发展的若干措施》

8 月 4 日，成都市经信局印发《成都市加快大模型创新应用推进人工智能产业高质量发展的若干措施》。文件强调，要加强生态要素聚集，推进数据开放利用，支持成都数据集团优化公共数据运营服务平台功能，探索开展企业、个人数据采购，推动相关数据产品和模型的社会化开发利用。

依托人工智能应用发展公共服务平台，推进建设系列人工智能训练数据资源库、标准测试数据集，推动相关数据的社会化开发利用。组织遴选市场领先的数据集建设单位，开展数据价值挖掘，探索基于数据共享、模型应用的商业化场景合作。（来源：成都市经信局）

3. 济南市发布《济南市公共数据授权运营办法（征求意见稿）》

8 月 10 日，济南市司法局发布《济南市公共数据授权运营办法（征求意见稿）》。征求意见稿明确，公共数据授权运营实行“谁授权谁监管、谁运营谁负责”的安全责任制。授权单位和运营单位的法定代表人或者主要负责人是授权运营公共数据安全的第一责任人。运营单位应当依照法律法规的规定和授权运营协议约定履行数据安全保护义务，完善数据安全制度，建设安全防护体系，开展技术人员岗前安全培训，确保公共数据开发利用全过程安全，不得擅自留存、使用、泄露或向他人提供公共数据，自觉接受授权单位的监督检查，定期报告运营安全情况。（来源：济南市人民政府）

4. 宁夏回族自治区印发《促进人工智能创新发展政策措施》

8 月 13 日，宁夏回族自治区人民政府办公厅印发《促进人工智能创新发展政策措施》。文件强调要加强安全监管，建立健全公开透明的人工智能监管体系，依法依规、包容审慎开展监管，围绕网络安全、数据安全、科技伦理、就业促进等领域建立风险防范和应对机制，防范和打击违法行

为，引导人工智能相关企业和组织健康发展。强化人工智能产品和系统的网络安全防护，建设安全可信和创新发展并重的宁夏枢纽。（来源：宁夏回族自治区发展和改革委员会）

5. 贵州省发布《贵州省数据流通交易促进条例（草案）（征求意见稿）》

8 月 16 日，贵州省大数据发展管理局发布《贵州省数据流通交易促进条例（草案）（征求意见稿）》。征求意见稿要求数据流通交易平台应当依法通过网信、公安、国安等部门组织的网络安全审查，符合国家信息安全等级保护等相关要求，建立健全平台运行维护制度和应急处置预案，报监管部门备案。数据授权运营按照谁授权谁负责、谁运营谁负责、谁使用谁负责的原则确定安全责任。数据授权机构应当严格控制授权范围，数据运营机构应当加强数据安全使用管理，不得将获得授权的公共数据超出授权范围擅自转让、使用，确保数据来源可溯、去向可查、行为留痕、责任可究。（来源：贵州省大数据发展管理局）

6. 北京市卫健委发布《北京市互联网诊疗监管实施办法（试行）（征求意见稿）》：严禁使用人工智能自动生成处方

8 月 17 日，北京市卫健委发布《北京市互联网诊疗监管实施办法（试行）（征求意见稿）》。征求意见稿规定，医疗机构应建立网络安全、数据安全、个人信息保护、隐私保护等制度，并与相关合作方签订协议，明

确各方权责关系，发生患者个人信息、医疗数据泄露等网络安全事件时，应当及时向相关主管部门报告，并采取有效应对措施。医师接诊前需进行实名认证，人工智能软件等不得冒用、替代医师本人提供诊疗服务。严禁使用人工智能等自动生成处方。（来源：北京市卫健委）

7. 杭州市发布《杭州市促进智能网联车辆测试与应用规定（草案）》

8 月 23 日，杭州市人大常委会法制工作委员会发布《杭州市促进智能网联车辆测试与应用规定（草案）》。草案指出，智能网联汽车测试与应用主体应当按照网络安全相关法律、法规和信息安全标准的强制性要求，建立网络安全管理制度，落实网络安全等级保护制度，采取技术措施和其他必要措施，提高网络安全保护水平，保障网络安全、稳定运行。智能网联车辆测试与应用主体应当建立全流程数据安全和个人信息保护制度，依法处理测试与应用活动中的全部信息，落实数据安全和个人信息保护责任，采取必要措施保障数据和个人信息安全。发生或者可能发生涉及国家安全、个人信息等数据泄露、损毁、丢失等情况时，测试与应用主体应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。（来源：杭州人大）

境内前沿观察三：治理实践

导读：8 月，公安部公布全国公安机关打击整治侵犯公民个人信息违法犯罪行为成效。2020 年以来全国公安机关累计侦破案件 3.6 万起，抓获犯罪嫌疑人 6.4 万名，同步开展行政执法工作，巡查互联网企业 5.5 万家，办理行政案件 1.3 万余起，处罚一批超范围采集公民个人信息的手机APP运营公司，修补安全漏洞 3000 余个，有力保障公民个人信息安全。

公安机关、网信部门、通信管理部门公布多起依据《网络安全法》《数据安全法》进行行政处罚的案件。其中，南昌某高校不履行数据安全保护义务，导致 3 万余条教职工、学生个人敏感信息数据在境外被公开售卖，南昌公安网安部门对该学校处以警告并处 80 万元罚款，是目前已公开披露的《数据安全法》执法案件中罚款数额较高的案件。此外，江西省通信管理局公布一起依据《数据安全法》对信息技术公司进行行政处罚的案件。目前公开披露的行政案件中执法主体多是公安机关或网信部门，通信管理部门较为少见，且此次公布的案件由省级通管部门作出。

结合 8 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. 采取必要措施，保护网站服务器安全；2. 对收集的个人信息采取加密等安全技术措施；3. 发生个人信息泄露情况时，及时告知用户并向有关主管部门报告；4. 留存网络日志不少于六个月；5. 制定全流程数据安全管理制度；6. 全面落实网络安全等级保护义务，定期开展等级测评；

7. 对办公区域与服务器区域进行划分隔离，避免计算机病毒等安全风险在网络内进行横向传播；8. 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。

关键词：打击侵犯公民个人信息违法犯罪、数据泄露、数据加密、事件报告、日志留存、等级测评、网络安全风险处置

（一）公安机关治理实践

1. 公安部通报打击侵犯公民个人信息违法犯罪成效：累计侦破案件 3.6 万起，办理行政案件 1.3 万余起

8 月 10 日，公安部在北京召开发布会，公布全国公安机关打击整治侵犯公民个人信息违法犯罪行为的举措成效。发布会指出，2020 年以来公安机关每年组织“净网”专项行动，依法重拳打击侵犯公民个人信息违法犯罪活动，累计侦破案件 3.6 万起，抓获犯罪嫌疑人 6.4 万名，查获手机黑卡 3000 余万张、网络黑号 3 亿余个，近 3 年来破获案件数量和抓获人数连续突破新高，打击力度和打击成果空前。

一是坚持以打开路，开辟网络空间新战场，全环节摧毁犯罪生态。公安机关按照“打源头、摧平台、断链条”的工作思路，锚定技术类侵犯公民个人信息犯罪源头，发起打击黑客犯罪集群战役，侦破一批利用木马病毒、钓鱼网站、渗透工具、网络爬虫等黑客手段窃取公民个人信息案件。

二是坚持问题导向，聚焦人民群众“急难愁盼”，深入开展专项整治。公安机关聚焦侵犯公民个人信息违法犯罪的难点、盲点，出重拳、下狠手，组织开展专项整治。针对“AI 换脸”导致群众被欺诈的问题，公安机关发起专项会战，侦破相关案件 79 起，抓获犯罪嫌疑人 515 名。

三是坚持防管结合，压实企业平台责任，筑牢数据安全防线。公安部立足于信息安全和数据安全，积极参与有关政策法规的制定工作，推动出

台了《个人信息保护法》《数据安全法》，会同中央网信办等部门制定印发了《APP 违法违规收集使用个人信息认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等，明确了个人信息认定标准、行业规范和企业责任，并同步开展行政执法工作，巡查互联网企业 5.5 万家，办理行政案件 1.3 万余起，处罚了一批超范围采集公民个人信息的手机 APP 运营公司，修补安全漏洞 3000 余个，督导互联网头部企业完善用户数据采集、存储、使用制度。为进一步筑牢数据安全防线，公安机关大力推动国家网络安全等级保护制度、《关键信息基础设施安全保护条例》的落实，持续加强系统建设、网络运营、数据存储、数据传输、数据处理等重点环节的安全防护措施，确保重要敏感数据的整个生命周期安全可靠。

四是坚持多方合力，构建协同作战机制，打造综合治理格局。公安部依托“净网”专项行动，与中央网信办、最高人民法院、最高人民检察院、工业和信息化部等相关单位建立长效合作机制，从严厉惩治犯罪、突出重点整治、加强行业监管、规范依法办案、开展宣传教育等多方面协同推进，切实形成了保护公民个人信息和数据安全的工作合力，构建起源头治理、综合治理、系统治理的工作格局。（来源：公安部网安局）

2. 公安部发布打击侵犯公民个人信息犯罪十大典型案例

8 月 10 日，公安部发布打击侵犯公民个人信息犯罪十大典型案例：（1）云南怒江“2.13”侵犯公民个人信息案；（2）广东佛山某汽车服务有限公司侵犯公民个人信息案；（3）山东济南席某倩侵犯公民个人信息案；（4）

安徽宣城“1.10”侵犯公民个人信息案；（5）江苏无锡秦某等网民侵犯公民个人信息案；（6）浙江宁波李某等人侵犯公民个人信息案；（7）福建厦门某科技有限公司信息泄露案；（8）上海闵行侵犯公民个人信息案；（9）陕西西安侵犯公民个人信息案；（10）福建龙岩某公司侵犯公民个人信息案。（来源：公安部）

3. 上海警方破获一起侵犯公民个人信息案件，远程操控非法获取物流面单 3 万张

8 月 6 日消息，在上海市公安局网安总队的指导下，上海市公安局青浦分局凤溪派出所近日在侦办一起诈骗案时发现部分受害人的快递信息被某物流公司泄露。获悉该线索后，警方立即开展侦查工作。警方在该物流公司一电脑内发现了两款不同的远程控制软件。据物流公司相关负责人反映其中一款操控软件是与总部远程调控该电脑而安装的，但另外一款软件其从未见过，公司员工也未曾使用过。

警方循线追踪，发现王某有重大作案嫌疑。经查，犯罪嫌疑人王某因在网上得知可以通过出售快递面单信息获利，伙同从事供应链业务的邹某和高某合谋非法获取出售物流面单信息。邹某假借至该物流公司“洽谈业务”的时候将王某带进公司内部，王某在存放面单信息的电脑上安装远程控制软件，其后高某通过远程控制软件提取面单有效信息并在网上贩卖，截至案发共非法获取物流面单 3 万余张，累计非法获利 9000 余元。

目前，犯罪嫌疑人王某因涉嫌侵犯公民个人信息罪被上海市青浦区人民检察院依法批准逮捕，犯罪嫌疑人高某与邹某因涉嫌侵犯公民个人信息罪被警方依法采取刑事强制措施。（来源：警民直通车上海）

4. 因数据泄露，广西公安网安部门适用《网络安全法》对违法单位罚款 20 万元

8 月 11 日消息，广西北海公安网安部门近日在查处一起涉个人信息保护违法案件时发现北海某网站存在数据泄露问题，网站约 22 万个人信息数据被挂在境外论坛售卖。

经查，涉案公司主要提供网上咨询服务，建设有一网站，在日常工作中收集了个人和企业等大量公民信息，但未能按照《数据安全法》《网络安全法》以及有关等级保护工作要求落实网络安全保护主体责任。公司网站服务器安全防护措施不足，仅能对 SQL 注入、XSS、WebShell 等简单攻击手段进行防御，网站存在被多个境外 IP 攻击入侵的情况。此外，公司未采取数据加密等有效的技术保护措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失，且在发现公司发生个人信息泄露的情况下，未及时告知用户和主动向公安机关报告。该公司还存在网站日志只存储 30 日，网络日志留存不足六个月及相关安全管理制度缺失等问题。

对此，广西北海公安机关根据《网络安全法》第四十二条的规定，对公司及直接负责人员分别作出罚款 20 万元、3 万元的行政处罚。同时，北海网安部门应用网络与信息安全信息通报机制，将该案例通报各党政机关

单位，监督指导其落实主体责任，提升网络安全保护能力和水平。（来源：公安部网安局）

5. 因数据泄露，南昌某高校被罚款 80 万元

8 月 17 日消息，南昌公安网安部门近日工作发现，南昌某高校 3 万余条师生个人信息数据在境外互联网上被公开售卖。南昌公安网安部门立即开展一案双查，成功抓获犯罪嫌疑人 3 名。同时，对涉案高校不履行数据安全保护义务违法行为开展执法检查。

经查，涉案高校在开展数据处理活动中，未建立全流程数据安全管理制度，未采取技术措施保障数据安全，未履行数据安全保护义务，导致学校存储教职工信息、学生信息、缴费信息等 3000 余万条信息的数据库被黑客非法入侵，其中 3 万余条教职工、学生个人敏感信息数据被非法兜售。

南昌公安网安部门根据《数据安全法》第四十五条的规定，对该学校作出责令改正、警告并处 80 万元罚款的处罚，对主要责任人作出 5 万元罚款的处罚。（来源：南昌网警）

6. 新疆公布八起侵犯公民个人信息犯罪典型案例

8 月 17 日，新疆维吾尔自治区公安厅公布全区公安机关打击整治侵犯公民个人信息违法犯罪行为 8 起典型案例：（1）巴州杜某侵犯公民个人信息案；（2）和田麦某侵犯公民个人信息案；（3）阿克苏玉某、张某侵犯公民个人信息案：（4）博州阿某侵犯公民个人信息案；（5）和田努某、

栗某侵犯公民个人信息案；（6）伊犁张某侵犯公民个人信息案；（7）伊犁张某侵犯公民个人信息案；（8）乌鲁木齐杨某、郝某侵犯公民个人信息案。（来源：公安部网安局）

7. 浙江全面整治网上违法犯罪乱象，破获一起利用 ChatGPT 盗刷提现案件

8 月 24 日，从浙江省公安机关夏季治安打击整治行动暨“净网 2023”专项行动新闻发布会上获悉，今年 1 月至 8 月，浙江公安机关共抓获各类网络违法犯罪嫌疑人 2.4 万余名，移送起诉 5980 余名，公安机关重点打击网络犯罪、网络黑灰产业链、网上乱象和重要系统平台，全面整治网上违法犯罪乱象。浙江公安机关通过深入研究侵犯公民个人信息犯罪规律特点，打源头、断链条，今年以来共侦办侵犯公民个人信息案件 375 起，刑事拘留 306 名。

此外，发布会现场还通报了一起利用 ChatGPT 盗刷提现企业账户资金的新型犯罪案件。犯罪嫌疑人利用 ChatGPT 编写用于批量盗刷的提款程序，实施批量盗刷企业账户资金的犯罪活动，并通过虚拟币洗钱变现，给相关企业带来巨大经济损失。今年 4 月，杭州市公安局网络警察分局在网上巡查发现后，通过大量的数据分析和追踪溯源工作，锁定位于泰国的犯罪嫌疑人谢某，并将其抓获。（来源：网信浙江）

8. 广东网警打击“网络水军”犯罪活动，涉案金额5.3亿元

8月24日消息，广东网安部门近日对刷量控评“网络水军”犯罪活动开展集群打击，其中东莞网安部门组织全市17个镇街分局开展三波次集中收网打击行动，成功打掉犯罪团伙22个，依法刑事拘留嫌疑人89名，涉案金额达5.3亿元。

案例一：东莞网安部门查明，某“网络水军”团伙技术人员伊某自2021年5月至今先后搭建了3个专门“刷单”的平台，并分别给赖某某、李某某、叶某某等人运营。该团伙利用刷单平台，组织商家和刷手在网络平台上大量进行虚假购物、发布虚假评价并从中赚取刷单佣金，伊某从中抽取30%利润。目前，属地公安机关已捣毁作案窝点4个，现场扣押作案电脑、手机、银行卡一批，涉案金额共5700余万元。

案例二：东莞网安部门查明，刘某乐开办电子商务公司，招聘员工通过各网络平台引流接单，再通过自动刷单软件为知名电商平台的网店商家提供“有偿刷单”的非法业务，使商家的店铺成交量、好评率、店铺权重得到提高，从而增加商家的商品销量。2023年7月，东莞网安部门联合大朗分局开展收网行动，抓获嫌疑人35名，涉案金额共约4000万元。

案例三：东莞网安部门查明，陈某、李某等人注册某科技公司，专门在网络上发广告，组织水军人员为医疗机构、车企等商家在网络平台进行删除、屏蔽和降权下沉等操作，有偿提供信息删除服务。经统计，该团伙从2022年3月至今有偿删帖约1.1万次，非法获利约53万元人民币。（来源：公安部网安局）

9. 西安警方捣毁特大“网络水军”团伙

8 月 31 日消息，西安警方近日捣毁一特大“网络水军”团伙。2023 年，西安网警在工作中发现，有多个短视频平台账号以新闻或法律从业者的名义发布消息，宣称可以通过网络自媒体曝光的方式解决问题。

经初步核查，这是一个以郭某某、刘某等人为头目的百人以上特大“网络水军”犯罪团伙。该团伙披着法律咨询、文化传媒的外衣，在各短视频网络平台发布噱头视频引流诱导炒作，公开出售有偿代刷点赞量、关注量、浏览量、粉丝量等服务。同时，该团伙还雇佣“刷手”通过非法脚本程序，模拟真实用户进行批量操作，短时间内即可将短视频的“浏览量”数值推至百万量级。

经查，涉案的 9 家公司均是由郭某某、刘某为组织者的某传媒公司发展而来。二人在意识到相关行为涉嫌违法后，便分散原始股东和员工，在同一时期注册了 9 家新公司，并选择了非骨干成员担任法人，而真正的老板则隐居幕后操控公司运营，以实现逃避打击的目的。警方已查明涉事 9 家公司的主要负责人，同时查明山东菏泽白某某、湖南娄底谢某、谭某某团伙，也利用非法程序为上述网络水军团伙引流刷量。

以上团伙以牟利为目的，披着文化传媒、法律咨询公司的外衣，通过隐瞒真相、歪曲事实等手段为网民策划网络炒作文案，拍摄曝光视频，蒙骗和煽动网民借助网络曝光、炒作等方式达成利益诉求。其内部组织严密、分工明确，背后黑灰产链条完整，大肆骗取群众钱财，制造社会矛盾，严重扰乱网络秩序和社会平稳。截至 7 月 17 日，西安警方已依法采取刑事强

制措施125人，行政拘留12人，止付金额218万余元。目前，相关案件正在进一步侦办中。（来源：西安网警）

（二）网信部门治理实践

1. 国家网信办公布“清朗·优化营商网络环境 保护企业合法权益”专项行动成果

8月1日，国家网信办公布“清朗·优化营商网络环境 保护企业合法权益”专项行动成果，重点网站平台清理涉企虚假不实等信息8.6万余条，依法依约处置账号8425个。专项行动重点开展以下几方面工作：（1）坚决查处恶意集纳炒作企业负面信息、谋求非法利益问题；（2）严厉打击散布涉企虚假不实信息问题；（3）集中查处假冒仿冒他人企业名称等问题；（4）全面整治虚构企业家私生活话题、炒作企业家个人隐私问题；（5）集中处置传播带有地域歧视、人群歧视等标签式、污名化信息的问题。（来源：中国网信网）

2. 中央网信办等部门联合开展“清朗·杭州亚运会和亚残运会网络环境整治”专项行动

8月28日，中央网信办秘书局、中央宣传部版权管理局、杭州第19届亚运会组委会办公室联合发布通知,决定自8月28日至10月29日开展“清朗·杭州亚运会和亚残运会网络环境整治”专项行动，集中整治片面、歪曲传播突发事件信息，假冒当事人或相关人员身份发声，关联翻炒旧闻旧

事；未经许可擅自开展互联网新闻信息服务活动；利用生成式人工智能技术制作和发布有关虚假赛事视频；组织“人肉搜索”，故意泄露运动员、裁判员、教练员等个人隐私信息，诱导实施网络暴力等8类突出问题。

通知要求各地网信办、版权局要提高政治站位，按照职责深入开展专项整治工作，督促属地网站平台严格履行主体责任，加强排查处置，对工作落实不力的网站平台，依法依规进行处罚。（来源：中国网信网）

3. “清朗·2023年暑期未成年人网络环境整治”专项行动曝光第一批典型处置案例

8月29日，国家网信办公布“清朗·2023年暑期未成年人网络环境整治”专项行动阶段成果，围绕集中整治诱导未成年人不良行为问题、严格排查下架应用商店违规APP、及时阻断境外仿冒网站平台向境内传播涉未成年人淫秽色情内容、严厉打击搭建运营涉未成年人色情网站的违法犯罪活动等六个方面公布一批典型案例。

国家网信办表示，6月下旬以来，网信部门深入开展专项行动，聚焦未成年人较为活跃的网站平台、产品功能和位置版块，及时发现处置危害未成年人身心健康的突出问题，有力遏制一些乱象隐形变异、反弹反复，为未成年人营造健康向上的网络环境。网信部门将持续深入推进专项行动，督导网站平台切实履行信息内容管理主体责任，对侵害未成年人合法权益的各类乱象行为，以及存在突出问题的网站平台，依法从严从重采取处置措施并公开曝光。（来源：网信中国）

4. 因未落实数据安全保护责任，余姚市网信办对一楼盘开发商进行行政处罚

8月14日消息，余姚市某楼盘业主近日在网上发帖反映频繁收到装修公司进行电话推销，怀疑个人信息数据遭到泄露，余姚市网信办在上级网信部门的指导下，立即根据线索对该楼盘开发商宁波某某有限公司进行立案调查。

经现场调查取证、约谈交流，余姚市网信办认定该公司在销售经营过程中对业主、访客个人信息未落实数据安全保护责任，其行为违反《数据安全法》第二十七条规定，依据《数据安全法》第四十五条第一款规定，对该公司作出警告的行政处罚，并责令其对数据安全保护落实不到位之处立即整改。（来源：余姚发布）

5. 因未履行等保测评等多项网络安全保护义务，南昌某高校被罚款5万元

8月29日消息，接上级网信部门近日通报，南昌属地某高校所属IP疑似被黑客远程控制，并频繁对外发起网络攻击。

经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：1.该高校未履行网络安全保护义务，未对运营的网络及信息系统开展网络安全等级保护测评等相关工作；2.该高校的防火墙配置策略存在缺陷，办公区域与服务器区域之间未作划分隔离，导致设备在感染了新型计算机病毒后横向传播，致使多台服务器和终端中毒；3.该高校未及

时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，所属网络持续对内对外发起大规模网络攻击，导致产生危害网络安全的后果。

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

6. 北京市互联网信息办公室发布《北京市扫码消费服务违规收集使用消费者个人信息案例解析及合规指引》

8月30日，北京市互联网信息办公室联合国家互联网应急中心北京分中心发布《北京市扫码消费服务违规收集使用消费者个人信息案例解析及合规指引》。

指引综合对北京市提供扫码消费服务二维码抽样测试情况，对六类常见易发违规问题进行案例解析，主要包括：（1）强制或诱导消费者关注公众号；（2）未通过弹窗等显著方式告知消费者隐私政策；（3）频繁提示注册登录，干扰消费者使用；（4）强制消费者提供与功能无关的个人信息；（5）违规向第三方提供消费者个人信息；（6）未向消费者提供删除个人信息的功能选项。针对上述问题，指引提出提供扫码消费服务的小程序，在收集消费者个人信息前应当以弹窗或其他显著方式向消费者提示隐私政策；不得默认勾选同意或仅提供同意选项等六条合规建议，供全市提供扫码消费服务的经营者遵照执行。（来源：网信北京）

（三）通信管理部门治理实践

1. 上海市通信管理局组织开展 2023 年电信和互联网行业重要数据评审

8 月 2 日，上海市通信管理局组织首批重点企业按照工业和信息化领域重要数据有关识别指南，开展重要数据识别认定及目录备案工作。评审认为，上海移动、得物、喜马拉雅、阅文、2345、七猫、携程、拼多多、小红书、莉莉丝、米哈游等公司报送的重要数据目录类别较为齐全、分类较为精准、内容较为详实，整体目录质量较好。同时也发现部分企业报送的重要数据目录未达到合格要求。（来源：上海市通信管理局）

2. 江西省通信管理局依据《数据安全法》对一信息技术公司进行行政处罚

8 月 15 日消息，根据上级部门通报，赣州某信息技术公司业务系统近日疑似遭受黑客攻击，存在数据泄露风险。江西省通信管理局立即依法组织开展案件调查，查明该公司在开展网络营销代理业务中未有效落实网络和数据安全保护主体责任，未依法采取相应的技术措施保障业务系统数据安全，该行为违反了《数据安全法》相关规定，江西省通信管理局对赣州某信息技术公司给予警告、罚款 15 万元，对直接负责的主管人员和直接责任人各罚款 1 万元。（来源：江西信息通信业）

3. 北京市通信管理局开展2023年电信和互联网行业网络与数据安全检查

8月25日，北京市通信管理局发布通知，开展2023年电信和互联网行业网络与数据安全检查。此次网络与数据安全检查对象为北京市基础电信企业、域名注册服务企业、云平台服务提供商、APP运营企业、车联网平台企业、工业互联网平台和标识解析节点企业等。重点检查相关企业建设运营的网络、系统、平台、应用、业务，特别是电信和互联网行业关键信息基础设施和重要网络单元及承载的信息系统。

此次主要检查以下六方面内容：（1）网络安全管理制度和保障体系建设落实情况；（2）通信网络安全防护工作落实情况；（3）数据安全保护落实情况；（4）个人信息保护及安全隐患工作情况；（5）工业互联网企业网络安全防护情况；（6）车联网网络安全防护定级备案管理情况。（来源：北京市通信管理局）

（四）其他部门治理实践

1. 因违反信用信息管理相关规定，百行征信被央行罚款51.5万元

8月4日，中国人民银行发布银罚决字〔2023〕71-73号行政处罚决定书。行政处罚决定书载明，因百行征信有限公司存在违反征信机构管理规定，违反信用信息采集、提供、查询及相关管理规定等两项违法行为被处以警告及罚款51.5万元的行政处罚。

因对公司违反信用信息采集、提供、查询及相关管理规定的违法行为负有责任，百行征信有限公司运营部客服中心异议处理员黄某某、运营部客服中心团队主管汪某某分别被处以罚款7.1万元的行政处罚。（来源：中国人民银行）

2. 北京互联网法院：近五年审结涉网络暴力案件465件

8月3日，北京互联网法院召开涉网络暴力案件审判情况新闻发布会，通报该院近五年涉网络暴力案件审判情况及典型案例。发布会指出，该院自2018年9月建院以来至2023年6月以自然人为原告、以判决形式审结的该类案件465件。

受理案件存在以下特征：（1）新型网络暴力手段更新较快、层出不穷。以人肉搜索、合成虚假照片、制作表情包、传播“AI换脸”视频等形式发生的网络暴力正愈演愈烈；（2）网络自媒体、营销号、网络大V因关注度较高易引发网暴严重后果。案件反映，部分网络自媒体、营销号、网络大V往往为了吸引关注度和流量，制造猎奇信息、挑起网民情绪或跟风炒作热点事件，引发众多跟帖评论进而引发网暴；部分则利用其较高的关注度和粉丝量，诱导粉丝不理智行为，从而产生网暴；（3）青少年易受误导加入网络暴力活动；（4）侵权人将线下矛盾转至线上的行为频发。（来源：中国法院网）

3. 北京市高级人民法院：侵犯公民个人信息犯罪案件中“爬虫”软件成为收集大量信息时的常用软件之一

8 月 23 日，北京市高级人民法院召开北京法院侵犯公民个人信息犯罪案件审判情况新闻通报会，通报侵犯公民个人信息罪案件审判情况，并发布典型案例。2018 年以来，北京三级法院共审结侵犯公民个人信息犯罪案件 219 件，其中一审 179 件、二审 40 件，判处犯罪分子 294 人。

通报会指出，涉案公民个人信息类型中高度敏感信息占比突出，所有已结案件中 24.6%的案件涉及包括行踪轨迹信息、通信内容、征信信息和财产信息高度敏感信息，涉案公民个人信息的数量规模日渐庞大，侵犯公民个人信息的犯罪手段越发隐蔽。不法分子多是通过社交软件群、网站论坛等平台买卖或交换个人信息，“爬虫”软件成为收集大量信息时的常用软件之一。五成案件的被告人有较为固定的工作单位或职业，从学历、职务看，不乏有被告人拥有较高的学历水平，在大型互联网公司、电商平台、通讯运营商等任较高职务。此外，侵犯公民个人信息犯罪与其他违法犯罪活动相关联，排除买卖、交换等中间环节，39.6%的涉案信息被用于违法甚至犯罪活动，如违规提取公积金或办理信用卡、同行不正当竞争、电信网络诈骗等。（来源：京法网事）

4. 杭州互联网法院审理一起个人信息保护民事公益诉讼案，涉及未经同意定制“AI 换脸”视频

8 月 23 日消息，杭州互联网法院近日组成七人合议庭，对公益诉讼起诉人杭州市萧山区人民检察院诉虞某个人信息保护民事公益诉讼案公开开庭审理，判令被告虞某删除非法获取的个人信息，公开赔礼道歉、消除影响并赔偿损失共 60000 元。被告虞某服从法院判决，现已履行道歉、赔偿义务等民事责任。赔偿金额将专门用于个人信息保护、人脸深度合成技术不当应用的治理等公益事项。

公益诉讼起诉人诉称，其在履职过程中发现，2021 年左右开始，虞某以牟利为目的，在未取得被编辑人同意的情况下，利用“AI 换脸”软件非法处理他人人脸信息，将他人人脸信息与部分视频中的人脸信息进行替换合成，制作生成虚假的换脸视频。上述行为侵害了承载在不特定多数社会主体个人信息之上的公共信息安全，破坏社会公共秩序，构成对公共信息安全领域的社会公共利益侵害，故向杭州互联网法院提起民事公益诉讼。

杭州互联网法院经审理认为，虞某使用换脸软件（技术）深度合成伪造视频和图片，未经相关信息主体同意，大量搜集、提取、替换、合成、存储他人人脸敏感信息等个人信息，并将深度合成伪造视频、图片发布于 2000 多人的多个社交软件群组中，同时，其为他人提供不特定主体的人脸替换定制服务，并为牟利而对外销售换脸软件、传授换脸技术教程，获得非法利益数万余元，上述行为构成对个人信息权益的侵害。虞某将合成伪造的视频、图片在人数众多的网络群组中发布，传播可能性高、影响范围

大，使得潜在的社会不特定群体可能成为受侵害的对象，更可能导致公众形成“眼见不为实”的心理预期，破坏互联网数字世界中社会共同体的信任，损害了相关领域的社会公共利益。（来源：杭州互联网法院）

5. 深圳市人民检察院发布《深圳市移动互联网应用程序分发业务合规指引》

8 月 29 日，深圳市人民检察院发布《深圳市移动互联网应用程序分发业务合规指引》。

指引指出，应用程序分发平台应当充分履行数据及信息安全保障义务，违反网络安全、数据安全、个人信息保护相关法律法规的应当依法承担行政或刑事责任。应用程序分发平台上线运营三十日内，分发平台经营者需要向所在地省级网信部门备案，备案的内容包括分发平台经营者的基本情况、分发平台有关信息、互联网信息服务许可或备案的情况以及相关的制度文件、平台管理规则、服务协议等有关材料。指引强调，应用程序分发平台应当按照国家网络安全等级保护制度的要求，采取严格措施保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改，履行网络安全保护义务。（来源：深圳市人民检察院）

境外前沿观察：月度速览十则

导读：8 月，美国总统拜登签署《关于处理美国在受关切国家的特定国家安全技术和产品领域投资的行政令》，限制美国企业对中国芯片、人工智能等关键技术行业进行新投资，再次引发全球对中美技术对抗升级的忧虑。印度总统正式批准《数字个人数据保护法》，要求数据受托人仅在父母同意的情况下处理儿童个人数据。美国网络安全和基础设施安全局正在制定关键基础设施网络事件报告规则，要求关键基础设施所有者和运营商披露赎金支付情况和网络安全事件情况。英国、瑞士多地发生警察局数据泄露事件，特斯拉“大规模”数据泄露事件原因查明。

关键词：半导体和人工智能投资限制，关键基础设施网络事件报告规则，人工智能工作组，警察局数据泄露

1. 美国总统拜登签署《关于处理美国在受关切国家的特定国家安全技术和产品领域投资的行政令》

8 月 9 日，美国总统拜登签署《关于处理美国在受关切国家的特定国家安全技术和产品领域投资的行政令》。行政令基于《国际紧急经济权力法》制定，重点关注美国风险资本和私募股权公司向受关切国家的军事和军民两用部门的技术投资能力，并授权美国财政部审查美国投资者的特定对外投资活动。行政令所谓的受关切国家主要是针对中国内地及港澳地区，在现阶段拟针对半导体和微电子、量子计算机和人工智能等特定领域加强审查，并在与美企协调后于明年付诸实施。白宫表示，行政令是对美国现有出口管制和入境筛查工具的补充，目的是“消除有关国家发展此类敏感技术对美国构成的安全威胁”。（来源：美国白宫）

2. 印度总统批准《数字个人数据保护法》

8 月 11 日，印度总统批准《数字个人数据保护法》，次日该法在《印度公报》公布。该法主要内容如下：（1）个人数据保护措施。该法规定数据受托人进行数据收集、存储或对个人数据进行任何其他处理过程中的义务，明确数据主体的权利义务，并明确对违反义务行为的经济处罚；（2）数据受托人义务。该法规定，数据受托人应当遵守以下义务：采取安全保障措施防止个人数据泄露、向受影响的数据主体和数据保护委员会通报个人数据泄露情况、实现处理目的后及时删除数据、撤销同意后删除个人数

据、建立申诉系统回复数据委托人的问询、履行被认定为重要数据受托人的额外义务，例如任命数据审计员并定期进行数据保护影响评估；（3）儿童个人数据保护。该法要求数据受托人仅在父母同意的情况下处理儿童的个人数据，且不允许进行有损儿童福祉或基于跟踪、行为监控或投放定向广告为目的的数据处理。（来源：印度政府）

3. 美国 CISA 即将出台关键基础设施网络事件报告规则

8 月 12 日，美国网络安全和基础设施安全局（CISA）局长表示，CISA 正在根据《关键基础设施网络事件报告法》规定的职权，制定关键基础设施网络事件报告规则，要求关键基础设施所有者和运营商披露赎金支付情况和网络安全事件情况。2022 年 3 月，拜登签署《关键基础设施网络事件报告法》，明确关键基础设施实体报告网络事件的流程及基本要求，规定该法所管辖的实体必须根据 CISA 发布的规则，留存与网络事件和赎金支付有关的信息。CISA 目前正处于编写规则细节的最后阶段，预计规则将于明年发布并实施。（来源：TheRecord 网站）

4. 约旦国王批准《网络犯罪法令》

8 月 12 日，约旦国王批准《网络犯罪法令》，法令将在约旦宪章报上发布 1 个月后生效。法令规定一系列网络犯罪行为及相应刑事责任。约旦境内任何人在网络上发布带有煽动国内叛乱、冲突、仇恨或暴力等内容的信息，将被判处 1 至 3 年监禁，或面临 5000 至 2 万约旦第纳尔罚款，或两

者并罚。任何人故意在网上发布虚假或诽谤他人的信息，将面临不少于3个月的监禁或5000至2万约旦第纳尔罚款，或两者并罚。（来源：约旦总理部）

5. 英国内阁发布《2023年国家风险登记报告》，指出英国关键基础设施有高达5%-25%的概率遭遇重大网络攻击

8月3日，英国内阁发布《2023年国家风险登记报告》，列举被确定为对英国安全与关键系统产生重大影响的89种威胁，为增强英国集体防御能力提供坚实基础。报告将网络领域威胁列为英国面临的仅次于恐怖主义的威胁，指出网络攻击风险日趋复杂化，可能会对多个经济领域造成重大损害。未来两年，英国关键基础设施有高达5%-25%的概率遭遇重大网络攻击，包括天然气基础设施、电力基础设施、民用核设施、燃料供应基础设施、政府机构、卫生保健系统、交通运输系统和电信系统。为此，英国政府将制定全面计划，增强针对特定风险的抵御能力，发布《国家网络战略》《英国能源安全战略》，制定社区风险登记册，重点关注各区域内的最大风险。（来源：英国政府）

6. 英国、瑞士多地发生警察局数据泄露事件

8月8日，北爱尔兰警察局（PSNI）发生一起个人信息泄露事件，源于警员在信息自由（FoI）网站寻求有关北爱尔兰警察局各级警官和工作人员人数的信息时，将请求信息与包含所有员工的姓氏、姓名缩写、工作地点

和部门的源数据一并发送，导致超过1万名警察和工作人员的个人信息被公开。8月9日，英国信息专员办公室针对此事发表声明，要求PSNI紧急采取适当行动，并将与PSNI合作确定风险级别和缓解措施。

8月15日，英国诺福克和萨福克警察局发表声明证实，警方在2021年4月至2022年3月期间回应信息自由（FOI）犯罪统计数据请求的回复中，因技术问题导致受害者、证人和嫌疑人的个人身份信息及犯罪描述信息被意外泄露。警方表示，对受影响数据的全面分析已经完成，并开始通过邮件、电话联系1230名数据被泄露的人员，提供受影响个人数据情况及寻求进一步帮助的方式等必要信息。萨福克警察局长助理对这起事件的发生表示歉意，并向公众保证将确保警察局控制下的所有数据都得到适当保护。

8月18日，瑞士伯尼尔警方发言人证实，身份不明的黑客已成功获取瑞士伯尔尼州警察局所有2800名员工的姓名和手机号码。此次数据泄露是由警方在智能手机上普遍使用的MobileIron应用程序中存在的安全漏洞导致的。MobileIron是一款在许多国家及地区广泛使用的应用程序，旨在确保公司或组织员工可将其移动设备安全连接到雇主的服务器。瑞士国家网络安全中心此前于7月21日向伯尔尼警方通报MobileIron存在安全漏洞。尽管漏洞问题很快得到解决，但泄露的信息已经被导出。伯尔尼警方表示，目前黑客获取的数据未广泛传播，并已启动侦查。（来源：英国信息专员办公室、英国诺福克和萨福克警察局、布鲁塞尔时报）

7. 美国国防部宣布成立生成式人工智能工作组

8 月 10 日，美国国防部宣布成立生成式人工智能特别工作组“利马工作组”，致力于实现负责任的人工智能应用。在美国首席数字和人工智能办公室领导下，工作组将利用、评估和发展整个国防部的生成式人工智能能力，确保国防部在维护国家安全的同时保持全球尖端技术使用的前沿地位。工作组将利用国防部、情报界和其他政府机构之间的合作伙伴关系，致力于在整个国防部内推行生成式人工智能计划的同时最大限度降低应用安全风险。（来源：美国国防部）

8. 特斯拉“大规模”数据泄露事件原因查明：系内部员工所为

8 月 17 日，美国缅因州总检察长办公室发布有关特斯拉公司数据泄露的通知，指出特斯拉公司今年 5 月份发生的数据泄露事件系因“内部不法行为”引起，并已影响超过 7.5 万人，包括 9 名缅因州居民。8 月 18 日，特斯拉在向受影响用户发送的一封附有数据泄露通知的信函中表示，一家名为《德国商报》的媒体于今年 5 月 10 日通知特斯拉，称有人给该报提供了大量来自特斯拉内部的保密信息。经过特斯拉调查发现，系两名前特斯拉员工违反特斯拉的 IT 安全和数据保护政策，盗用包括现任和前任员工的姓名和联系信息，并将其分享给媒体，有超过 7.5 万人在这次事件中被影响。特斯拉在信函中表示已经采取行动控制事件以保护个人信息，并且已对两名泄密的前员工提起诉讼，目前已获得禁止两名被告进一步使用、访问或传播数据的法院命令。

据媒体报道，《德国商报》此前虽表示不会发布获取到的个人信息，也不会违法使用这些信息，但仍披露了数据泄露中的部分情况。该报称，被泄露的信息数据量多达100G，里面不仅有大量在职员工和前员工的个人信息（含姓名、住址、电话、电邮、薪资）——包括特斯拉老板马斯克自己的社保号码也在其中，也有客户的银行信息等个人信息，还有2400条对特斯拉车辆突然加速问题的客户投诉，以及1500条对刹车问题的投诉等。（来源：美国缅因州总检察长办公室）

9. 美国检察官办公室发起民事司法没收，追回诈骗活动涉及的加密货币

8月24日，美国检察官办公室发起民事司法没收，以追回加密货币。这些加密货币是针对马萨诸塞州居民的商业电子邮件泄露（BEC）诈骗活动的犯罪所得及其收益。政府试图没收从加密货币交易所币安美国账户中扣押的18.836比特币，估值约为50万美元。

2022年6月起，美国检察官办公室开始调查一系列针对马萨诸塞州居民的BEC诈骗活动。在BEC诈骗活动中，犯罪分子通常入侵企业用于发送商业、房地产和其他金融交易信息的电子邮件账户，冒充预期会从这些交易中收到款项的个人，要求将付款汇往犯罪分子控制的一系列银行账户。（来源：美国司法部）

10. 美国 CISA 发布首份《漏洞披露政策平台年度报告》，强制漏洞披露成为最佳实践

8 月 25 日，美国网络安全和基础设施安全局（CISA）发布首份《漏洞披露政策平台年度报告》，表示漏洞披露共享服务已帮助参与的联邦机构发现并解决 1000 多个可能被黑客利用的漏洞。年度报告指出，迄今为止，漏洞披露政策平台已有 40 多项机构漏洞披露计划。截至 2022 年 12 月，研究人员向平台上报 1300 多个已验证的漏洞。相关机构已修复 84%的上报漏洞，平均修复时间为 38 天。在 1300 多个被确认为有效披露的漏洞中，有 192 个是最危险的关键漏洞，82 个是严重漏洞，757 个是中等漏洞，299 个是低级或信息性漏洞。（来源：美国CISA）

行业前沿观察一：2023 调查活动启动

导读：9 月 12 日，2023 网民网络安全感满意度调查活动新闻发布会暨样本采集启动仪式在京召开，国内调查范围最大、参与人数最多的全国网络社会调查活动正式开启。

关键词：调查活动，新闻发布会

1. 2023 网民网络安全感满意度调查活动正式启动

9 月 12 日，2023 网民网络安全感满意度调查活动新闻发布会暨样本采集启动仪式在京举行，宣布调查活动于 9 月 13 日 0 时-22 日 24 时开展，为期 10 天，正式面向广大网民征集上网用网体验，广泛收集意见建议，为维护网络安全献计献策。为确保调查活动顺利进行，在此之前的 8-9 日，组委会组织发起单位和网安联志愿服务站进行了内测，10 日是演练，11-12 日公测。全国 135 家发起单位在发布会上同步举行样本采集工作启动仪式，志愿服务团队代表集体宣读《网络安全志愿服务倡议书》，呼吁更多的人加入志愿服务，共建清朗网络空间，守护精神家园。

调查活动组委会主任，公安部第一、三研究所原所长严明主持活动，组委会副主任，公安部网络安全保卫局原常务副局长、北京网络安全行业协会会长袁旭阳，北京市民政局社会组织管理中心一级调研员宋学懂，中国网络社会组织联合会研究部负责人，中国网络空间安全协会国际合作与研究部负责人徐玉蓉，北京网络空间安全协会副理事长林勇忠，以及贝壳找房、腾讯企鹅有调、虎牙直播等互联网企业代表等领导及嘉宾，志愿服务团队代表出席发布会，全国 135 家共同发起单位在视频分会场同步参会。新华社、人民网、中国新闻网、中国网、光明网、法治日报、中国消费者报、南方都市报、北京日报、北京商报等全国十多家主流媒体参加新闻发布会并进行相关报道。（来源：网安联）

2. 新闻发布会与会嘉宾高度评价调查活动

与会嘉宾在新闻发布会上的致辞中，对网民网络安全感满意度调查活动给予了高度评价和充分认可。

宋学懂：是社会组织参与社会治理的一种创新

北京市社会组织管理中心一级调研员宋学懂从社会组织行业主管部门的角度对调查活动表示充分肯定。

他认为，5 年来调查活动为政府和相关研究机构提供可靠的一手材料，为网络安全建设作出了突出贡献。调查活动是社会组织开展的公益性社会活动，具有广泛的社会影响力，彰显了社会组织在经济社会建设和科技发展中的重要作用。随着调查活动的深入开展，逐步形成了一直志愿服务队伍。通过广泛发动社会志愿团队，在学校、社区等地建立起志愿服务站，以此为依托，开展志愿服务，以调查活动为契机，把网络安全宣传工作送到群众身边；同时建立起了公益讲师服务体系，为志愿团队免费培养宣传人才，为志愿服务提供人才保障，开展常态化网络安全宣传，这是社会组织参与社会治理的一种创新。

袁旭阳：已成为社会调查知名品牌

调查活动组委会副主任、公安部网络安全保卫局原常务副局长、北京网络行业协会会长袁旭阳表示，经过组委会五年来的不懈努力，网民网络安全感满意度调查活动，已成为众多社会调查问卷调查活动中的一个比较知名的品牌，成为了网络安全社会公益活动中的一件大事，他呼吁全国广

大网民积极踊跃参与到问卷采集工作当中来，将自己上网用网的体验感受反馈给国家相关政府部门。

袁旭阳表示，北京网络行业协会作为调查活动核心发起单位，是全国135家调查活动发起单位之一，与调查活动一起走过了第一个辉煌五年，一起推动国家网络空间安全建设，一起践行了网络安全为人民、网络安全靠人民的重要思想。北京网络行业协会将一如既往地全力投入到北京地区样本采集工作中，今年的样本采集量争创历史新高，为国家网络安全建设和共筑清朗网络空间环境贡献力量。

中网联：是深入贯彻总书记重要指示的生动实践

中国网络社会组织联合会（简称“中网联”）研究部负责人出席活动，对调查活动的顺利启动表示热烈祝贺，对调查活动组委会每年给予中网联《中国网络诚信发展报告》的支持表示衷心感谢。他在致辞中表示，网络安全事关国家安全和社会稳定，事关人民群众切身利益。由网安联牵头，全国135家网络安全社会组织及相关机构共同发起的网民网络安全感满意度调查活动，是深入贯彻落实习近平总书记关于“网络安全为人民，网络安全靠人民”重要指示的生动实践，也为国家和相关部门开展互联网治理与监管提供了网情民意支持。

中网联代表表示，继去年在整个调查活动中成功开展“网络诚信建设专题”调查之后，今年再次设置此项专题调查内容，这是对整个调查活动内容的有力拓展和丰富。去年有36万网民参与了网络诚信建设调查，取得了丰硕成果，相关调查数据被引用到《中国网络诚信发展报告2023》，并

在2023年中国网络文明大会网络诚信建设高峰论坛上成功发布，引起了社会广泛反响。希望社会各界、广大网民朋友继续踊跃参与“网络诚信建设专题问卷调查”，力争取得更多高质量调查成果。

该负责人表示中网联将继续重视支持、参与国家网络安全方面的社会公益活动，希望组委会认真组织专题调查，深入搞好宣传发动，积极做好成功运用，以丰富的调查成果为编制发布《中国网络诚信发展报告2024》提供有效的数据支撑，为共建网上美好精神家园，加快网络强国、数字中国建设作出新的更大贡献。（来源：网安联）

3. 时新•十新：盘点本届调查活动十大创新亮点

采集时间新。为方便各年龄层特别是学生群体参与答题，同时方便各参与单位结合国家网络安全宣传周工作开展活动，2023调查活动问卷采集时间由往年的八月份改到了九月份中旬开展。

测试环境新。通过优化组织团队和平台，2023调查活动新增了很多强有力的发起单位，同时首次启用了新的问卷采集系统。为帮助各采集单位熟悉采集流程，让网民群众对活动及问卷采集有更清晰的了解，同时进一步深化问卷系统个性化服务，2023调查活动增加内测、演练、公测环节。

组织团队新。除了网络安全行业协会及相关机构，2023调查活动还组织全国范围内各省市的网安联•网络安全志愿服务站、志愿团队、志愿者、公益讲师、公益宣传员等，深入基层，开展“五进”活动，进机关、进网站、进企业、进校园、进社区，同步启动问卷调查，服务最广大人民群众，

让网络空间安全意识深入人心，在全国形成一道志愿服务靓丽风景线。

宣讲团队新。组委会联合网安联认证中心，为符合条件的公益讲师提供国家级免费认证，为全国建设一支网络安全高素质公益宣讲团奠定基础，为调查活动和网络安全知识的常态化宣传助力。

激励机制新。2023 调查活动从物资奖励到精神鼓励，设计了多层次立体激励机制。组委会为了进一步推动调查活动的采集工作，确保样本的质与量双提升，一方面在组织层面制订了更加完善科学的组织、宣传补贴政策，为各地开展工作提供后勤支撑。另一方面通过网安联小程序开发更加多样化、个性化服务功能，让组织者、参与者能更方便、快捷了解自身的采集情况和补贴情况。

问卷体系新。在当前国内外新形势新变化的大背景下，2023 年调查问卷内容更突出安全与发展的核心主题，选题方向以公众期望和主管部门治理工作需求为导向，关注治理成效和人民群众的实际感受。

热点专题新。2023 调查活动的热点专题问卷，将围绕数字经济发展方向进行调研，紧跟社会时势，聚焦民生热点。力求客观、全面地收集网民需求及评价意见，及时了解和掌握最新的网情民意，为开展相关课题研究打下坚实基础。

支撑平台新。为更好更高质量地支撑 2023 调查问卷的样本采集以及调查活动各阶段的工作开展，今年的调查问卷系统、活动官网（网络安全共建网）、网安联小程序进行了升级和改版。问卷系统框架优化，使用更加人性化答题，题目展示方式和断点续答进一步加强，并打通了小程序播报

系统。“网安联”小程序作为支撑调查活动和网安联志愿服务工作的综合性多功能公益平台，设置“2023 调查活动”“数据播报”“百问百答”“报告查询”“证书下载”等专栏，系统性展示活动有关内容，打通活动相关服务通道。

答题奖品新。2023 调查活动答题公益奖品新增“网安联积分”奖励。网安联积分在网安联小程序公益店兑换公益礼品，也可以通过小程序打通的第三方商城兑换京东和苏宁易购等购物平台的商品。

数据势能新。全新整合数据库，结合网安联博士工作站势能，以网安大数据服务社会公益。依托网安联博士工作站和广东新兴国家网络安全和信息化发展研究院，联合国内各大知名高校研究院所，加大数据分析和挖掘力度，今年新鲜出炉的调查报告将更值得期待。（来源：网安联）

行业前沿观察二：调查活动精彩纷呈

导读：9 月 12 日，2023 网民网络安全感满意度调查活动新闻发布会暨样本采集启动仪式在京召开，全国各地网络安全协会和社会组织在地方党政机关的支持下，发挥主观能动性，积极主动开展调查活动，调查活动开展得有声有色、精彩纷呈。

关键词：调查活动，新闻发布会

1. 广州天河：联合网警街头讲座，调查采集群众点赞

广州天河区以“网络安全为人民，网络安全靠人民”为主题的国家网络安全宣传周重要活动，在繁华的天河南步行街志愿驿站举行。

当天，天河区网警精心为志愿者们提供了一场的网络安全教育讲座。这次讲座旨在增强志愿者们的网络安全意识，教育他们如何预防网络诈骗等安全问题。网络警察们以案例分析和实际操作演示，生动地介绍了网络诈骗的常见手法和防范方法，引导志愿者们更好地保护自己和身边的人，同时引导大家填写“网民网络安全感满意度调查”的问卷。

讲座结束后，志愿者们迅速投入到宣传工作中。他们分发了丰富的宣传资料，向路过的市民详细介绍了网络安全的重要性和防范措施。志愿者们用自己的实际行动传播网络安全知识，邀请群众填写“网民网络安全感满意度调查”的问卷，一些群众为活动点赞，表示会将网络安全的理念传递给更多人，系列活动强化了社会对网络安全的关注和重视。

这次广州天河区的国家网络安全宣传周活动充分展示了网络安全的重要性，通过教育和宣传，人们更加清晰地认识到了网络安全不仅仅是个人问题，更是全社会的责任。希望这样的宣传活动能够持续开展，让更多人受益，共同维护网络安全的大环境。（来源：广州网络空间安全协会）

2. 河北衡水：开展网络安全宣传同步进行调查样本采集

9 月 13 日，河北衡水好人志愿者协会在共青团衡水市桃城区委和衡水市公安局桃城分局反诈中心的支持指导下，举办国家网络安全宣传活动，积极引导广大网民遵德守法、文明互动，提升网络文明素养，净化网络环境，共创、共享天朗气清、生态良好的网络空间。

2023年网民网络安全感满意度调查活动作为当天宣传活动的重头戏隆重推出，在志愿者的宣传引导下，市民纷纷扫描答卷，参与活动，携手并肩一起维护好亿万网民的共同精神家园，营造积极健康、向上向善的清朗网络空间。（来源：衡水好人网）

3. 黑龙江：调查活动启动仪式上省网络安全志愿者服务队成立

9月12日，2023网民网络安全感满意度调查活动启动仪式在哈尔滨召开，黑龙江省网络安全志愿者服务队宣告成立。黑龙江省公安厅网安总队相关领导、黑龙江省网络安全协会领导、新闻媒体及网络安全行业代表、黑龙江省网络安全志愿者服务队代表等60余人参加。

黑龙江省网络安全志愿者服务队是黑龙江省网络安全协会根据当前信息网络安全宣贯及社会服务需要而成立的。作为政府公共服务及行业延伸到基层的工作平台，将配合有关党政部门开展网络安全治理，推动基层网络安全宣传教育工作，畅通群众网络安全求助和维权举报渠道。

黑龙江省网络安全志愿者服务队成立后，作为黑龙江省网络安全协会向广大网民推广网络安全知识的重要依托力量，将通过志愿服务的形式开展工作，提高网民网络安全意识及防范能力，畅通投诉举报渠道，引导广大网民尊德守法、文明互动、理性表达，提升全社会的网络文明素养，净化网络环境，不断增强网民群众的获得感、幸福感、安全感。

在活动仪式上，孙甲子会长向志愿者服务队颁发了黑龙江省网络安全志愿者服务队队旗和服装。启动会还对2022黑龙江网民网络安全感满意度调查活动进行了总结和表彰，对今年的调查活动进行了部署。（来源：央广网）

4. 河南平舆：星火志愿者协会调查活动启动首日采集量破 2000 份

9 月 13 日，2023 网民网络安全感满意度调查活动正式启动，河南省平舆县星火志愿者协会在总负责人白望明带领下，60 多名志愿者共分五个小队，线上线下协作，进社区、进学校、进企业、进养老机构、进医院，当天采集量突破 2000 份，取得阶段性成果。

活动当天，协会动员星火志愿者各个分队通过身边家庭成员，及所在微信群，进行一对一，一对多样本采集，并通过志愿者教师身份动员学生家长及教师内部广泛采集。线下采集主要在广场、社区、医院、商场等公共场所周边，通过发放宣传单，填写问卷奖励毛巾、围裙等小礼品的形式进行采集工作。

经过所有志愿者的辛苦努力，通过本次调查活动，让更多的人针对网络空间安全知识、网络文明等更加深入了解。

协会负责人白望明表示：通过网络安全项目来服务社会和推动网络安全发展，拓展了协会的服务社会的能力。星火志愿一直在用志愿者的执着与快乐，带动和感染周围更多的朋友参与到维护安全网络的志愿服务中，把“我志愿、我奉献、我快乐”的精神一直传承下去。（来源：网安联）

5. 广西南宁：调查活动启动仪式在广西信息职业技术学院成功举办

9 月 13 日“2023 年国家网络安全宣传周科普进校园广西活动暨 2023 全国网民网络安全感满意度调查（广西）活动”启动仪式在广西信息职业技术学院成功举办。

南宁市公安局网络安全保卫支队副支队长唐世竞，南宁市大数据发展局四级调研员肖继世，南宁市委网信办网络安全和信息化发展协调科副科

长吴廷才，广西信息职业技术学院副校长黄河，广西互联网协会常务副秘书长黎东勇，南宁市信息网络安全协会秘书长何毅，南宁市信息技术学会党支部书记、副会长兼秘书长毛宁等主办方领导出席仪式，还有来自广西信息职业技术学院师生代表以及主办方邀请的关心广西网络安全事业的各企业嘉宾代表共计200人参加本次启动仪式。

会上，嘉宾与参会师生共同参加2023年全国网民网络安全感满意度调查问卷的填写，共同参与调查活动，就关心的网络安全问题提出了宝贵意见和建议。

本次活动是在南宁市大数据发展局、南宁市科学技术协会、南宁市公安局网络安全保卫支队共同指导下，广西互联网协会、南宁市信息网络安全协会、南宁市信息技术学会联合主办，广西信息职业技术学院承办，并得到了广西信息化发展组织联合会、广西长泰网络报警服务有限责任公司、深圳昂楷科技有限公司、南宁赛鸣信息技术有限公司的大力支持。（来源：南宁市信息技术学会）

6. 贵州贵阳：借网络安全宣传周东风，迅速掀起调查活动热潮

9月13日，贵州省贵阳市信息网络安全协会借网络安全宣传周东风，结合网安技术展会员单位参展多、观众多、从业人员多等实际，启动网民网络安全感满意度调查活动，取得良好宣传效果。

协会组织会员参展企业以宣传实物、视频呈现等多种形式，展示技术实力，增加答题量，并在贵州主流媒体贵州日报天眼新闻和多彩贵州网众望新闻宣传报道，迅速掀起了调查活动的热潮。

协会负责人表示，今年的贵阳市信息网络安全协会认真组织，精心安全，力争在去年的基础上，总结经验，扩展思路，创新做法，发动更广大

的会员参与活动，影响更多的社会群体参加，确保今年的调查活动和网络安全宣传活动取得实效。（来源：贵阳市信息网络安全协会）

7. 山东滨州：星火公益志愿者走上街头发动群众参加调查活动

9 月 17 日至 22 日，山东滨州星火公益事业发展中心积极组织发动 2023 网民网络安全感满意度调查活动，志愿者走上街头，广泛发动群众参与活动，取得实效，获社会各界好评。

2023 网民网络安全感满意度调查活动开展期间，山东滨州星火公益事业发展中心通过参加网络视频会议学习，参与志愿者分享等形式，深入了解调查活动的意义和具体的做法，在积极学习其他省市志愿团队先进经验的基础上，结合滨州实际，组织志愿者持续六天走上街头宣传网络安全知识，引导群众参与调查活动。志愿者主动向市民宣传“网民网络安全满意度调查活动”相关内容，让更多网民了解活动的意义并参与，积极主动扫描答卷参与活动。

公益无大小、行动即力量。滨州星火公益的志愿者们将以实际行动，助力网络安全。（来源：山东滨州星火公益事业发展中心）

8. 福建安溪：志愿者积极参与调查活动赢得好评

2023 网民网络安全感满意度调查活动启动后，福建安心义工协会组织志愿者走上街头、走进店铺，发动社会各界群众扫码答卷，在参加调查活动的过程中，帮助广大群众学习网络安全知识，提升网络安全防范技能，获得社会各界一致赞誉。

福建安心义工协会今年是首次参加活动，在活动组委会的精心辅导下，快速掌握了样本采集的方法，以小组为单位走上街头，发动群众答卷，同时宣传网络安全知识，人人对他们竖起大拇指。（来源：福建安心义工协会）

9. 云南：2023 调查活动实现质的突破

为全面了解、反映广大网民对我国网络安全状况的感受和看法，向各级党政有关部门开展互联网治理与监管提供详实的网情民意支撑，云南省2023 网民网络安全感满意度调查活动于 9 月 13-22 日正式开展样本采集工作，面向广大网民征集意见。

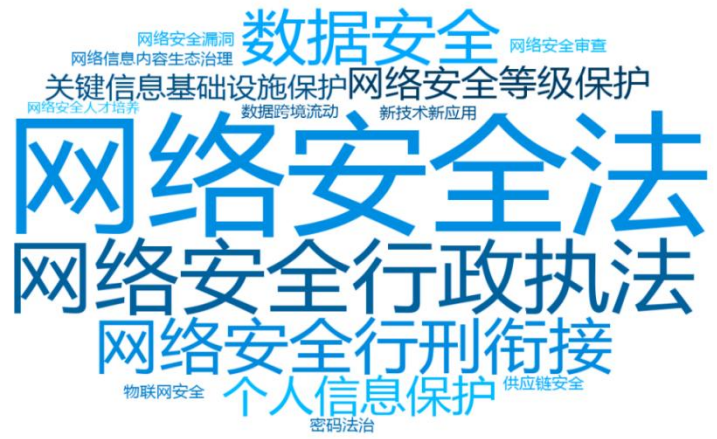
2023 年是全面贯彻党的二十大精神开局之年。在全党全国上下践行“大兴调查研究之风”的大背景下，网民网络安全感满意度调查活动（以下简称“调查活动”）启动第二个五年计划，传承第一个五年“聚焦网民关切，探索网安方向”宗旨思想，以“奉献友爱，互助进步；守护网络安全，共建网络文明”为宗旨开启新里程。

云南省调查活动服务总队、发起单位采用网信办和公安发文、国家网络安全宣传周、协会网站、公众号等形式广泛宣传，各志愿者站、支持单位、网络安全协会会员单位落地落实网安调查，达到网络安全宣传教育的作用。通过大家一致努力，云南省的 2023 年的调查总份数有望冲破一万大关，比起去年 699 份数实现了质的突破。（来源：昆明市网络安全协会 衡利英 供稿）

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

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

……