网安联
Wang An Lian

网络与数据安全监管前沿洞察

Frontiers of Regulatory Oversight in Cyber Security and Data Governance

2023年8月 第1期（总第1期）

2023年7月31日

主办单位：公安部第三研究所网络安全法律研究中心
联合主办：北京网络空间安全协会网安联发展工作委员会
协办单位：网安联认证中心
技术支持：北京关键信息基础设施安全保护中心
广东关键信息基础设施保护中心

声明：本刊定位于网络与数据安全前沿动态梳理，侧重全面跟踪、及时掌握，如需针对特定领域或前沿动态进行针对性专题研究，请将需求发送至以下邮箱：cinsabj@163.com。

目　录

境内前沿观察一：安全态势

导读：本月，武汉市应急管理局所属武汉市地震监测中心部分地震速报数据前端台站采集点网络设备遭受境外组织的网络攻击。武汉市公安局江汉分局已根据《刑法》第285条之规定立案侦查，经初步判定，此事件为境外具有政府背景的黑客组织和不法分子发起的网络攻击行为。

此外，中国人民大学部分学生信息被非法获取一案引发关注，经查系本校毕业生利用专业技术盗取了全校学生个人信息，并搭建给全校学生颜值打分的网站，目前该生已被北京市公安局海淀分局依法刑事拘留，案件正在进一步调查中。

关键词：境外网络攻击、个人信息非法获取

1. 中国人民大学部分学生信息被非法获取

7 月 2 日，中国人民大学通过微博账户“中国人民大学”发布通报称部分学生信息被非法获取，学校对此高度重视，第一时间联系警方并积极配合警方等相关部门开展调查，学校强烈谴责侵犯个人隐私、危害信息安全的行为。

据报道，该校毕业生马某某在读硕士研究生期间，利用专业技术盗取全校学生个人信息，包括照片、姓名、学号、籍贯、生日等，并搭建了给全校学生颜值打分的网站。该毕业生还曾在个人社交账号上发布动态公开此事。

7 月 3 日，北京市公安局海淀分局通过微博账户“平安北京海淀”发布通报称，已初步查明犯罪嫌疑人马某某涉嫌非法获取中国人民大学部分学生个人信息等违法犯罪行为，目前马某某已被北京市公安局海淀分局依法刑事拘留，案件正在进一步调查中。（来源：新民晚报）

2. 武汉地震设备遭境外黑客网络攻击，警方已立案侦查

7 月 26 日，武汉市应急管理局发布消息称，国家计算机病毒应急处理中心和 360 公司近期向武汉市应急管理局通报，经上述机构监测发现，武汉市应急管理局所属武汉市地震监测中心部分地震速报数据前端台站采集点网络设备遭受境外组织的网络攻击。在此，武汉市应急管理局公开声明：我单位及武汉市地震监测中心高度重视网络安全防护工作，坚决反对任何

组织或个人以任何形式对我实施网络攻击，任何危害地震监测基础设施的行为都将被依法追究相关法律责任。为进一步查明事实，依法处理相关幕后黑客组织和不法分子的网络攻击行为，武汉市地震监测中心第一时间封存相关网络设备，并将遭受网络攻击的情况向辖区公安机关报案，我单位将保留进一步追诉的权利。

同日，武汉市公安局江汉分局发布警情通报。通报指出，25 日，武汉市应急管理局地震监测中心报警称，该中心发现部分地震速报数据前端台站采集点网络设备被植入后门程序，该行为对国家安全构成严重威胁。武汉市公安局江汉分局根据《刑法》第 285 条之规定立案侦查，并对提取到的后门样本进一步开展技术分析，该后门程序能非法控制并窃取地震速报前端台站采集的地震烈度数据。初步判定，此事件为境外具有政府背景的黑客组织和不法分子发起的网络攻击行为。（来源：央视网）

境内前沿观察二：立法动向

导读：本月，国家网信办、工信部、公安部、国家认监委发布公告，更新网络关键设备和网络安全专用产品目录，包括 4 类网络关键设备和 34 类网络安全专用产品。《生成式人工智能服务管理暂行办法》正式发布，明确提供和使用生成式人工智能服务总体要求。国家铁路局发布《铁路关键信息基础设施安全保护管理办法（征求意见稿）》，要求运营者应当按照国家有关规定对采取的安全保护措施予以验证。

浙江省经济和信息化厅发布《浙江省企业首席数据官制度建设指南（试行）》，鼓励在企业设置首席数据官，全面负责企业数据管理工作。北京市通信管理局发布《北京地区电信领域数据安全管理实施细则》，要求电信领域数据处理者应当按要求将识别出的重要数据和核心数据进行目录填报，并报北京市通信管理局备案。

关键词：网络关键设备和网络安全专用产品、网络暴力、人工智能监管、网络安全保险、个人信息出境标准合同

（一）监管部门立法

1. 四部委发布《关于调整<网络关键设备和网络安全专用产品目录>的公告》

7 月 3 日，国家网信办、工信部、公安部、国家认监委联合发布《关于调整<网络关键设备和网络安全专用产品目录>的公告》。公告指出，四部委对《网络关键设备和网络安全专用产品目录》予以更新，2017 年四部门联合发布的《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017 年第 1 号）中的网络关键设备和网络安全专用产品目录同步废止。

本次发布的目录包括路由器、交换机等 4 类网络关键设备，以及防火墙、入侵防御系统（IPS）、网络安全态势感知产品、数据泄露防护产品等 34 类网络安全专用产品。（来源：中国网信网）

2. 国家网信办发布《网络暴力信息治理规定（征求意见稿）》

7 月 7 日，国家网信办发布《网络暴力信息治理规定（征求意见稿）》，从适用范围、相关定义、监测预警、信息处置、保护机制等方面对网络暴力信息治理作出规定。

征求意见稿强调，网络信息服务提供者应当建立健全网络暴力信息分类标准和典型案例样本库，在区分舆论监督和善意批评的基础上，明确细化网络暴力信息标准，增强识别准确性。网络信息服务提供者应当向用户提供针对网络暴力信息的一键取证等功能，提高证据收集便捷性。依法依

规为用户维权，司法机关、有关部门调查取证工作等提供及时必要的技术支持和协助。（来源：中国网信网）

3. 中央网信办发布《关于加强“自媒体”管理的通知》

7月10日，中央网信办发布《关于加强“自媒体”管理的通知》，提出13项具体工作内容，分别是：（1）严防假冒仿冒行为；（2）强化资质认证展示；（3）规范信息来源标注；（4）加强信息真实性管理；（5）加注虚构内容或争议信息标签；（6）完善谣言标签功能；（7）规范账号运营行为；（8）明确营利权限开通条件；（9）限制违规行为获利；（10）完善粉丝数量管理措施；（11）加大对“自媒体”所属MCN机构管理力度；（12）严格违规行为处置；（13）强化典型案例处置曝光。

具体来说，通知要求网站平台应当强化注册、拟变更账号信息、动态核验环节账号信息审核，有效防止“自媒体”假冒仿冒行为。对账号信息中含有党政军机关、新闻媒体、行政区划名称或标识的，必须人工审核，发现假冒仿冒的，不得提供相关服务。网站平台应当及时发现并严格处置“自媒体”违规行为。对制作发布谣言，蹭炒社会热点事件或矩阵式发布传播违法和不良信息造成恶劣影响的“自媒体”，一律予以关闭，纳入平台黑名单账号数据库并上报网信部门。（来源：中国网信网）

4. 七部门公布《生成式人工智能服务管理暂行办法》

7月10日，国家网信办联合国家发展改革委、教育部、科技部、工信部、公安部、广电总局公布《生成式人工智能服务管理暂行办法》，对生

成式人工智能服务实行包容审慎和分类分级监管，明确提供和使用生成式人工智能服务总体要求。

办法提出生成式人工智能服务提供者应当依法开展预训练、优化训练等训练数据处理活动，遵守以下规定：（1）使用具有合法来源的数据和基础模型；（2）涉及知识产权的，不得侵害他人依法享有的知识产权；（3）涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形；（4）采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性；（5）《网络安全法》《数据安全法》《个人信息保护法》等法律、行政法规的其他有关规定和有关主管部门相关监管要求。

办法明确生成式人工智能服务提供者应当采取有效措施防范未成年人用户过度依赖或者沉迷生成式人工智能服务，按照《互联网信息服务深度合成管理规定》对图片、视频等生成内容进行标识，发现违法内容应当及时采取处置措施。（来源：中国网信网）

5. 工信部与国家金融监管总局联合发布《关于促进网络安全保险规范健康发展的意见》

7 月 17 日，工信部与国家金融监管总局联合发布《关于促进网络安全保险规范健康发展的意见》，围绕完善政策标准、创新产品服务、强化技术支持等提出五个方面十条意见。

意见指出，要健全网络安全保险标准规范。支持网络安全产业和保险业加强合作，建立覆盖网络安全保险服务全生命周期的标准体系，统一行

业术语规范，明确核保、承保、理赔等主要环节基本流程和通用要求。意见要求加强网络安全风险监测能力。开展网络安全保险全生命周期风险监测，覆盖事前、事中、事后等重要环节。鼓励网络安全企业、专业网络安全测评机构等充分发挥网络安全风险监测技术优势，充分利用安全技术手段，针对网络安全漏洞、恶意网络资源、网络安全事件等开展网络安全威胁实时监测，及时发现网络安全风险隐患，提升网络安全风险监测预警、应急处置等能力。（来源：工信部）

6. 国家铁路局发布《铁路关键信息基础设施安全保护管理办法（征求意见稿）》

7 月 18 日，国家铁路局发布《铁路关键信息基础设施安全保护管理办法（征求意见稿）》，从铁路关键信息基础设施认定、运营者责任和义务、保障和监督等层面对铁路关键信息基础设施安全保护作出规定。

征求意见稿明确，国家铁路局依法负责全国铁路关键信息基础设施安全保护和监督管理工作，是铁路关键信息基础设施安全保护工作部门。地区铁路监督管理局依据国家铁路局要求，开展相关工作。征求意见稿强调，新建、改建、扩建铁路关键信息基础设施的，运营者应当做到安全防护措施与关键信息基础设施同步规划、同步建设、同步使用。运营者应当按照国家有关规定对安全保护措施予以验证。（来源：国家铁路局）

7. 中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》

7 月 24 日，中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》，从数据分类分级、数据安全保护总体要求、风险监测评估审计与事件处置措施等方面对银行业务领域数据安全进行规定。

征求意见稿强调要规范数据分类分级要求，数据处理者应当建立数据分类分级制度规程，梳理数据资源目录标识分类信息，在国家数据安全工作协调机制统筹协调下，根据中国人民银行制定的重要数据识别标准，统一对数据实施分级，严格落实网络安全等级保护和风险评估等义务。

（来源：中国人民银行）

（二）地方层面动向

1. 多地网信办公布个人信息出境标准合同备案指引/备案通知

（1）福建

7 月 4 日，福建省网信办公布个人信息出境标准合同备案指引，适用于所在地为福建省的个人信息处理者。指引强调个人信息处理者备案个人信息出境标准合同时，应当严格按照《个人信息出境标准合同备案指南（第一版）》要求提交材料。个人信息处理者应自行或委托第三方开展个人信息保护影响评估，并根据评估情况进行整改。（来源：网信福建）

（2）湖北

7 月 5 日，湖北省网信办公布个人信息出境标准合同备案指引，适用于所在地为湖北省的个人信息处理者。指引强调个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带材料电子版的方式，向省网信办备案。个人信息处理者备案标准合同应按照《个人信息出境标准合同备案指南（第一版）》要求进行材料准备，包含自行或委托第三方进行个人信息保护影响评估的报告。（来源：网信湖北）

（3）河北

7 月 7 日，河北省网信办公布个人信息出境标准合同备案指引，适用于所在地为河北省的个人信息处理者。指引重申《个人信息出境标准合同办法》中的适用要求，强调个人信息处理者不得采取数量拆分等手段，将依法应当通过数据出境安全评估的个人信息通过订立标准合同的方式向境外提供。个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带电子版（PDF 格式、光盘刻录）的方式，向河北省网信办备案。（来源：网信河北）

（4）江苏

7 月 7 日，江苏省网信办公布个人信息出境标准合同备案指引，适用于所在地为江苏省的个人信息处理者。指引指出，备案主体须为法人实体，且备案主体应与境内合同签署方一致。如多家独立法人企业同属一家集团公司，可由集团公司作为个人信息出境标准合同备案主体。分公司不具备独立法人地位，不可代替总部或子公司备案。指引强调自 2023 年 6 月 1 日

起,个人信息处理者应当在标准合同生效之起10个工作日内进行备案,2023年6月1日前已经开展的个人信息出境活动，如适用《个人信息出境标准合同办法》且未履行相关规定的，应当在12月1日前完成整改。

（来源：网信江苏）

（5）广东

7月10日，广东省网信办公布个人信息出境标准合同备案通知，适用于所在地为广东省的个人信息处理者。通知强调个人信息处理者先将备案材料电子版提交所在地级以上市互联网信息办公室，经材料完整性检查后，由所在地级以上市互联网信息办公室送广东省互联网信息办公室。

（来源：网信广东）

2. 深圳市发改委发布《深圳市数据产权登记管理暂行办法》

6月15日，深圳市发改委发布《深圳市数据产权登记管理暂行办法》，包括总则、登记主体、登记机构、等级行为、管理与监督共七章34条。

办法创新明确数据产权登记适用范围，适用数据资源和数据产品在本市行政区域内的首次登记、许可登记、转移登记、变更登记、注销登记和异议登记行为，推动数据资源市场化流动和数据产品高效流通。办法创新提出数据确权方式，以政府规范性文件形式提出对数据产权登记行为进行规范管理，通过首次登记对数据资源或数据产品相关权利归属情况进行记录，探索开展数据确权工作。（来源：深圳市发改委）

3. 北京市发布《北京市智能网联汽车政策先行区数据分类分级管理细则（试行）》

7 月 3 日消息，北京市高级别自动驾驶示范区工作办公室近日正式发布《北京市智能网联汽车政策先行区数据分类分级管理细则（试行）》。

管理细则构建了多维统一的数据层级。要求相关单位全面理清自身数据资产形成数据资产识别清单，依据数据资产目录，按业务条线、业务属性等确立数据分类。管理细则细化国家数据安全法相关规定，将影响对象明确为六大类，区分四种危害影响程度，最终综合确认由低到高的 1-6 级数据级别。其中，个人信息定级不得低于 2 级，敏感个人信息定级不得低于 4 级。（来源：北京经济技术开发区）

4. 北京市经信局发布《北京市公共数据专区授权运营管理办法（征求意见稿）》

7 月 18 日，北京市经济和信息化局发布《北京市公共数据专区授权运营管理办法（征求意见稿）》。

征求意见稿指出，专区数据遵照“原始数据不出域，数据可用不可见”的总体要求，在保护个人隐私和确保公共安全的前提下开展授权运营。对不承载个人信息和不影响公共安全的公共数据，推动按用途加大供给使用范围。涉及个人信息、商业秘密的，在获得真实、有效、安全授权后按应用场景使用。专区运营单位应在专区监管部门的监督指导下，建立健全安

全管理制度，建立职能清晰的运营团队，明确数据安全责任人，严格管理公共数据专区运营工作。（来源：北京市经济和信息化局）

5. 北京市通管局发布《北京地区电信领域数据安全管理实施细则》

7 月 24 日，北京市通信管理局发布《北京地区电信领域数据安全管理实施细则》，从基础性数据安全保护要求、数据全生命周期安全保护要求、支持与保障等方面对电信领域数据安全管理作出规定。

实施细则要求，电信领域数据处理者应当按要求将识别出的重要数据和核心数据进行目录填报，并报北京市通信管理局备案。电信领域数据处理者应定期开展数据安全审计，审计对象完整覆盖全部数据处理活动，审计发现问题需及时进行整改，并对审计及处置记录进行留存管理。重要数据处理活动应至少每半年开展一次审计，核心数据处理活动应至少每季度开展一次审计。（来源：北京市通信管理局）

6. 浙江省经信厅发布《浙江省企业首席数据官制度建设指南（试行）》

7 月 14 日，浙江省经济和信息化厅发布《浙江省企业首席数据官制度建设指南（试行）》，鼓励在企业设置首席数据官，全面负责企业数据管理工作。

指南鼓励企业在决策层设置首席数据官，全面负责企业数据管理工作，领导数据归口管理部门。条件暂不成熟的企业，可先由现任信息化主管领

导兼任首席数据官。鼓励将首席数据官制度的基本内容写入企业章程或列入企业管理制度，赋予首席数据官对企业重大事务的知情权、参与权和决策权。指南对企业首席数据官的岗位职责进行界定，主要负责制定和执行数据战略，协调各部门落实相关数据项目；整合企业内外数据，创新挖掘数据资产价值，用数据赋能社会经济发展；制定企业数据标准和政策，强化数据合规、数据治理等。（来源：浙江经信）

7. 广州市政务服务数据管理局发布《广州市数据条例（征求意见稿）》

7 月 21 日，广州市政务服务数据管理局发布《广州市数据条例（征求意见稿）》，包括数据权益保护、公共数据、数据要素市场、数据应用、数据安全等方面。

数据安全方面，征求意见稿确立数据安全管理原则，坚持安全和发展并重，建立健全分类分级、风险防范、应急处置等数据安全管理机制，鼓励研发数据安全技术，保障数据全生命周期安全，并实行数据安全主体责任制、建立健全数据分类分级保护制度和数据安全风险评估与监管体系，加强数据要素安全监管治理，保障数据安全。

（来源：广州市政务服务数据管理局）

8. 上海市杨浦区人民检察院、法院联合发布《企业数据合规指引》《个人信息保护指引》

7月7日，上海市杨浦区人民法院、上海市杨浦区人民检察院联合发布《企业数据合规指引》《个人信息保护指引》。

《企业数据合规指引》主要对企业的数据合规管理架构与风险识别处理规范作出规定，包括数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障等内容，督促企业对数据进行合规管理，有效惩治预防数据违法犯罪。

《个人信息保护指引》对处理个人信息的基本原则、合法前提、个人信息收集、提供与共享、存储与传输、自动化决策等方面内容作出规定。指引强调处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向境外提供个人信息等情形应事前进行个人信息保护影响评估，并对处理情况进行记录。（来源：上海高院）

境内前沿观察三： 执法实践

导读：本月，公安部通报全国公安机关维护国家网络和数据安全的举措成效情况，指出党的十八大以来，已累计对近 10 万家重点单位开展监督检查，下发整改通知书 20 余万份。广州警方全力推进“净网 2023”专项行动和夏季治安打击整治行动，上半年共循环检测全市 1000 余个重要信息系统，发现并通报 1100 余个安全隐患。国家网信办通报 2023 年上半年全国网信系统执法情况，累计约谈网站 5518 家。

广东、山东、重庆等地公安机关和网信部门公布多起网络与数据安全行政执法案件，涉及的违法行为集中在：（1）互联网网站未进行国际联网备案；（2）虚假撤销等级保护测评备案；（3）未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的措施；（4）信息系统存在弱口令；（5）管理员与普通用户权限未进行合理隔离；（6）未按法律法规要求建立健全全流程网络数据安全管理制度；（7）未组织开展网络数据安全教育培训；（8）未采取相应的技术措施和其他必要措施，保障网络数据安全；（9）未对公民敏感信息数据采取去标识化和加密保护；（10）服务器存在未授权访问的漏洞。

关键词：网络谣言、弱口令、安全漏洞、数据泄露、利用 AI 制作传播虚假信息

（一）监管工作进展

1. 中央网信办开展“清朗·成都大运会网络环境整治”专项行动

7月18日，中央网信办发布公告，决定自即日起开展为期20天的“清朗·成都大运会网络环境整治”专项行动。专项行动将围绕大运会举办，集中整治未经许可擅自开展互联网新闻信息服务活动，或者在名称、头像、背景、简介、直播间或短视频背景等环节假冒仿冒官方机构、新闻媒体等六大类突出问题。公告要求各地网信办要提高政治站位，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：网信中国）

2. 全国网信系统依法查处网上各类违法违规行为：累计约谈网站5518家

7月31日消息，国家网信办公布上半年网信系统执法概况。上半年全国网信系统结合开展“清朗”系列专项行动，依法查处网上各类违法违规行为，累计约谈网站5518家、暂停功能或更新网站188家，下架移动应用程序120款，关停小程序87款，会同电信主管部门取消违法网站许可或备案、关闭违法网站7704家，督促相关网站平台依法依约关闭违法违规账号39100个。

针对抖音、新浪微博等网站平台存在法律、法规禁止发布或者传输的信息问题，国家网信办指导属地网信办分别依法约谈相关网站负责人，责

令其限期整改，处置相关账号，从严处理责任人，并分别给予罚款行政处罚。针对快手、百度、腾讯微信、网易等网络平台履行主体责任不力，对其用户发布的信息未尽管理义务，造成淫秽色情、封建迷信、诱导充值、为劣迹艺人辩护等有害信息在网上传播问题，国家网信办指导属地网信办分别依法约谈相关网站负责人，责令其限期整改，处置相关账号，从严处理责任人，并分别给予罚款的行政处罚。（来源：网信中国）

3. 浙江省通过首家企业个人信息出境标准合同备案

7 月 10 日消息，浙邦贝液压机械(杭州)有限公司提交的个人信息出境标准合同通过浙江省互联网信息办公室组织的备案审核，这是浙江省首家通过订立标准合同实现个人信息合规出境的企业，标志着个人信息出境标准合同备案工作在浙江省正式展开。（来源：网信浙江）

4. 北京市委网信办召开 App 收集使用个人信息整改指导会

7 月 13 日，北京市委网信办会同国家互联网应急中心北京分中心组织召开整改指导会，向“闪送”、“顺丰同城急送”、“大麦”、“赶集直招”、“亿通行”、“黄油相机”等 10 家企业集中通报专项治理行动中检查发现的 App 违规收集个人信息问题，逐一下达《整改通知书》，指导企业开展产品合规改造，要求限期整改。

今年 5 月以来，市委网信办联合市通信管理局、市公安局、市市场监管局等部门在全市范围内持续开展 App 收集使用个人信息专项治理行动。

近期，市委网信办组织完成了本年度专项治理行动首轮监督检查工作，共对拍摄美化类、求职招聘类、邮件快件寄递类等58款下载使用量较大的App开展技术检测，检查发现“违反必要原则，收集与其提供的服务无关的个人信息”、“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”等问题较为突出。　　（来源：网信北京）

5. 公安部召开维护国家网络和数据安全工作新闻发布会：已累计对近10万家重点单位开展监督检查

7月6日，公安部召开维护国家网络和数据安全工作新闻发布会，通报公安部党委部署全国公安机关认真履行网络安全监管职责，严厉打击网络违法犯罪活动，切实维护国家网络和数据安全的举措成效情况。

发布会指出，公安部主要从以下方面推动网络和数据安全工作：（1）持续深化网络安全等级保护制度，筑牢网络安全基石；（2）深入推进关键信息基础设施安全保护工作，全力保障经济社会正常运转；（3）强化落实数据安全保护工作，为数字经济发展保驾护航；（4）全面加强网络安全监测预警和通报处置，构建完善通报预警体系；（5）持续开展网络安全监督检查和行政执法工作，筑牢网络安全防线；（6）严厉打击危害网络和数据安全违法犯罪活动，切实维护网络秩序和群众网络权益。

发布会指出，自2010年开始，公安部每年组织全国公安机关开展网络安全大检查，监督、指导重要行业部门落实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。党的十八大以来，累计对近10万家重点单位

开展监督检查，及时排查风险、堵塞漏洞、消除隐患、补齐短板，共下发整改通知书20余万份，健全、完善了我国网络安全保障体系，提升了我国网络安全防护能力水平。

同时，公安机关聚焦网络攻击活动新动向，跟踪网络攻击技术新特点，组织开展打击危害网络和数据安全犯罪等系列专项行动，依法严惩非法侵入、控制、破坏计算机信息系统等行为，并加强国际执法合作，联合打击境外黑客对我网络攻击活动，有力保障了关键信息基础设施、重要信息系统和数据安全。2022年，公安机关深入推进“净网2022”专项行动，侦办案件8.3万起，抓获一大批犯罪嫌疑人，切实维护网络秩序和群众合法利益。（来源：公安部网安局）

6. 公安部召开发布会通报网络谣言打击整治工作情况：整治互联网平台企业近8000家（次）

7月21日，公安部召开新闻发布会通报网络谣言打击整治工作举措成效情况。发布会指出，网络谣言打击整治专项行动期间，全国公安机关共侦办案件2300余起，整治互联网平台企业近8000家（次），依法关停违法违规账号2.1万余个，清理网络谣言信息70.5万余条，以强有力的实际行动整治网络谣言问题乱象，有效净化网络生态，积极营造清朗有序的网络环境。

主要措施包括：（1）依法严厉打击借热点事件编造传播谣言违法犯罪行为，共侦办此类案件500余起，约占案件总数的21%；（2）依法严厉打

击“网络水军”违法犯罪团伙，依法侦办“网络水军”案件130余起，抓获犯罪嫌疑人620余人；（3）加强网站平台源头综合治理。公安机关集中开展互联网安全监督检查和行政执法，同互联网企业、网站签订违法犯罪信息清理整治责任书，督导网站平台严格落实网络安全主体责任，对案件侦办中拒不配合、拒不履行主体责任和义务的网站平台，坚决开展“一案双查”工作，依法依规加大查处整治力度；（4）曝光典型案例加强普法宣传教育。

7月，公安部网安局公布网络谣言打击整治专项行动第二批、第三批，共计20起典型案例。江苏、湖南、云南、浙江、安徽、湖北、福建、天津、甘肃、吉林等地公安机关同样公布多起典型案例。（来源：公安部网安局）

7. 广州警方推进“净网2023”专项行动：循环检测全市1000余个重要信息系统

7月19日消息，广州警方全力推进“净网2023”专项行动和夏季治安打击整治行动，全链条打击“网络水军”等突出网络违法犯罪，全角度防范网络安全风险隐患，全网域整治网络违法有害信息，取得了显著成效，上半年广州警方共侦破网络主侦案件144起，抓获犯罪嫌疑人616人，依法刑事拘留503人。

同时，广州警方以网络攻防演练和网络安全执法检查为抓手，全面加强关键信息基础设施和重要信息系统网络安全风险隐患排查整治，今年上半年共走访检查重点单位1100余家次，循环检测全市1000余个重要信息

系统，发现并通报1100余个安全隐患，督促相关单位整改隐患、堵塞漏洞。对未履行网络安全职责、未落实网络安全保护技术措施的单位，依法作出行政处罚160余宗。

广州警方还开展打击整治网络谣言专项行动，全面加强涉“黄赌毒”、涉枪爆、涉网络诈骗等违法有害信息的清理整治。今年上半年，共清理网络谣言信息43000余条，关停违法违规账号58个，办理网络打谣案件18宗，抓获涉案人员18人。依法清理处置各类违法有害信息24万余条。

（来源：广州网警巡查执法）

8. 工信部通报31款侵害用户权益行为的APP

7月7日，工信部通报侵害用户权益行为的APP（SDK）（2023年第4批，总第30批）。通报指出，工信部近期组织第三方检测机构对群众关注的休闲娱乐、实用工具、出行服务等APP及SDK进行检查，发现31款侵害用户权益行为的APP。

通报APP所涉问题如下：（1）应用分发平台上的APP信息明示不到位；（2）违规收集个人信息；（3）强制用户使用定向推送功能；（4）APP强制、频繁、过度索取权限；（5）欺骗误导强迫用户；（6）超范围收集个人信息；（7）违规使用个人信息；（8）违规利用个人信息开展自动化决策；（9）收集个人信息明示告知不到位；（10）违规使用第三方服务。

（来源：工信微报）

9. 上海市通信管理局开展2023年上海市电信和互联网行业网络和数据安全检查

7月3日，上海市通信管理局发布通知，开展2023年上海市电信和互联网行业网络和数据安全检查。

此次检查对象为提供公共互联网网络信息服务的基础电信企业、互联网企业、域名注册服务机构。重点检查相关网络运行单位的重要网络单元及承载重要数据的信息系统，包括但不限于关键信息基础设施、通信网络基础设施、公共云服务平台、域名服务系统、工业互联网平台、标识解析系统、车联网应用服务平台、网约车信息服务平台等。

此次检查内容分为六个方面：（1）网络和数据安全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）车联网网络安全防护定级备案管理情况；（4）工业互联网企业网络安全防护情况；（5）网络数据安全保护落实情况；以及（6）个人信息和用户权益保护工作情况。

（来源：上海通信圈）

10. 上海市杨浦区人民检察院、法院联合发布《2018-2022年涉数字经济犯罪案件司法白皮书》

7月7日，上海市杨浦区人民法院、上海市杨浦区人民检察院联合发布《2018-2022年涉数字经济犯罪案件司法白皮书》。

白皮书统计了2018年至2022年杨浦区人民法院审理的涉数字经济犯罪案件，指出四年内共审结涉数字经济犯罪案件1157件共2158人，案件

数量总体呈现波动式上升趋势。涉数字经济犯罪呈现出平台化、智能化、网络化等特征，具体特点如下：（1）犯罪主体平台化，共同犯罪较多；（2）犯罪手段复杂化，危害后果难以估算；（3）涉案金额高、犯罪场域广、受害基数大。（来源：上海高院）

11. 中国消费者协会针对云存储安全启动消费监督工作

7 月 10 日，中国消费者协会针对云存储安全启动消费监督工作，中消协调查了当前手机应用市场上下载量较大、用户评论较为活跃的云存储服务应用程序，发现多数应用程序服务协议中均注明服务逾期后如不采取续费等措施，数据会被永久删除。

中消协就此向云存储服务公司及云存储服务消费者提出以下建议：（1）消费者收到云存储服务到期的信息，必须采取措施，否则逾期数据将会被永久删除；（2）云存储服务公司在消费者云存储服务使用时长到期前后，要通过多种有效方式提醒消费者；（3）云存储服务公司与消费者签订的服务协议中对“数据安全”的约定要显著明确，并注重公平；（4）倡导云存储服务公司通过分类分级划分市场、丰富业务内容、采取多种措施提升服务消费者能力。（来源：中国消费者协会）

（二）行政执法案例

1. 因未进行国际联网备案、未履行网络安全保护义务，山东烟台警方对一公司处以警告

7月4日消息，山东省烟台市公安局龙口网安大队近日工作发现，辖区某公司互联网网站未进行国际联网备案。在开展调查时，警方又发现该企业未对网站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工作措施，未履行网络安全保护义务。龙口市公安局根据《计算机信息网络国际联网安全保护管理办法》第十二条第一款、第二十三条之规定，依法对该企业给予警告，并责令限期改正。（来源：公安部网安局）

2. 因虚假撤销等级保护测评备案，广州某科技公司被处罚

7月18日消息，广州警方近日发现，广州某科技有限公司运营的“**智慧办公管理软件”未依法开展等级保护测评工作。该系统于2020年7月定级为三级等级保护系统并取得备案证明，却在依然正常投入使用的情况下撤销等级保护测评备案，在2021年度、2022年度均未依法开展三级系统的等级保护测评，未履行网络安全等级保护测评的法定职责。广州警方对该虚假撤销备案的违法行为给予警告的行政处罚，并责令限期改正。该案是全国首起对虚假撤销等级保护测评备案作出处罚的行政案件。

（来源：平安广州）

3. 因信息系统存在弱口令等问题，山东烟台警方对一热力公司进行处罚

7月4日消息，山东省烟台市公安局芝罘分局网安大队近日工作发现，烟台市某热力公司供热客服语音管理系统存在弱口令问题。该系统存储着辖区用户向公司反映的各类供热问题，信息内容具体包含用户姓名、联系电话、家庭住址、反映的具体问题等，涉及公民个人信息达18万余条。此外，该网站管理员和其他工作人员使用的密码均是弱口令，并且管理员和普通用户之间的权限也未进行合理的隔离，甚至系统未采取必要的安全保护技术措施进行防护。烟台市公安局芝罘分局根据《数据安全法》第二十七条、第四十五条第一款之规定，给予该企业警告处罚，并责令限期整改。

（来源：公安部网安局）

4. 因存在未授权访问漏洞，广东中山警方依据《数据安全法》对一公司作出处罚

7月6日消息，广东省中山市三乡公安分局鹤湾派出所近日在对辖区内的公司进行数据安全检查过程中，发现某信息科技公司疑似存在网络数据泄露隐患。通过询问相关责任人、调取网络设备日志信息、开展技术检测等方式，发现该公司在没有依法建立数据安全管理制度和操作规程等数据保护措施的前提下，对存储的公民敏感信息数据未采取去标识化和加密保护。通过现场检查，发现该公司用于存储公民敏感信息的服务器也存在未授权访问的漏洞，用户隐私数据存在泄露风险。中山市三乡公安分局依

据《数据安全法》第二十七条、第四十五条规定对该公司处以警告以及罚款5万元，对该公司负责人作出罚款1万元的行政处罚。

（来源：网信广东）

5. 因存在数据库泄露情形，重庆市网信办依据《数据安全法》对一公司作出处罚

7月31日消息，根据有关部门移交的线索，重庆市网信办近日对属地一科技公司涉网络数据安全违法行为进行立案调查。经查，该公司因业务开展，收集、存储、处理的网络数据量较大，但未按法律法规要求建立健全全流程网络数据安全管理制度，未组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施，保障网络数据安全等数据安全保护义务，且存在数据库数据泄露的情形。重庆市网信办依据《数据安全法》第二十七条、第二十九条、第四十五条之规定，对该公司作出责令限期改正，给予警告，并处10万元罚款的行政处罚。　　（来源：网信重庆）

6. 因违规处理消费者个人信息等行为，蚂蚁集团被罚没37.6亿

7月7日，国家监管总局公布金罚决字〔2023〕1号行政处罚决定书，针对蚂蚁科技集团股份有限公司存在的违法违规行为，国家金融监督管理总局依据《银行业监督管理法》《保险法》《消费者权益保护法》相关规定，对其处以没收违法所得112977.62万元，罚款263270.44万元的行政处罚，罚没共计376248.06万元。侵害消费者合法权益方面，蚂蚁集团的

违规行为包括存在引人误解的金融营销宣传行为，侵害消费者知情权；未按规定处理部分消费者个人信息等。　　（来源：国家金融监督管理总局）

7. 因安全措施不足导致网络安全事件，中信证券被警示

7 月 7 日，证监会深圳监管局公布〔2023〕102 号行政监管措施决定书，对中信证券股份有限公司采取出具警示函措施。决定书载明，中信证券股份有限公司在 2023 年 6 月 19 日的网络安全事件中，存在机房基础设施建设安全性不足，信息系统设备可靠性管理疏漏等问题。上述行为违反《证券期货业网络和信息安全管理办法》第十三条相关规定，因故对该公司采取出具警示函的行政监管措施。决定书强调，中信证券股份有限公司应对相关问题进行全面整改，于 3 个月内完成上述整改工作并向深圳监管局报送整改报告。　　（来源：深圳证监局）

8. 广东省茂名市公安机关查处利用 AI 技术编造传播虚假信息案件

7 月 26 日，广东省茂名市公安局茂南分局依法查处茂名市首宗利用 AI 技术编造传播虚假信息案件，违法行为人被依法处以行政处罚。

26 日凌晨，茂名公安网安部门巡查发现某视频平台传播一条标题为“一个 7 岁小孩因为偷了同学一支铅笔被老师绑在电线杆上面 5 个小时”的短视频，视频声称事件发生于 2021 年广东茂名下辖某县级市，小孩在警察到场前已无力站立。经核查，该视频内容纯属不实信息。网民崔某为博取流

量，对在网上看到的一篇关于“小孩偷铅笔”内容的文章，通过AI软件生成视频，编造为茂名市下辖某县级市发生的案件，并在三个网络社交短视频平台发布传播，造成恶劣影响。目前，违法行为人崔某被公安机关依法作出行政拘留十日处罚。（来源：平安茂南）

（三）刑事处罚案件

1. 浙江绍兴公安机关摧毁利用ChatGPT制作虚假视频的造谣团伙

7月5日消息，浙江省绍兴市上虞区公安分局近日对“网络水军”通过组织发布虚假视频获利行为开展收网打击，摧毁一利用ChatGPT制作虚假视频的造谣团伙。该案系浙江首例团伙制作虚假视频案件。

6月2日，上虞警方在网上巡查时发现用户名为“舷忆解说”的某APP网民发布关于上虞工业园区发生火灾的视频，在短时间内浏览量迅速攀升。对此，警方介入核实，确认视频系不实信息，并很快锁定外省某科技公司有较大作案嫌疑。经查，5月以来，该公司从网上非法收购一批视频账号，通过ChatGPT技术，拼接制作虚假视频发布网络，博取流量，并通过流量算法返款盈利。截至目前，该团伙非法购买视频账号1500余个，发布未经核实视频3000个以上。目前，该公司涉案3名犯罪嫌疑人涉嫌寻衅滋事罪被警方采取刑事强制措施，案件正在进一步侦办中。

（来源：浙江网警巡查执法）

2. 黑龙江哈尔滨市南岗区法院审结首例侵犯公民个人信息罪刑事附带民事公益诉讼案

7月10日消息，黑龙江省哈尔滨市南岗区法院近日审结首例侵犯公民个人信息罪刑事附带民事公益诉讼案。

2022年5月至10月，被告人麻某在哈尔滨市南岗区某小区的家中，通过手动修改ID参数及使用后羿采集器软件自动爬取的方式，利用API遍历漏洞进入哈尔滨某医院微信公众号挂号系统，非法获取该系统内患者电子病历包括患者姓名、身份证号码、手机号、家庭住址、患者主诉等数据，将上述数据传输固定至自己的台式电脑中，麻某将上述数据转卖并获利9963.44元。

公诉机关以被告人麻某涉嫌犯侵犯公民个人信息罪提起公诉并提起刑事附带民事公益诉讼，请求判决麻某支付公益损害赔偿金9963.44元，并在黑龙江省级以上媒体公开道歉。南岗区法院经审理认为，被告人麻某违反国家有关规定，非法获取、出售公民个人信息，情节特别严重，其行为已构成侵犯公民个人信息罪，依法判决被告人麻某犯侵犯公民个人信息罪，判处有期徒刑三年一个月，并处罚金人民币10000元。

（来源：哈尔滨市南岗区法院）

3. 云南楚雄公安机关侦破首例破坏计算机信息系统案件

7月31日消息，云南省楚雄市公安局落实夏季治安打击整治行动，严厉打击涉网络违法犯罪，成功侦破首例破坏计算机信息系统案件，抓获犯罪嫌疑人1人，缴获涉案电脑2台、手机2部。

2023年7月，辖区某科技公司开发营运的APP被人连续攻击后台服务器，恶意向用户发送无效登录的短信验证码共计2万余条，导致用户无法正常登录，服务器一度中断，给公司造成巨大损失。接警后，楚雄市公安局对该案展开调查并锁定犯罪嫌疑人俞某某，经查明，俞某某于2023年2月入职该公司，工作中与主管人员发生冲突后心怀不满，离职后出于报复心理，编写程序脚本持续对公司开发的APP服务器实施攻击。目前，俞某某已被公安机关刑事拘留，案件正在进一步侦办中。（来源：平安楚雄）

境外前沿观察：月度速览十则

导读：本月，欧美跨境数据流动规则取得新进展。欧盟委员会批准欧美间数据传输新协议《欧美数据隐私框架》，标志着欧美间个人数据合法流动的第三次尝试正式落地。美国 SEC 通过上市公司网络安全事件披露规则，要求上市公司应当在重大网络安全事件发生后 4 个工作日内向 SEC 披露该事件。IBM 发布《2023 年数据泄露成本报告》，指出数据泄露的平均成本在 2023 年达到历史新高，为 445 万美元，同时指出遭受勒索攻击后，不向执法部门汇报会导致更高的损失。美国 FTC 对 ChatGPT 背后的公司 OpenAI 正式发起调查，主要围绕 OpenAI 的数据处理以及向用户提供不准确信息是否违反消费者保护法。类似的，韩国个人信息保护委员会决定对 OpenAI 处以 360 万韩元罚款，因为其在 2023 年 3 月泄露了 687 名韩国用户的个人数据。

关键词：美欧数据跨境流动、智能设备标签计划、网络安全事件披露、勒索攻击、数据泄露、OpenAI 监管

1. 欧盟委员会通过《欧盟-美国数据隐私框架的充分性决定》，欧美间个人数据合法流动第三次尝试正式落地

7 月 10 日，欧盟委员会投票通过《欧盟-美国数据隐私框架的充分性决定》。充分性决定认为，对于根据欧盟-美国数据隐私框架（DPF）从欧盟控制者或处理者传输到美国经认证组织的个人数据，美国方面能够提供基本上与欧盟相同的保护水平。具体而言，充分性决定的效果是，个人数据可以从欧盟的控制者和处理者转移到美国经认证的组织，而无需获得任何进一步的授权。

充分性决定还规定了新的具有约束力的保障措施，以解决欧洲法院对美国情报活动提出的担忧。这包括确保对美国信号情报活动在追求既定国家安全目标的过程中对其采取必要且相称的限制。此外，数据保护审查法院（DPRC）的建立允许欧盟境内的个人就涉嫌侵犯其隐私和公民自由的行为提起诉讼。必要时，DPRC 可以责令有关情报机构采取补救措施，包括删除数据、终止获取、改变收集方式等。被发现持续不遵守这些原则的组织将从 DPF 名单中删除，并且必须归还或删除根据 DPF 收集到的个人数据。

（来源：欧盟委员会）

2. 美国拜登政府宣布“美国网络信任标识计划”

7 月 18 日，拜登政府宣布“美国网络信任标识计划”，将于 2024 年正式启动，零售商和制造商提供的符合网络安全标准的智能设备将获得“网

络信任”标签，帮助美国消费者更轻松地选择不易受到网络攻击的设备。白宫将与亚马逊、谷歌和百思买等公司合作，对智能设备进行网络安全认证。相关设备需要密码、数据保护、软件更新和事件检测等功能方面通过美国国家标准与技术研究院（NIST）发布的特定网络安全标准。

（来源：美国白宫）

3. 美国 SEC 通过上市公司网络安全事件披露规则：应在 4 个工作日内披露重大网络安全事件

7 月 26 日，美国证券交易委员会（SEC）通过最终规则《网络安全风险管理、策略、治理及事件披露》，明确上市公司重大网络安全事件的强制性披露要求。具体来说：（1）披露范围是重大网络安全事件。根据SEC解释，当该事件信息对于理性投资者而言，构成作出投资决策所需的重要信息或者将显著改变上市公司已公开信息显示的经营情况时，该事件即构成重大安全事件。（2）披露内容侧重于描述重大网络安全事件影响，无需对事件本身的细节进行披露。（3）上市公司确定自身发生重大网络安全事件后的 4 个工作日内向SEC提交载明事件信息的 8-K表。在特殊情况下，若美国司法部长认为立即披露会对国家安全或公共安全构成重大风险，上市公司可在司法部长指定的延迟期限进行披露。（来源：美国证券交易委员会）

4. 欧盟网络安全局发布《医疗行业网络安全威胁形势》：勒索软件占网络安全威胁的 54%

7 月 5 日，欧盟网络安全局发布报告《医疗行业网络安全威胁形势》，对 2021 年 1 月至 2023 年 3 月期间发生的医疗行业网络事件进行分析。报告发现，勒索软件和数据相关威胁是医疗行业面临的最普遍、最有影响力的网络安全威胁，主要影响医疗服务提供者和医院。勒索软件占网络安全威胁的 54%，其中 43%勒索软件事件都伴随着数据泄露或数据盗窃。网络犯罪分子是医疗行业的主要威胁行为者，尤其是出于经济利益而进行勒索攻击的行为者。

报告还发现，事件主要导致数据泄露或数据盗窃、医疗服务中断和与医疗无关的其他服务中断。数据泄露影响了 40%的医疗实体，尤其是医院和初级保健机构。其他影响包括财务损失、数据保护当局制裁以及医疗服务提供者在重大数据泄露后的声誉损害。患者安全仍然是健康界的重要关注点，存在导致患者分诊和治疗延迟、患者敏感信息被泄露、患者受到勒索等不良影响。（来源：欧盟网络安全局）

5. 台积电遭遇勒索攻击，索要 7000 万美元赎金

7 月 5 日消息，台积电日前发布声明表示遭到勒索软件团伙 LockBit 的网络攻击。LockBit 并没有说明从台积电窃取了多少数据，但已经设定了 8 月 6 日为支付赎金的最后期限，否则会将其数据发布到暗网。该团伙还为

台积电提供了将赎金计时器延长 24 小时的选项，价格为每天 5000 美元；另一个选项是销毁 Lockbit 获取或下载的所有数据，赎金为 7000 万美元。

台积电表示，其供应商之一、IT 服务提供商 Kinmax 的系统遭到入侵，这可能是导致台积电数据被盗的原因，但台积电声称没有泄露客户数据。在数据泄露事件发生后，台积电根据安全协议和标准操作程序，立即终止了与 Kinmax 的数据交换。Kinmax 的业务专注于网络、云计算、存储、安全和数据库管理。该公司在 6 月 29 日遭到入侵，并表示其内部特定测试环境遭到网络攻击，一些信息被泄露。Kinmax 表示，泄露的内容主要包括该公司提供给客户的系统安装信息。（来源：极客网）

6. IBM 发布《2023 年数据泄露成本报告》：不向执法部门汇报会导致更高损失

7 月 24 日，IBM发布《2023 年数据泄露成本报告》，调查了在 2022 年 3 月至 2023 年 3 月期间受到数据泄露影响的 553 家组织。报告指出，数据泄露的平均成本在 2023 年达到历史新高，相比 2022 年的 435 万美元增加 2.3%，为 445 万美元。虽然数据泄露成本持续上升，但是受访者对于是否计划因数据泄露而增加安全投资的意见几乎各占一半。需要增加投资的首要领域包括事件响应规划和测试、员工培训以及威胁检测和响应技术。

报告指出，67%的数据泄露事件是由善意第三方或攻击者自己报告的。与内部检测相比，当攻击者披露漏洞时，企业要多付出近 100 万美元的代价。因此，组织需要配备更完善的内部威胁检测技术。报告指出，安全的

人工智能和自动化技术是降低成本、最大限度缩短识别和遏制漏洞时间的重要投资。广泛使用这些技术的组织平均缩短了108天的时间识别、控制安全漏洞，同时将数据泄露损失成本降低了176万美元。报告还发现，受访者在遭受勒索攻击后，不向执法部门汇报会导致更高的损失。在未向执法部门寻求帮助的受访者中，37%普遍多支付了9.6%的费用，并经历长达33天的数据泄露周期。（来源：IBM）

7. 因用谷歌分析功能向美传输数据，瑞典企业被罚千万

7月3日，瑞典隐私保护局（IMY）在对CDON、Coop、Dagens Industri和Tele2四家企业进行数据传输调查后发布公告，称其使用谷歌分析工具导致用户个人数据传输到美国的行为违反GDPR，对其中两家企业处以1200万和30万瑞典克朗的行政罚款，并警告其他公司不得使用谷歌分析功能。

2020年，欧盟法院宣布“隐私盾”无效。宣布无效后，仍有许多公司使用谷歌分析等功能进行数据传输，谷歌等企业也依旧以“隐私盾”为数据传输的法律依据。为此，非营利组织NOYB针对此事向欧洲监管机构发起数十起投诉。IMY公告显示，其发现谷歌对发送到美国进行处理的欧洲用户数据采取的保护措施无法达到欧盟的法律标准。比如，被调查的瑞典企业之一无法证明谷歌是在其数据传输到美国之前还是之后采取的数据匿名化措施，因此不排除谷歌通过谷歌分析功能获取了更多额外个人数据的嫌疑。此外，被调查的四家企业都是基于标准合同条款，做出利用谷歌分析功能

传输个人数据的决定，此举违反了GDPR，且企业采取的技术安全措施也不够。（来源：隐私护卫队）

8. 美国正式调查 OpenAI，涉数据安全问题

7 月 13 日消息，美国联邦贸易委员会（FTC）近日对 ChatGPT 背后的公司 OpenAI 正式发起调查，调查主要围绕 OpenAI 的数据处理以及向用户提供不准确信息是否违反消费者保护法。

在长达 20 页的详细信函中，FTC 向 OpenAI 询问了一系列有关 ChatGPT 潜在风险的问题，并要求其提供包括：处理个人数据、向用户提供不准确信息的可能性；对消费者造成损害（包括声誉损害）风险的记录信息；关于收到的所有投诉的详细描述，这些投诉涉及其产品做出“虚假、误导、贬低或有害”的陈述；有关数据安全事件以及软件更新前采取的预防措施等方面的信息。（来源：华盛顿邮报）

9. 因违反《儿童在线隐私保护法》，亚马逊签署和解协议

7 月 19 日，美国司法部与联邦贸易委员会（FTC）联合宣布，由于亚马逊专有语音激活服务Alexa涉嫌违反《儿童在线隐私保护法》（COPPA）等法律，亚马逊已签署包含 2500 万美元民事罚款的和解协议，并采取识别并删除不活跃的儿童个人信息，除非家长要求保留；根据用户或家长要求分别删除地理位置信息、语音信息和儿童个人信息等 4 项改进措施。

2018 年 5 月以来，亚马逊针对 13 岁以下儿童的声控产品开始支持Alexa。

当用户向支持Alexa的设备发出口头请求，亚马逊会保存请求录音并创建书面记录。根据指控，亚马逊默认无限期保留儿童录音，违反COPPA关于仅在实现收集目的合理必要的范围内保留这些录音的要求。其他被指控的违规行为包括欺骗性地向Alexa应用程序用户表示他们可以删除自己或孩子的录音，包括音频文件、文本以及地理位置信息，而实际上亚马逊没有应用户的要求删除这些信息。（来源：美国司法部）

10. 因数据泄露，韩国对 OpenAI 罚款 360 万韩元

7 月 27 日，韩国个人信息保护委员会（PIPC）宣布，因违反《个人信息保护法》（PIPA），对OpenAI处以 360 万韩元罚款。PIPC调查发现，2023 年 3 月，作为全球数据泄露事件的一部分，ChatGPTPlus约 687 名韩国用户的个人数据，包括姓名、电子邮件和信用卡详细信息被泄露。PIPC指出，尽管无法得出OpenAI忽视个人数据预期保护措施的结论，但PIPC指责OpenAI未能在 24 小时内向PIPC报告数据泄露，违反PIPA。此外，PIPC指出OpenAI在PIPA合规方面的某些不足，包括仅以英语提供隐私保护政策，缺乏明确的同意程序，数据处理关系不明确以及关于用户年龄的限制不一致等。PIPC建议OpenAI对个人数据处理系统进行评估，以确保符合韩国法律法规要求。（来源：韩国个人信息保护委员会）

行业前沿观察一：持续深化“等保”“关保”制度

导读： 7 月 6 日，公安部举行新闻发布会。会上，公安部网络安全保卫局副局长李彤、警务技术二级总监黄小苏出席。

李彤表示，党中央高度重视网络安全问题，习近平总书记多次强调，没有网络安全就没有国家安全。公安部党委坚决贯彻落实习近平总书记重要指示精神，坚持总体国家安全观，牢固树立底线思维，带领全国公安机关聚焦防范化解各类网络安全重大风险隐患，以保护关键信息基础设施、重要网络和大数据安全为重点，深化落实网络安全等级保护制度、关键信息基础设施安全保护制度和数据安全保护制度，全面加强网络安全防范管理、监测预警、信息通报、应急处置和侦查打击等各项措施，积极构建“打防管控”一体化的网络安全综合防控体系，有力维护了我国网络空间安全，取得了显著成效。

关键词：网络安全、关键信息基础设施安全保护制度、网络安全等级保护制度、网络安全

1. 公安部网络安全保卫局副局长李彤强调持续深化网络安全等级保护制度，筑牢网络安全基石

李彤表示，党的十八大以来，有关网络与信息安全保障的法律制度逐步建立并不断发展完善。其中，公安部牵头建立的网络安全等级保护制度，已经成为网络安全领域的基本制度。十多年来，公安机关勇于担当、守正创新，会同相关部门构建完善网络安全等级保护的法

律政策体系积极推动网络安全等级保护的法律政策体系、标准体系、技术体系和工作体系，监督指导各单位、各部门深入开展网络安全等级保护定级、备案、等级测评、安全建设和监督检查等重点工作。督促指导网络运营者、数据处理者提高网络安全意识，依法落实网络安全保护责任义务，不断加强网络安全管理，构建完善技术防护体系，有力维护了重点行业部门、企事业单位的网络和数据安全。

深入推进关键信息基础设施安全保护工作，全力保障经济社会正常运转。根据《关键信息基础设施安全保护条例》，按照法定职责，公安部制定出台了一系列配套文件和工作指南，组织重点行业领域制定关键信息基础设施认定规则，识别认定关键信息基础设施，深入开展关键信息基础设施安全保护工作。同时，组织指导有关单位制定《关键信息基础设施安全保护要求》等国家标准，加强标准宣贯培训工作，组织重点行业领域开展关键信息基础设施安全保护试点示范工作，深化安全保护措施，着力构建关键信息基础设施综合防御体系，有力维护了关键信息基础设施安全。（来源：公安部官网）

行业前沿观察二：产业前景巨大，人才建设大有可为

导读：日前，在中央网信办指导下，首届武汉网络安全创新论坛召开，发布《中国网络安全人才建设报告（2022 年）》。《报告》首次针对网络安全领域人才培养供需两侧做出问卷调研，为网安人才的培养提供了基础数据和方向。

《报告》显示，目前国内网络安全领域人才队伍逐渐成形，人才培养机制渐趋成熟，人才供给不断增加，但依然存在高端专才紧缺、师资力量不足、人才供需不均衡等问题。

7 月 6 日，公安部举行新闻发布会。会上，公安部网络安全保卫局副局长李彤、警务技术二级总监黄小苏出席，黄小苏表示，公安机关加快建立完善网络安全专门人才培养体系，打造实战化网络安全专门人才，并通过指导举办网络安全大赛等提升了全社会网络安全意识。

网络安全产业前景巨大，加强加快网安人才建设大有可为。

关键词：网络安全人才建设、人才培养机制、人才供给

1. 公安部：加快建立完善网络安全专门人才培养体系

公安部 7 月 6 日举行新闻发布会。会上，公安部网络安全保卫局副局长李彤、警务技术二级总监黄小苏出席。

对记者关于公安机关近年来如何培养、选拔、使用网络安全人才的提问，黄小苏表示，公安机关加快建立完善网络安全专门人才培养

体系，打造实战化网络安全专门人才，并通过指导举办网络安全大赛等提升了全社会网络安全意识。

黄小苏表示，人才是网络安全发展的核心要素和关键，是保卫国家关键信息基础设施的重要社会支撑力量。公安机关加快建立完善网络安全专门人才培养体系，打造实战化网络安全专门人才。通过比赛，汇聚各界智慧、凝聚各方力量、发挥各方技术优势，发现了一大批网络安全高端人才，磨砺了网络安全实战攻防能力水平，提升了全社会网络安全意识。（来源：北京日报客户端）

2. 宁波第六届网络安全大赛纳入职工技能大赛和人社部门职业技能竞赛

6 月 11 日，“天一永安杯”宁波市第六届网络安全大赛落幕。本届大赛共有来自全国各地的 311 支队伍参与，21 支行业组队伍和 16 支高校组队伍成功晋级决赛。

经过激烈角逐，本次大赛最终决出了 5 个一等奖队伍。这些冠军队伍展现了卓越的技术实力和团队合作能力，为宁波市的网络安全发展做出了重要贡献。他们在解决网络安全漏洞、进行攻防演练等项目中展现了深厚的专业素养和创新思维。本次大赛的成功举办充分展示了宁波市在网络安全领域的实力和成就。这不仅积极推动着宁波市网络安全事业的发展，也为全市广大市民提供了一个加强网络安全意识和知识的平台，标志着宁波市网络安全事业迈上了新的台阶。

据了解，自 2018 年首次举办以来，从 48 支报名队伍开始，该大赛一直备受社会各界的关注和支持，每年参赛队伍数同比增长超过 60%，本届大赛参赛队伍数相较往年更是数量翻倍，创造了历届新纪录。宁波市委宣传部副部长、市委网信办主任林大吉强调指出，本届大赛纳入了宁波职工技能大赛和人社部门职业技能竞赛，并与职称和薪资挂钩，对符合规定的选手推荐申报宁波市“首席工人”或“技术能手”称号；对行业组决赛总成绩一、二、三等奖及优胜奖的队伍成员推荐申报网络与信息安全管理员职业技能等级认定。此举将提升网络安全领域对人才的吸引力和培养力度，推动网安行业的发展。

“此次大赛的举办不仅是一场网络安全技术的角逐，更是对宁波市网络安全领域成果的集中展示。通过比赛，各界专家和观摩人员不仅了解到了最新的网络安全技术和解决方案，还见证了宁波市在网络安全领域取得的突破和进步。这将进一步提升宁波市的网络安全形象，吸引更多的人才和投资，促进整个行业的发展。”该负责人表示。

（来源：宁波市计算机信息网络安全协会）

3. 安徽宿州举办网络安全职业技能竞赛选拔人才

8 月 11 日，2023“宿安杯”网络安全职业技能竞赛决赛在安徽省宿州市成功举办。此次活动由市委网信办、市总工会、市公安局联合主办，中国电信股份有限公司宿州分公司承办。

当日，来自全市各地各部门的 19 支队伍 57 名选手同场竞技，竞赛包括网络安全知识竞赛和解题夺旗赛（CTF 模式）两个部分。

据市委网信办有关负责人介绍，此次竞赛是该市首次举办的较大规模网络安全专业技能赛事，也是2023年宿州网络安全宣传周预热活动之一，旨在为全市网络安全人才提供一个公平竞争、磨砺技术、切磋交流的平台，充分调动各地各部门参与网络安全工作的积极性、主动性和创造性。通过以赛促学、以赛促练、以赛促建，进一步强化网络安全责任意识，提升网络安全防护水平。同时，为发现、培养、选拔网络安全人才提供有效参考，为宿州市网络空间安全提供坚实人才保障。（来源：拂晓报）

行业前沿观察三：网络安全认证价值和作用日益凸显

导读：随着信息技术的不断发展，网络安全已经成为了一个不可忽视的问题。由于互联网的广泛运用，数据的流动性也愈发增强，这使得网络安全问题愈发突出。在这种情况下，网络安全认证信息的重要性就愈加凸显。为推进网络安全服务认证体系建设，加强网络安全服务监督管理，促进网络安全服务产业发展。近日，国家市场监管总局、中央网信办、工业和信息化部、公安部发布了关于开展网络安全服务认证工作的实施意见。

关键词：网络安全、认证、价值、作用、市场监管总局等四部门

1. 国家市场监管总局等四部门发布《关于开展网络安全服务认证工作的实施意见》

为推进网络安全服务认证体系建设，提升网络安全服务机构能力水平和服务质量，根据《网络安全法》《认证认可条例》，市场监管总局、中央网信办、工业和信息化部、公安部就开展国家统一推行的网络安全服务认证工作发布《关于开展网络安全服务认证工作的实施意见》，强调加强认证工作的组织实施和监督管理，鼓励网络运营者等广泛采信网络安全服务认证结果，促进网络安全服务产业健康有序发展，要求通过认证的网络安全服务机构应当按照有关法律法规、标准规范等开展网络安全服务工作，确保持续符合认证要求。

《意见》的发布，对规范网络安全服务认证工作，提高网络安全服务认证机构能力，提升网络安全行业发展水平有积极作用。

（来源：中国网信网）

2. 站在网络安全时代“风口”的网安联认证中心

当前，我国网络安全产业链虽然已经逐步完善，上中下游都有相关企业提供产品和服务，但不可否认的是，我国网络安全市场上安全硬件占比最高。相比之下，网络安全服务的规模占比还有待提高。随着市场需求以及政府政策的推动，网络安全服务规模在不断发展扩大，并且由于政府对网络安全的重视程度不断提高，网络安全服务也已上升为国家战略，并在制度和法规层面强化了对网络安全服务的要求。

国家市场监督管理总局等四部门发布的《关于开展网络安全服务认证工作的实施意见》对网络安全服务机构和市场提出了更高的要求，进一步规范了网络安全服务市场秩序，推动网络安全服务企业向规范

化、法制化、专业化方向健康有序发展，同时，也进一步提升了网络安全服务认证的价值和作用，促进了网络安全行业发展。

企业想要凭借网络安全的“风口”腾飞，必须按照有关法律法规、标准规范建立起一套完善的网络安全服务体系，为用户提供优质的网络安全服务。企业想要建立符合有关法律法规、标准规范的网络安全服务体系，需要依法设立的权威第三方认证机构对企业进行认证。通过第三方认证机构的客观评价认证，找出企业自身信息数据安全服务存在的问题并改进，提升企业信息数据安全服务水平。

网安联认证中心是集认证、培训、科研、政策研究、标准制定、国际合作于一体，面向全球的综合性技术服务机构，拥有数百名技术专家和经验丰富的优秀审核团队，与业内领先企事业合作，主导和参与国内多项国家标准、行业标准、团体标准、地方标准的制定，在网络安全认证领域享有盛誉。2021 年 2 月，网安联认证中心获得国家认证认可监督委员会批准开展认证工作(批准号:CN-CA-R-2021-762)，是国内第二家获批的可以从事网络空间安全认证的机构。认证内容主要包括以下四大类三十多种:

信息安全服务资质认证:

计算机信息系统安全服务等级认证

网络空间安全服务资质认证（安全咨询、监测预警、安全集成、安全运维、应急响应、软件安全、工业控制系统安全、数据安全、风险评估、云计算安全、安全审计、渗透测试等 12 个领域）

管理体系认证:

信息安全管理体系认证　　信息技术服务管理体系认证

产品认证:

信息技术应用创新软件适配认证

建材认证　　家具认证

电子设备和元器件认证　　陆地交通产品认证

专业人员认证：

网络空间安全专业人员认证

网络安全管理　　网络安全规划设计

软件安全开发　　安全集成

安全运维　　风险评估

应急处理　　网络安全审计

工业控制系统安全　　大数据安全

物联网安全　　云计算安全

人工智能安全　　渗透测试

关键信息基础设施保护　　重要数据保护

个人信息保护

香港注册网络空间安全工程师/网络空间安全工程技术人才专业能力认证

网络安全测试能力（团队）认证

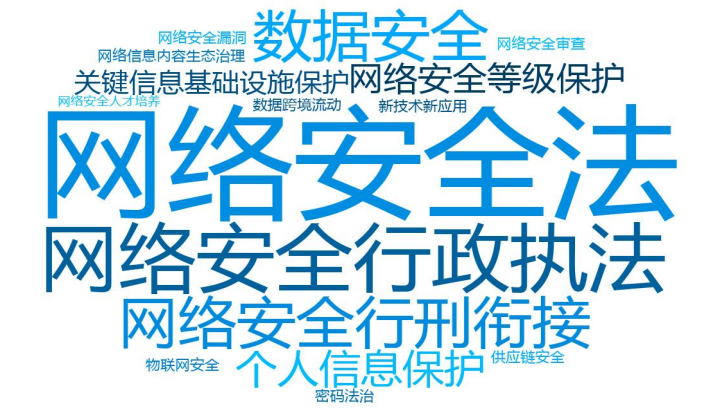
面对网络安全服务这一不可逆转的时代趋势以及用户对网络信息安全的需求，网络安全服务行业也必将成为一个强劲的“风口”，从事网络信息安全相关产业的企业也将会迎来极具光明的发展前景。

只有抓住“风口”机遇，提前做好相应的网络安全服务认证的企业才能够在激烈的竞争中脱颖而出，顺势起飞。（来源：网安联）

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

……