网安联
Wang An Lian

网络与数据安全治理

FRONTIERS OF REGULATORY OVERSIGHT IN CYBERSECURITY AND DATA GOVERNANCE

前沿洞察（月刊）

2024年10月第10期 (总第15期)

2024年10月12日

目　录

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

牵头组织：网安联秘书处

协办单位：网安联认证中心

技术支持：北京关键信息基础设施安全保护中心

广东关键信息基础设施保护中心

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

境内前沿观察一：安全事件

导读：9 月，弥合数字鸿沟、推动人工智能全球治理仍是我国开展国际交流与合作的重要议题。《关于共筑新时代全天候中非命运共同体的北京宣言》通过，中非双方同意携手努力，通过建立国家行为准则、发展数字扫盲等举措，推动停止滥用人工智能。中方提出《人工智能能力建设普惠计划》，旨在弥合智能鸿沟和推动落实联合国 2030 年可持续发展议程，围绕各方尤其是全球南方期待的人工智能基础设施、产业赋能、人才培养等领域合作开展行动。

国内方面，全国网安标委发布《人工智能安全治理框架》1.0 版，基于风险管理理念，该框架针对不同类型的人工智能安全风险，从技术、 管理两方面提出防范应对措施。与此同时，国家互联网信息办公室发布《国家信息化发展报告（2023 年）》。报告显示，受调查的网民普遍认为 2023 年信息化发展在丰富精神文化生活、提升公共服务水平、增强社会治理能力、促进共同富裕等方面发挥了重要作用，人民群众的获得感、幸福感、安全感不断提升。

国家安全部发布“台独”网军“匿名者 64”相关情况，并表示国家安全机关锁定了实施相关网络攻击活动的台湾人员身份信息，已依法对其立案侦查。

关键词：人工智能治理、信息化发展、“台独”网军

1. 中非合作论坛北京峰会通过《关于共筑新时代全天候中非命运共同体的北京宣言》

9月4日至6日，中非合作论坛北京峰会召开。峰会协商一致通过《关于共筑新时代全天候中非命运共同体的北京宣言》，围绕关于共筑高水平中非命运共同体、全球安全倡议为中非维护国际和平与安全共同行动提供强劲动力等6方面提出30项内容。

宣言指出，为抓住新一轮科技革命和产业变革的历史性机遇，中方愿与非洲携手加快发展新质生产力，共同强化科技创新和成果转化，推进数字经济和实体经济深度融合。双方要携手完善全球科技治理，营造包容、开放、公平、公正、非歧视的科技发展环境。双方强调和平利用科技是国际法赋予各国不可剥夺的权利，支持联合国大会“在国际安全领域促进和平利用国际合作”决议，确保发展中国家充分享受和平利用科技的权利。双方赞赏联合国大会协商一致通过“加强人工智能能力建设国际合作”决议。非方欢迎中方提出的《全球人工智能治理倡议》《全球数据安全倡议》，赞赏中方为增强发展中国家在人工智能、网络、数据领域全球治理中的权利所作努力。中非双方同意携手努力，通过建立国家行为准则、发展数字扫盲等举措，推动停止滥用人工智能。双方认为应坚持发展与安全并重原则，不断弥合智能鸿沟、数字鸿沟，共同做好风险防范，探讨形成以联合国为主渠道的相关国际治理框架。双方欢迎2024年7月在上海举行的世界人工智能大会暨人工智能全球治理高级别会议通过的《人工智能全球治理

上海宣言》。双方欢迎2024年6月在拉巴特举行的人工智能高级别论坛通过的《非洲人工智能共识宣言》。（来源：外交部）

2. 中方提出《人工智能能力建设普惠计划》

9月25日，由中国和赞比亚合办的“加强人工智能能力建设国际合作高级别会议”在联合国总部举行。各方围绕加强人工智能能力建设国际合作深入交换意见，达成广泛共识。

中方提出的《人工智能能力建设普惠计划》得到各方积极支持和响应。普惠计划旨在弥合智能鸿沟和推动落实联合国2030年可持续发展议程，围绕各方尤其是全球南方期待的人工智能基础设施、产业赋能、人才培养、数据建设、安全治理等领域合作提出“五大愿景”，明确中方将采取的“十项行动”，包括促进人工智能和数字基础设施联通，开展模型研发和应用、语料建设等合作，加强人工智能战略对接和政策交流，积极分享技术实践。中方将于2025年底前重点面向发展中国家举办十期人工智能领域研修研讨项目。为推进普惠计划落实，中方还倡议成立“人工智能能力建设国际合作之友小组”。（来源：外交部）

3. 国家互联网信息办公室发布《国家信息化发展报告（2023年）》

9月8日消息，国家互联网信息办公室近日发布《国家信息化发展报告（2023年）》。

报告显示，2023年各地区、各部门深入贯彻落实党中央、国务院决策部署，强化顶层设计、统筹协调、整体推进、督促落实，推动信息化关键

能力建设取得新突破，网络信息技术创新步伐不断加快，新一代信息基础设施持续完善，数据资源开发利用水平明显提升；信息化驱动引领经济社会发展取得新成效，数字经济赋能高质量发展，信息化赋能高品质生活，电子政务赋能高效能治理；信息化发展环境建设迈上新台阶，全国信息化发展整体水平得到新提升，为强国建设、民族复兴伟业注入新动能。

报告分析了信息化发展情况网络问卷调查结果，参与调查的网民普遍认为，2023 年信息化发展在丰富精神文化生活、提升公共服务水平、增强社会治理能力、促进共同富裕等方面发挥了重要作用，人民群众的获得感、幸福感、安全感不断提升；受访企业普遍加大创新研发投入，提高信息化人才培养力度，不断提升技术产品和服务竞争力。

报告提出，2024 年，要准确把握党的二十届三中全会对信息化发展作出的新部署新任务新要求，切实把信息化工作融入到改革发展大局中，扎实推动相关改革任务落地见效：一是聚焦高水平科技自立自强，增强信息化发展关键能力；二是聚焦发展新质生产力，进一步发挥信息化对经济高质量发展的驱动引领作用；三是聚焦保障和改善民生，持续深化信息惠民为民服务；四是聚焦提高党的领导水平和长期执政能力，加快以信息化推进国家治理体系和治理能力现代化；五是聚焦统筹高质量发展和高水平安全，不断优化信息化发展环境。（来源：中国政府网）

4. 全国网安标委发布《人工智能安全治理框架》1.0 版

9 月 9 日，全国网安标委发布《人工智能安全治理框架》1.0 版，包括人工智能安全治理原则、人工智能安全风险分类、技术应对措施、综合治理措施、人工智能安全开发应用指引等内容。

框架将人工智能安全风险分为内生安全风险和应用安全风险。内生安全风险包括模型算法安全风险、数据安全风险、系统安全风险。应用安全风险包括网络域安全风险、现实域安全风险、认知域安全风险和伦理域安全风险。

框架提出十项综合治理措施，包括实施人工智能应用分类分级管理、建立人工智能服务可追溯管理制度、完善人工智能数据安全和个人信息保护规范、构建负责任的人工智能研发应用体系、强化人工智能供应链安全保障、人工智能安全风险威胁信息共享和应急处置机制等。（来源：全国网安标委）

5. 国家安全部发布“台独”网军“匿名者 64”相关情况

9 月 23 日，国家安全部发布“台独”网军“匿名者 64”相关情况。

2024 年以来，一个名为“匿名者 64”的黑客组织，针对中国大陆和港澳地区，频繁开展网络攻击，试图获取有关门户网站、户外电子屏幕、网络电视等控制权限，进而非法上传、插播诋毁大陆政治制度和大政方针的内容，颠倒黑白，散布谣言。对此，国家安全机关深入调查确认，“匿名者 64”组织并非普通黑客，而是由“台独”势力豢养的一支网军。

“匿名者64”组织的真实背景是台湾资通电军下属的网络战联队网络环境研析中心。该中心专职负责对大陆实施网络认知战、舆论战。2023年6月，该中心以“匿名者64”组织的名义，注册社交媒体账号，肆无忌惮地实施网络攻击和反宣破坏活动。

台湾资通电军是台湾当局于2017年6月主导建立的“第四军种”，2022年改革为台湾“国防部”直属机构，主要承担电子作战、信息作战、网络作战及军线维护管理等职能，是台湾当局对大陆实施网络作战的主力。

台湾资通电军一经成立，便对大陆大肆开展各类网络渗透破坏活动，是危害网络空间安全的毒瘤。一方面，以大陆国防军工、航空航天、能源基建等领域为重点，搜寻目标定向实施网络攻击，妄图窃取敏感数据资料，为台湾当局搜集情报。另一方面，频繁扭曲网络舆论，雇佣水军，借机生事，放大矛盾，挑唆对立，从中渔利。

目前，国家安全机关锁定了实施相关网络攻击活动的台湾人员身份信息，其中包括台湾资通电军现役人员罗俊铭、洪莉棋、廖韦纶。国家安全机关已依法对三人立案侦查。（来源：国家安全部）

境内前沿观察二：政策立法

导读：9 月，《网络数据安全管理条例》正式公布，自 2025 年 1 月 1 日起施行。作为细化《网络安全法》《数据安全法》《个人信息保护法》的一项重要行政法规，条例坚持总体国家安全观，统筹发展和安全，既加强网络数据安全保护，又鼓励和促进网络数据依法合理有效利用；同时，条例坚持问题导向，聚焦个人信息、重要数据、网络数据跨境流动等方面突出问题，有针对性地健全制度措施；坚持统筹协调，妥善处理与上位法的关系，对相关制度规定予以细化、补充、完善。

《人工智能生成合成内容标识办法（征求意见稿）》与强制性国家标准《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》同日公开征求意见。其中，《人工智能生成合成内容标识办法（征求意见稿）》明确人工智能生成合成内容标识包括显式标识和隐式标识。服务提供者应当按照有关强制性国家标准的要求进行标识。《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》给出显式标识和隐式标识的具体方法，如显式标识的实现方式包括内容显式标识、交互场景界面显式标识等；隐式标识的实现方式包括元数据隐式标识、内容隐式标识等。

二十届三中全会审议通过的《中共中央关于进一步全面深化改革 推进中国式现代化的决定》中提出“培育全国一体化技术和数据市场”“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”。9 月，为贯彻落实党的二十届三中全会决策部署，

国家数据局发布《关于促进数据产业高质量发展的指导意见（征求意见稿）》，将数据采集、数据存储、数据治理、数据分析、数据交易、数据应用、数据安全、数据基础设施列为数据技术和产业重点支持方向；同日发布《关于促进企业数据资源开发利用的意见（征求意见稿）》，明确企业有权依法或依合同约定，自主或委托他人基于其合法持有数据开发数据产品或提供数据服务。

平台治理方面，9 月，民政部等五部门发布《个人求助网络服务平台管理办法》，针对专门为因疾病等原因导致家庭经济困难的个人，提供求助信息发布和捐助资金归集、管理、拨付等服务的网络平台进行管理。办法要求个人求助网络服务平台，应当经国务院民政部门指定。市场监管总局发布《关于推动网络交易平台企业落实合规管理主体责任的指导意见（征求意见稿）》，强调网络交易平台企业一般应当明确合规负责人，并根据自身组织架构等因素和合规管理工作需要，配备适当数量的合规管理员。

关键词：网络数据安全管理条例、人工智能生成合成内容标识、数据产业高质量发展、企业数据开发利用、平台治理

（一）国家层面动向

1.《网络数据安全管理条例》公布，自2025年1月1日起施行

9月24日，国务院总理李强签署国务院令，公布《网络数据安全管理条例》，自2025年1月1日起施行。条例共9章64条，包括个人信息保护、重要数据安全、网络数据跨境安全管理等内容，旨在细化、补充、完善《网络安全法》《数据安全法》《个人信息保护法》等法律规定的相关制度。具体来说：

一是提出网络数据安全管理总体要求和一般规定。明确鼓励网络数据在各行业、各领域的创新应用，对网络数据实行分类分级保护，积极参与网络数据安全相关国际规则和标准的制定，加强行业自律，禁止非法网络数据处理活动。要求网络数据处理者履行建立健全网络数据安全管理制度、安全风险报告、安全事件处置等义务。

二是细化个人信息保护规定。明确处理个人信息的规则和应当遵守的具体规定。要求网络数据处理者提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。明确使用自动化采集技术等采集个人信息的保护义务，细化个人信息转移请求实现途径等。

三是完善重要数据安全制度。明确制定重要数据目录职责要求，规定网络数据处理者识别、申报重要数据义务。规定网络数据安全管理机构和网络数据安全负责人的责任。明确重要数据风险评估具体要求。

四是优化网络数据跨境安全管理规定。明确网络数据处理者可以向境外提供个人信息的条件，规定可以按照缔结或者参加的国际条约、协定向境外提供个人信息。规定未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。

五是明确网络平台服务提供者义务。规定网络平台服务提供者、第三方产品和服务提供者等主体的网络数据安全保护要求。明确通过自动化决策方式向个人进行信息推送的规则，规定大型网络平台服务提供者发布个人信息保护社会责任年度报告、防范网络数据跨境安全风险等要求。（来源：中国政府网）

（二）部委层面动向

1. 中央网信办与澳门特别行政区政府两部门发布《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》

9 月 10 日，国家互联网信息办公室、澳门特别行政区政府经济及科技发展局、澳门特别行政区政府个人资料保护局发布《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》。指引附件给出《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同》和《承诺书》。

实施指引明确，个人信息处理者及接收方应注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者澳门特别行政区。

实施指引提出，按照本实施指引，通过订立标准合同跨境提供个人信息的，应当履行标准合同列明的义务和责任，包括满足以下条件：（一）个人信息处理者跨境提供个人信息前，应当按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意；（二）不得向粤港澳大湾区以外的组织、个人提供。

实施指引强调，个人信息处理者及接收方应在标准合同生效之日起10个工作日内按照属地向广东省互联网信息办公室或者澳门特别行政区政府个人资料保护局进行标准合同备案，提交承诺书、标准合同和属地监管机构要求的其他材料。（来源：中国网信网）

2. 中央网信办发布强制性国家标准《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》

9月14日，中央网络安全和信息化委员会办公室发布强制性国家标准《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》，提出人工智能生成合成内容显式标识和隐式标识的方法，适用于规范生成合成服务提供者和内容传播服务提供者对人工智能生成合成内容开展的标识活动。

征求意见稿指出，显式标识指能被用户直接感知的标识，主要用途是提示用户当前内容由人工智能生成合成，实现方式包括内容显式标识、交互场景界面显式标识等。隐式标识指用户不能直接感知、不影响用户正常使用，但通过技术手段能从内容中提取的标识，主要用途是记录生成合成

内容信息，实现方式包括元数据隐式标识、内容隐式标识等。（来源：中国网信网）

3. 国家互联网信息办公室发布《人工智能生成合成内容标识办法（征求意见稿）》

9 月 14 日，国家互联网信息办公室发布《人工智能生成合成内容标识办法（征求意见稿）》。

征求意见稿共 14 条。其中，明确人工智能生成合成内容是指利用人工智能技术制作、生成、合成的文本、图片、音频、视频等信息。人工智能生成合成内容标识包括显式标识和隐式标识。服务提供者应当按照有关强制性国家标准的要求进行标识。服务提供者应当在用户服务协议中明确说明生成合成内容标识的方法、样式等规范内容，并提示用户仔细阅读并理解相关的标识管理要求。

征求意见稿强调，提供网络信息内容传播平台服务的服务提供者应当采取措施，规范生成合成内容传播活动：一是应当核验文件元数据中是否含有隐式标识，对于含有隐式标识的，应当采取适当方式在发布内容周边添加显著的提示标识，明确提醒用户该内容属于生成合成内容；二是文件元数据中未核验到隐式标识，但用户声明为生成合成内容的，应当采取适当方式在发布内容周边添加显著的提示标识，提醒用户该内容可能为生成合成内容；三是文件元数据中未核验到隐式标识，用户也未声明为生成合成内容，但提供网络信息内容传播平台服务的服务提供者检测到显式标识或其他生成合成痕迹的，可识别为疑似生成合成内容，应当采取适当方式

在发布内容周边添加显著的提示标识，提醒用户该内容疑似为生成合成内容；四是对于确为、可能和疑似生成合成内容的，应当在文件元数据中添加生成合成内容属性信息、传播平台名称或编码、内容编号等传播要素信息；五是提供必要的标识功能，并提醒用户主动声明发布内容中是否包含生成合成内容。（来源：中国网信网）

4. 国家互联网信息办公室发布《终端设备直连卫星服务管理规定（征求意见稿）》

9 月 27 日，国家互联网信息办公室发布《终端设备直连卫星服务管理规定（征求意见稿）》。征求意见稿共 5 章 41 条，包括发展与促进、设备设施与服务管理、监督管理等内容。

征求意见稿适用于向中华人民共和国境内提供终端设备直连卫星服务，以及在中华人民共和国境内生产、组装、提供、销售和使用支持直连卫星服务的终端设备。其中，终端设备直连卫星服务，是指利用终端设备通过无线通信方式，不经过中转设备，直接连接通信卫星提供语音呼叫、短信收发或数据交换服务的活动。

征求意见稿强调，向中华人民共和国境内提供终端设备直连卫星服务，应当将关口站、地球站等地面设施建设在境内，或者使用境内的地面设施，接入在境内合法运营的地面通信网络。境内用户数据应当在境内地面设施处理，未经批准不得经由卫星转发至境外关口站、地球站等设施。提供和使用终端设备直连卫星服务，涉及数据出境的，应当遵守法律、行政法规和国家有关规定。（来源：中国网信网）

5. 工信部发布《电子认证服务管理办法（征求意见稿）》

9 月 2 日，工信部信息技术发展司发布《电子认证服务管理办法（征求意见稿）》。征求意见稿共 8 章 56 条，旨在修订 2015 年版本，新增和修改多个条款，重点包括强化电子认证服务机构运营管理。

征求意见稿规定，电子认证服务机构应当确保电子签名认证证书及认证相关信息可追溯。电子认证服务机构应当如实上报数据，并将数据接入至国家电子认证服务管理平台。电子认证服务机构应将证书链提交工业和信息化部备案，其电子认证服务应当纳入电子认证信任体系，遵循电子认证服务互信互认要求。

征求意见稿明确，工业和信息化部对电子认证服务机构进行监督检查，内容包括法律法规符合性、安全运营管理、风险管理、投诉处理等。电子认证服务机构应当每年至少进行一次合规性评估，对发现的问题及时整改，并向住所地省、自治区、直辖市工业和信息化主管部门报送合规性评估报告。地方工业和信息化主管部门将合规性评估情况报工业和信息化部。（来源：工信部）

6. 工信部发布《关于推进移动物联网“万物智联”发展的通知》

9 月 12 日，工信部办公厅发布《关于推进移动物联网“万物智联”发展的通知》，围绕夯实物联网络底座、提升产业创新能力、深化智能融合应用、营造良好发展环境、保障措施 5 方面提出 13 条要求。

其中，夯实物联网络底座方面，通知要求加强网络规划建设、提升网络智联能力。基础电信企业要开展移动物联网年度滚动规划，结合需求适

度超前建设移动物联网络。基础电信企业要加快探索人工智能技术在移动物联网络的应用部署，推动实现网络连接、资源管理、运行维护等方面的内生智能，提升网络智能化水平。

营造良好发展环境方面，通知要求完善安全保护机制。基础电信企业要强化移动物联网安全防护能力建设，不断深化移动物联网安全风险评估。加强物联网卡安全管理，严格落实物联网卡安全管控措施，提升物联网模组、终端等设备安全性。加强数据分类分级保护，引导数据处理者加强数据安全防护和风险监测预警能力建设，定期开展数据安全风险评估，不断提升数据安全保护水平。立足国家安全，科学规划物联网网络建设和业务发展，规范落实“三同步”要求。（来源：工信部）

7. 国家数据局发布《关于促进数据产业高质量发展的指导意见（征求意见稿）》

9 月 27 日，国家数据局发布《关于促进数据产业高质量发展的指导意见（征求意见稿）》，围绕加强数据产业规划布局、培育多元经营主体、加快数据技术创新、强化基础设施支撑等 8 方面提出 22 条意见。

加强数据产业规划布局方面，征求意见稿要求优化产业发展结构、促进产业链协同发展、推动数据产业区域聚集；并将数据采集、数据存储、数据治理、数据分析、数据交易、数据应用、数据安全、数据基础设施列为数据技术和产业重点支持方向。

提高数据领域动态安全保障能力方面，征求意见稿要求创新数据安全产品服务、加强动态数据安全保障。推动基础设施安全、数据安全、应用

安全协同发展，加强身份认证、数据加密、安全传输、合规检测等技术创新，培育壮大适应数据流通特征和人工智能应用的安全服务业态。支持企业创新数据分类分级、隐私保护、安全监测、应急处置等数据安全产品和服务。扩大数据空间、区块链、隐私计算等可信流通技术及模式应用范围，增强数据可信、可控、可计量开发利用能力。建立健全数据安全风险识别、监测预警、应急处置等相关规范，落实数据流通利用全过程相关主体的安全责任。健全数据分类分级标准，加强对涉及国家安全、商业秘密、个人隐私等数据的保护。（来源：国家数据局）

8. 国家数据局发布《关于促进企业数据资源开发利用的意见（征求意见稿）》

9 月 27 日，国家数据局发布《关于促进企业数据资源开发利用的意见（征求意见稿）》，围绕健全企业数据权益实现机制、营造开放透明可预期的发展环境等 6 方面提出 16 条意见。

健全企业数据权益实现机制方面，征求意见稿明确，企业对其在生产经营过程中形成或合法获取、持有的数据，依法享有法律法规规定的、民商事合同或行政协议约定的数据权益。保护企业对其合法持有数据的开发利用、经营收益、流通交易等合法权益。企业有权依法或依合同约定，自主或委托他人基于其合法持有数据开发数据产品或提供数据服务。坚持由市场评价贡献、按贡献决定报酬，根据相关主体在数据产品和服务价值形成过程的实际作用，获得与其贡献相称的收益。

营造开放透明可预期的发展环境方面，征求意见稿提出，完善数据联管联治机制，强化部门协调和央地协同。针对新技术应用和新模式新业态，建立容错纠错、尽职免责制度机制，探索运用“监管沙箱”等模式，构建鼓励创新、弹性包容的治理环境。健全政企沟通机制，稳定企业合规预期。推动制定行业数据分类分级标准，健全数据资源开发利用安全技术规范。健全数据安全管理、个人信息保护认证制度。加强对数据领域违法行为的监管，强化行业自律建设，营造公平竞争、规范有序的市场环境。（来源：国家数据局）

9. 十一部门发布《关于推动新型信息基础设施协调发展有关事项的通知》

9 月 4 日，工信部、中央网信办、教育部等十一部门联合发布《关于推动新型信息基础设施协调发展有关事项的通知》，围绕加强全国统筹规划布局、加强跨网络协调联动发展、增强全方位安全保障能力等 8 方面提出 21 条要求。

其中，在增强全方位安全保障能力方面，通知要求，一是提升网络和数据安全保障能力。基础电信企业要加强网络安全设施与信息基础设施协同建设。相关企业要配合开展网络安全能力成熟度评价，强化物联网、人工智能等新技术风险评估，严格落实物联网卡安全管理要求。要建立健全数据安全管理制度，强化重要数据识别备案和分级防护，加强数据安全监测预警和应急处置手段建设，开展数据安全风险评估，提升数据安全保障能力；二是增强跨行业安全服务赋能。各地通信管理局要组织相关单位升

级完善国家工业互联网安全技术监测体系，支持重点工业互联网企业、车联网企业建设网络和数据安全技术监测手段。推广实施工业互联网安全分类分级管理、车联网网络安全定级防护备案，加快安全防护贯标，加强车联网卡实名登记管理；三是增强信息基础设施稳定安全运行能力。各地通信管理局要指导基础电信企业开展运行安全风险评估，严格落实“三同步”要求，对重要网元进行分级分类管理。（来源：工信部）

10. 国家密码管理局发布《电子政务电子认证服务管理办法》

9 月 4 日，国家密码管理局发布《电子政务电子认证服务管理办法》。办法共 6 章 42 条，包括资质认定、行为规范、监督管理等内容。

办法明确，电子政务电子认证服务，是指采用商用密码技术为政务活动提供电子签名认证服务，保证电子签名的真实性和可靠性的活动。从事电子政务电子认证服务的机构，应当经国家密码管理局认定，依法取得电子政务电子认证服务机构资质。

办法指出，电子政务电子认证服务机构应当按照国家密码管理局公布的电子政务电子认证业务规则规范等要求，制定本机构的电子政务电子认证业务规则和相应的电子签名认证证书策略，在提供电子政务电子认证服务前予以公布，并向住所地省、自治区、直辖市密码管理部门备案。电子政务电子认证服务机构应当完整记录和保存与电子签名认证相关的信息，保证认证过程和结果具有可追溯性，信息保存期限至少为电子签名认证证书失效后 5 年。（来源：国家密码管理局）

11. 五部门发布《个人求助网络服务平台管理办法》

9 月 5 日，民政部、中央网信办、工信部等五部门共同发布《个人求助网络服务平台管理办法》，针对专门为因疾病等原因导致家庭经济困难的个人，提供求助信息发布和捐助资金归集、管理、拨付等服务的网络平台进行管理。

办法规定，个人求助网络服务平台，应当经国务院民政部门指定。申请指定为个人求助网络服务平台的，应当已经办理公安机关联网备案手续，并依法开展具有舆论属性或者社会动员能力的安全评估；网络安全保护等级不低于三级，并取得公安机关出具的信息系统安全管理保护备案证明；并且只从事个人求助网络服务，有功能完备的业务系统，具备线上线下服务能力，具备查验通过其发布的求助信息真实性的能力。

办法规定，个人求助网络服务平台应当按照《个人信息保护法》等法律法规规定，加强个人信息保护，规范个人信息处理。发生或者可能发生个人信息泄露、篡改、丢失的，个人求助网络服务平台应当立即采取补救措施，并按规定通知履行个人信息保护职责的部门和个人。个人求助网络服务平台对求助信息的保存时间自求助完成之日起不少于三年。法律法规另有规定的，依照其规定。（来源：民政部）

12. 市场监管总局发布《关于推动网络交易平台企业落实合规管理主体责任的指导意见（征求意见稿）》

9 月 9 日，市场监管总局发布《关于推动网络交易平台企业落实合规管理主体责任的指导意见（征求意见稿）》，围绕健全合规管理组织、明确合规管理职责、完善合规管理运行机制等 4 方面提出 16 条意见。

征求意见稿规定，网络交易平台企业一般应当明确合规负责人。网络交易平台企业根据自身组织架构、业务类型、经营规模、人员数量等因素，结合合规管理工作需要，配备适当数量的合规管理员。

完善合规管理运行机制方面，征求意见稿提出，指导网络交易平台企业将合规管理人员的岗位职责、任职调整、培训考核等情况，以及合规风险管控清单、合规管理人员在履行合规管理职责中形成的文件资料存档备查。网络交易平台企业在合规管理工作中发现的问题，应当按照法律法规要求，主动向主管部门报告。（来源：市场监管总局）

13. 国家金融监督管理总局发布《关于加强银行业保险业移动互联网应用程序管理的通知》

9 月 12 日，国家金融监督管理总局办公厅发布《关于加强银行业保险业移动互联网应用程序管理的通知》，共提出 18 条要求。

通知提出，金融机构应当加强移动应用网络安全管理，严格落实国家网络安全等级保护制度，定期对移动应用进行安全加固，采取加密方式进行数据传输，监测识别异常流量、恶意程序、攻击入侵、安全漏洞、非法

逆向分析破解、代码篡改及重打包等风险，发现问题及时处置。金融机构应当对移动应用注册用户进行有效身份核验。

通知要求，金融机构应当将移动应用风险纳入全面风险管理，识别违规展业、侵害消费者权益等业务风险及网络安全漏洞等科技风险，健全风险防控措施，每年至少开展一次移动应用风险评估，每三年至少开展一次审计，发生重大移动应用风险事件时，应立即开展专项审计。（来源：中国政府网）

14. 六部门印发《国家数据标准体系建设指南》

9 月 25 日，国家发展改革委、国家数据局、中央网信办等六部门印发《国家数据标准体系建设指南》，提出国家数据标准体系建设思路、建设内容等。

建设思路方面，指南提出包含基础通用、数据基础设施、数据资源、数据技术、数据流通、融合应用、安全保障 7 个部分的数据标准体系框架。建设内容方面，指南提出建设基础通用标准、数据基础设施标准、数据资源标准、数据技术标准、数据流通标准、融合应用标准、安全保障标准。（来源：中国政府网）

15. 全国网安标委发布国家标准《网络安全技术 网络身份认证公共服务 应用接入规范（征求意见稿）》

9 月 12 日，全国网安标委发布国家标准《网络安全技术 网络身份认证公共服务 应用接入规范（征求意见稿）》。

征求意见稿提供多种应用接入国家网络身份认证公共服务平台的总体接入框架、接入流程和安全测试方法，规定接入国家网络身份认证公共服务平台的应用服务的安全要求，适用于对接国家网络身份认证公共服务平台的应用服务的设计、开发、测试、运行。（来源：全国网安标委）

16. 全国网安标委发布《网络安全标准实践指南——敏感个人信息识别指南》

9 月 14 日，全国网安标委发布《网络安全标准实践指南——敏感个人信息识别指南》，给出敏感个人信息识别规则以及常见敏感个人信息类别和示例，可用于指导各组织识别敏感个人信息，也可为敏感个人信息处理和保护工作提供参考。

在敏感个人信息识别规则方面，指南提出：（一）符合下述任一条件的个人信息，应识别为敏感个人信息：一是一旦遭到泄露或者非法使用，容易导致自然人的人格尊严受到侵害；二是一旦遭到泄露或者非法使用，容易导致自然人的人身安全受到危害；三是一旦遭到泄露或者非法使用，容易导致自然人财产安全受到危害。（二）常见的敏感个人信息：生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息等。（三）既要考虑单项敏感个人信息识别，也要考虑多项一般个人信息汇聚或融合后的整体属性，分析其一旦泄露或非法使用可能对个人权益造成的影响，如果符合（一）所述条件，应将汇聚或融合后的个人信息整体参照敏感个人信息进行识别与保护。（四）法律法规规定为敏感个人信息的，从其规定。

9月发布的正式版，相较于6月征求意见稿，主要区别在于：一是在敏感个人信息识别规则方面，正式版明确法律法规规定为敏感个人信息的，应当从其规定；二是在附件“常见敏感个人信息类别示例”中，军人、警察身份不作为“特定身份信息”的列举内容，航班高铁出行记录不作为“行踪轨迹信息”的列举内容。（来源：全国网安标委）

（三）地方层面动向

1. 湖南省印发《湖南省数据知识产权登记管理办法（试行）》

8月22日，湖南省市场监督管理局、湖南省高级人民法院、湖南省人民检察院等11部门印发《湖南省数据知识产权登记管理办法（试行）》，自公布之日起施行，有效期两年。

办法共24条，适用于为依法获取并经过一定规则处理形成的，具有智力成果属性和商业价值的，可以电子或其他手段读取、识别或访问的数据集合提供登记服务。

办法规定，申请登记的数据应当进行公证存证或者运用可信技术进行存证，提升数据的可信赖、可追溯水平。申请登记的数据在申请登记前已经进行存证的，应当提供公证存证或者可信技术存证的凭证。数据登记后，申请人可以根据实际需求，开展过程数据的存证和公证，提升全过程动态管理水平。提供数据可信技术存证的平台或者机构，应当符合国家法律法规规定，完善数据安全制度，建立必要的技术防护和运行管理体系。

办法强调，登记证书可以作为数据集合依法持有、加工使用、流通交易、收益分配和权益保护的初步证明，以促进数据要素合理流动、有效保护、充分利用。登记证书的有效期为三年，自登记公告之日起计算。（来源：湖南省市场监督管理局）

2. 山东省济南市发布《济南市公共数据开放利用管理办法》

9 月 4 日，山东省济南市人民政府发布《济南市公共数据开放利用管理办法》，共 29 条。办法所称“公共数据开放主体”（以下简称开放主体），是指国家机关，法律法规授权的具有管理公共事务职能的组织，具有公共服务职能的企业事业单位，人民团体等。

办法规定，开放主体应当依托济南公共数据开放网（以下简称开放网）提供公共数据开放利用服务，不得新建独立的开放渠道。已经建设完成的，应当进行整合、归并，纳入开放网。根据国家规定不能通过开放网开放公共数据的，开放主体应当告知本级大数据主管部门。市大数据主管部门应当建立开放网管理制度，增强数据安全监管和防护能力，保障开放网安全稳定运行。

办法提出，开放主体将公共数据列为不予开放类、有条件开放类的，应当向本级大数据主管部门提供相关依据。市、区县大数据主管部门可以对数据开放属性提出修改意见，与开放主体意见不一致的，由市大数据主管部门确定；重大、疑难的，由市大数据主管部门组织专家论证后确定。（来源：山东省济南市人民政府）

3. 吉林省长春市印发《长春市数据产权登记管理办法》

9 月 10 日，吉林省长春市政务服务和数字化建设管理局印发《长春市数据产权登记管理办法》，共 7 章 34 条，包括登记主体、登记机构、登记行为等内容。

办法规定，登记主体应履行以下义务：一是确保登记申请材料及登记内容的真实性和完整性，确保所登记的数据资源或产品来源合法、内容合规、授权明晰；二是数据资源或产品登记后，登记主体需在保护公共利益、数据安全和数据来源者合法权益的前提下，使用或授权他人使用数据资源，依法使用和处分数据产品。登记主体在经登记机构审核后，获取数据产权登记证书，可为数据交易、融资抵押、数据资产入表、会计核算、争议仲裁提供参考。

办法指出，数据产权登记类型包括首次登记、转移登记、变更登记、续展登记、注销登记。办理转移登记、变更登记、续展登记、注销登记前，需办理首次登记。其中，首次登记是指数据资源或数据产品的第一次登记，是对数据资源或数据产品持有、使用、经营等相关权利归属及相关情况的记录。（来源：长春市政务服务和数字化建设管理局）

4. 广东省深圳市发布《深圳市关于支持数字金融高质量发展的实施意见（征求意见稿）》

9 月 11 日，广东省深圳市地方金融管理局发布《深圳市关于支持数字金融高质量发展的实施意见（征求意见稿）》，围绕推动数字金融主体高

水平集聚、持续优化数字金融创新监管环境、创新营造数字金融发展生态等 4 方面提出 12 项重点任务。

持续优化数字金融创新监管环境方面，征求意见稿提出，用好中国人民银行金融科技创新监管工具、香港金融管理局金融科技监管沙盒、澳门金融管理局创新金融科技试行项目的联网对接机制，在风险可控前提下支持扩大应用推广范围，鼓励监管科技项目进入测试。积极探索监管数字化转型，全面推进非现场监管流程标准化、数字化，全面推进非现场监管流程标准化、数字化，支持对金融机构全周期、金融风险全过程、金融业务全链条动态监管。运用大数据、人工智能等现代技术手段，结合数据模型、典型场景等，加强对非法金融活动监测预警，提升非法集资线索发现、归集研判、分发查核、打击处置等全链条运行效能。（来源：深圳市地方金融管理局）

境内前沿观察三：治理实践

导读：9 月，公安机关、网信部门、通信管理部门陆续启动专项行动或发布专项行动工作成效。从发布内容可以看出，强化监督管理、严厉打击违法犯罪行为与积极引导企业合规、推动行业自律自治均已成为网络与数据安全治理的重要方式。具体来说：

一是依法管网治网，持续强化监督检查和行政执法力度。天津警方公布“净网 2024”专项行动工作成果。天津警方严格落实属地监管责任，督促网络运营者落实安全管理责任，开展执法检查 1885 家次，依法查处存在不履行信息网络安全管理义务等问题互联网企业 6 家次，约谈整改 462 家次。北京市通信管理局启动 2024 年电信和互联网行业网络与数据安全检查，将对企业存在高中危漏洞、僵尸网络、移动互联网恶意程序、恶意主机、数据泄露等安全威胁开展专项治理，依法对相关企业采取通报、约谈、（暂停）停止接入、行政处罚等措施。

二是重视通过公约协议、发布合规指引等方式引导企业落实主体责任。公安机关网安部门在持续高压严打网络违法犯罪、强化网络乱象治理的同时，指导超大型互联网平台切实压紧压实主体责任，充分发挥公约协议的自律自治作用，共同营造清朗网络空间，各大互联网平台积极响应。上海市委网信办组织编写《上海属地网络平台履行未成年人网络保护义务的合规指引（试行版）》，在哔哩哔哩、小红书、阅文集团、喜马拉雅、虎扑等属地重点平台试行。

个案方面，内蒙古、江西、山东等多地公安机关、网信部门发布诸多网络安全行政执法案件，违法行为仍聚焦在网络运营者不履行网络安全保护义务导致网络被攻击篡改和个人信息保护不到位，导致个人信息存在安全风险两方面。具体违法行为包括：1.网络安全意识淡薄、网络安全管理制度不健全；2.未采取有效技术防护措施；3.弱口令等安全漏洞未及时处置；4.公安机关对安全漏洞处以警告的情况下未有效整改，使得网络“带病运行”；5.为便于远程维护，在无技术防护措施的情况下，将IPTV网关设备直接映射在互联网端；6.未对网站、域名进行有效管理，域名到期后不维护；7.未落实网络安全等级保护制度；8.未按规定部署日志设备；9.未对个人信息进行脱敏或去标识化处理。

刑事案件方面，公安机关发布的案件聚焦在网络黑灰产、网络暴力、电信网络诈骗、侵犯公民个人信息等犯罪类型。其中，广东警方公布五起利用苹果手机FaceTime实现通话呼叫功能实施诈骗的新型犯罪案件。浙江绍兴警方捣毁一个开发外卖、快递等行业“外挂”软件、线上线下制售的犯罪产业链，该犯罪团伙涉及金主、开发、破解、卡密、运维、平台、引流、代理、造证等九个层级。

关键词：网络安全监督管理、自律自治、漏洞处置、利用FaceTime实施诈骗、网络暴力

（一）公安机关治理实践

1. 公安机关网安部门指导互联网平台强化自律自治

9月4日消息，公安机关网安部门近日指导互联网平台强化自律自治。

受“流量经济”刺激，个别网民为博眼球、求关注，频繁发布“改头换面、张冠李戴”式不实信息，进行造谣诽谤、恶意炒作，更有甚者，多次发布“移花接木、指桑骂槐”式谣言信息，侮辱谩骂、攻击诋毁他人，或挑起对立、煽动拉踩，借此博取流量，以达快速涨粉、谋取非法利益之目的，严重扰乱社会秩序和网络空间秩序，危害广大网民合法权益。

对此，公安机关网安部门高度重视，在持续高压严打网络违法犯罪、强化网络乱象治理的同时，指导超大型互联网平台切实压紧压实主体责任，充分发挥公约协议的自律自治作用，共同营造清朗网络空间，各大互联网平台积极响应。 有的视频平台发布《关于更新“违规蹭热不当获利”内容治理规范的公告》，明确要求“账号不得借热点事件，仿冒、不当关联当事人与涉事品牌，并借此发布虚假营销信息违规蹭热，引发关注后不当获利”，严禁利用“虚假身份”“虚假内容”“虚假营销”“虚假流量”不当获利。有的内容分享平台发布《关于“违规蹭热”内容治理新公告》，明确提出请勿冒充他人、请勿发布虚假的内容、请勿通过不当方式引流、请勿批量发布同质化低质内容、尊重原创并分享真实内容。有的互联网公司发布《关于进一步加强“体育饭圈”专项整治的公告》，严厉打击对运动员、教练员发布恶意攻击谩骂言论，甚至造谣抹黑、挑动对立，煽动运

动员粉丝群体进行拉踩引战等行为。有的互动平台启动“体育饭圈生态治理”专项行动，并发布相关公告，持续加强违规内容及账号处置，加强用户教育引导与违规行为公示，完善治理措施和手段，让追星行为回归理性，在合法、合规、合理框架之内。（来源：公安部）

2. 全国公安机关重拳打击网络谣言，查处3.1万余人

9月19日，公安部网安局公布全国公安机关打击网络谣言工作情况。

2024年以来，依托“净网2024”专项行动，公安部组织全国公安机关持续开展打击整治网络谣言专项行动，及时发现查处借热点舆情事件进行造谣传谣线索，坚决整治自媒体运营人员移花接木、摆拍造谣等利用网络谣言进行吸粉引流、非法牟利等行为，重拳打击编造虚假险情、灾情、警情等违法犯罪活动。截至目前，全国公安机关网安部门已办理网络谣言类案件2.7万余起，依法查处造谣传谣网民3.1万余人，依法关停违法违规账号19.9万余个，清理网络谣言信息156.2万余条。同期，公安部公布打击整治“移花接木”拼接网络谣言违法犯罪5起典型案例。

案例一：广东公安机关侦办的张某某拼接虚假字幕谣言案。2024年8月，张某某为博流量、吸引关注，在网上下载某国外名人的演讲视频，使用手机视频剪辑软件恶意编辑，并配以与视频原内容无关的中文字幕，恶意制作不实视频信息，在网上发布传播，引发网民误解，造成虚假信息传播扩散，影响恶劣。公安机关已依法对张某某采取刑事强制措施。

案例二：江苏公安机关侦办的徐某某拼接“高速公路交通事故55人死亡”网络谣言案。2024年8月，徐某某为博流量、吸引关注，在网上收集

挑选过往车祸现场图片，拼接整合成视频后进行发布，配文称“常泸高速公路”“55人死亡”等虚假信息。经核实，该视频图片内容均为拼接生成，涉事地点、伤亡人数等信息均为恶意编造，相关信息被传播扩散后，引起恶劣影响。公安机关已依法对徐某某采取刑事强制措施。

案例三：湖北公安机关办理的袁某拼接“公安交警与部队人员发生冲突”谣言案。2024年5月，袁某为博取眼球、吸引流量，在网上发布一段内容“公安交警与部队人员发生冲突，部队派出装甲车”的谣言视频。经查，视频内容系某电视剧片段与网络视频拼接形成。公安机关已依法对袁某处以行政处罚。

案例四：江苏公安机关办理的马某某拼接“南京机场女子排队中暑进大厅休息被安检员拒绝”网络谣言案。2024年7月，马某某为博流量、吸引关注，自行编造拼接图文，造谣“南京某机场一女子排队中暑，进大厅休息被安检员冷漠拒绝”，以视频形式在网上发布，造成虚假信息传播扩散，影响恶劣。公安机关已依法对马某某处以行政处罚。

案例五：青海公安机关办理的童某某拼接“网约车罢工”网络谣言案。2024年5月，童某某为博流量、吸引关注，在网上收集某网约车公司组织旗下网约车集中更换贴图的现场图片，拼接形成“网约车罢工”谣言视频进行发布，造成虚假信息传播扩散，影响恶劣，公安机关已依法对童某某处以行政处罚。（来源：公安部网安局）

3. 公安部公布8起广告推广型网络黑灰产犯罪典型案例

9月2日，公安部公布8起广告推广型网络黑灰产犯罪典型案例。

案例一：北京公安机关破获一起“美女搭讪”型帮助信息网络犯罪活动案。北京公安网安部门侦查查明，某犯罪团伙利用大量虚拟账号，通过设置头像、签名、发帖等方式打造“美女人设”，在社交平台群组和直播间内与网民进行“搭讪”，聊天过程中以邀请对方一起玩游戏、赚钱为由，吸引多名网民在境外赌博网站上注册充值并参与赌博，造成巨大财产损失。北京公安机关抓获犯罪嫌疑人21名，查获作案设备20余部。

案例二：江苏公安机关破获一起“精准获客”型侵犯公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人王某等人通过在平台植入网页监控代码的方式，获取大量特定网站访客信息并对外出售，非法获利数十万元。经查，王某等人自行开发平台监控代码，此代码可植入网站后台系统，当有用户访问该网站时即可获取用户的浏览时间、浏览内容、手机号和设备型号等数据，为需要客户源的商家提供“精准获客”服务，严重侵犯公民个人隐私。江苏公安机关抓获犯罪嫌疑人15名，扣押计算机、手机等涉案设备70余台。

案例三：江苏公安机关破获一起“劫持流量”型破坏计算机信息系统案。江苏公安网安部门侦查查明，犯罪嫌疑人陈某伙同李某共同设计并开发了一个黑客程序，随后串通网吧运维人员在全国20个省市5千余家网吧近20万台电脑中非法植入该黑客程序，直接篡改热门网络游戏配置文件，非法获取各网吧管理系统推广游戏产生的流量，以此获取游戏推广商奖励分成。江苏公安机关抓获犯罪嫌疑人40名，查获涉案金额600余万元。

案例四：江苏公安机关破获一起“强制弹窗”型非法控制计算机信息系统案。江苏公安网安部门侦查查明，犯罪嫌疑人打着“除广告、防病毒”

的旗号，伙同网吧运维人员，在网吧电脑上安装具有修改、替换浏览器进程参数等功能的“某猎手”软件，通过锁定网吧电脑主页、增加网页弹窗来非法控制网吧电脑，为诈骗、赌博等犯罪提供引流服务。江苏公安机关抓获犯罪嫌疑人30名，查封涉案网站2个。

案例五：安徽公安机关破获一起“加工数据”型侵犯公民个人信息案。安徽公安网安部门侦查查明，某犯罪团伙以广告公司名义宣称其持有含银行贷款、股票、教育、医美等多行业品牌APP、公众号的活跃用户数据，利用境内聊天软件进行推广宣传，吸引需要客户源的商家主动联系，确定需要客户数据的种类、平台等。随后犯罪团伙向境外黑客人员购买定制数据，经过加工后出售牟利。安徽公安机关抓获犯罪嫌疑人11名，查封涉案公司3家。

案例六：安徽公安机关破获一起“出海投资”型帮助信息网络犯罪活动案。安徽公安网安部门侦查查明，以张某、陈某、黄某为首的犯罪团伙通过各大社交媒体平台挖掘具有投资需求的用户，根据其投资意向推荐投资项目，以境外投资为由将潜在投资类用户批量引流至境外诈骗团伙的投资平台实施诈骗。境外诈骗团伙按照“引流”成功的人员数量与境内组织者进行资金结算。安徽公安机关抓获犯罪嫌疑人18名，查获作案设备30余部、涉案资金100余万元。

案例七：重庆公安机关破获一起“视频插码”型帮助信息网络犯罪活动案。重庆公安网安部门侦查查明，以康某为首的犯罪团伙为赚取涉黄、赌、诈平台的广告推广费用，接收上游团伙下发的含有赌博、色情等链接的二维码，将相关二维码插入到短视频中，随后利用各类平台账号发布数

十万条已“插码”的短视频，为赌博、色情团伙推广引流。如果网民在观看短视频后不慎扫描二维码，极易被引流至涉及网络色情、网络赌博、网络诈骗的网页，造成巨大经济损失。重庆公安机关抓获犯罪嫌疑人12名，捣毁作案窝点3处，查扣涉案电子设备100余部、涉案资金2000余万元。

案例八：四川公安机关破获一起“募捐红包”型帮助信息网络犯罪活动案。四川公安网安部门侦查查明，刘某利用国内部分企事业单位的网站漏洞，添加虚假“转发分享领红包”的跳转代码，网民在进入该网站后，会自动跳转到领“红包”的页面，并不断提示只要分享微信群、朋友圈即可对“红包”进行提现。但经过多次分享后，却并不能领取到红包，而是会二次跳转到募捐众筹平台页面，为实施众筹骗捐网络诈骗的犯罪团伙推广引流，骗取群众的爱心捐款，实施网络诈骗。四川公安机关抓获犯罪嫌疑人2名，查获涉案资金500余万元。（来源：公安部）

4. 公安部公布10起网络暴力违法犯罪典型案例

9月14日，公安部公布打击整治网络暴力违法犯罪专项行动工作成效。

2024年以来，按照公安部“净网 2024”专项行动统一部署，全国公安机关持续开展打击整治网络暴力违法犯罪专项行动，重拳打击通过网络实施侮辱谩骂、造谣诽谤、侵犯隐私等网络暴力违法犯罪活动，取得阶段性成效。上半年，全国公安机关共侦办网络暴力案件3500余起，依法采取刑事强制措施800余人，行政处罚3400余人。同期，公安部公布10起网络暴力违法犯罪典型案例。

案例一：北京公安机关侦破赵某、成某某实施“开盒”网络暴力案。公安机关查明，犯罪嫌疑人赵某、成某某等人通过黑客等手段非法获取公民个人信息，在网络上“开盒”曝光某虚拟偶像团体成员和“粉丝”等800余人隐私信息，并恶意侮辱谩骂受害人，造成恶劣影响。目前，2名犯罪嫌疑人已被依法采取刑事强制措施。

案例二：辽宁大连公安机关侦破石某某等人实施“有偿代骂”网络暴力案。公安机关查明，犯罪嫌疑人石某某等人为牟取非法利益，发布广告提供“有偿代骂”服务，通过录制辱骂视频、实施电话短信“轰炸”等方式攻击辱骂他人。目前，该团伙6名犯罪嫌疑人已被依法采取刑事强制措施。

案例三：江苏无锡公安机关办理浦某某捏造事实诽谤他人案。公安机关查明，违法人员浦某某在网上讨论“江浙沪独生女被诈骗1.3亿”等不实内容，造谣该不实事件与本地某公司女高管相关联，并将女高管简历、照片等个人信息截图在网上传播扩散，引发网民对该女高管谩骂攻击，损害他人名誉，造成不良影响。目前，公安机关已依法对浦某某处以行政拘留处罚。

案例四：浙江杭州公安机关侦破杨某等人侵犯公民个人信息案。公安机关查明，犯罪嫌疑人杨某等人通过非法手段搜集获取包含姓名、住址、照片在内的大量公民个人信息，并通过“开盒”网暴部分“网红”吸引关注，进而买卖公民个人信息牟取非法利益。目前，该团伙4名犯罪嫌疑人已被依法采取刑事强制措施。

案例五：安徽亳州公安机关侦破常某某传播隐私视频和图片案。公安机关查明，犯罪嫌疑人常某某因与受害人分手后心生怨恨，在网络上散布受害人隐私视频和图片，引起大量网民围观攻击，严重损害受害人身心健康。目前，犯罪嫌疑人常某某已被依法采取刑事强制措施。

案例六：山东青岛公安机关侦破薛某某侮辱、诽谤他人案。公安机关查明，犯罪嫌疑人薛某某为吸粉引流，借受害人家庭纠纷编造虚假信息，多次在直播间通过与粉丝互动等形式辱骂受害人，引起大量网民围观攻击，导致受害人精神失常并产生自杀倾向。目前，犯罪嫌疑人薛某某已被依法采取刑事强制措施。

案例七：山东枣庄公安机关侦破刘某某传播淫秽物品案。公安机关查明，犯罪嫌疑人刘某某通过偷拍、“朋友圈”下载等方式获取他人照片后，利用 AI 软件制作受害人虚假淫秽图片，并添加受害人个人信息后在网络上散布，引起大量网民围观攻击，严重影响受害人正常工作和生活。目前，犯罪嫌疑人刘某某已被依法采取刑事强制措施。

案例八：湖北武汉公安机关侦破周某某等人侮辱、诽谤他人案。公安机关查明，犯罪嫌疑人周某某等人为牟取非法利益，雇佣人员对大量网络用户实施侮辱诽谤等网络暴力行为，导致相关网络用户名誉受损、直播中断、作品被查封，严重扰乱网络公共秩序。目前，该团伙 14 名犯罪嫌疑人已被依法采取刑事强制措施。

案例九：重庆公安机关侦破杨某侵犯公民个人信息案。公安机关查明，犯罪嫌疑人杨某非法获取并在网络上散布受害人手机号、支付宝账号等个

人信息，煽动大量网民通过支付宝转账附言方式辱骂受害人，造成恶劣影响。目前，犯罪嫌疑人杨某已被依法采取刑事强制措施。

案例十：四川成都公安机关侦破万某等人非法利用信息网络案。公安机关查明，犯罪嫌疑人万某、周某某等人通过帮助他人代发短信、代打电话、代举报投诉等方式牟取非法利益，对大量受害人进行侮辱谩骂、造谣诽谤，严重干扰受害人正常工作和生活。目前，该团伙4名犯罪嫌疑人已被依法采取刑事强制措施。（来源：公安部）

5. 浙江警方2024年以来共清理谣言信息7.9万余条

9月14日消息，浙江省公安厅近日发布2024年全省公安机关网安部门清理谣言情况。2024年以来，全省公安机关网安部门以“净网”“护网”行动为抓手，以打开路、打防并举，先后侦破各类涉网案件1234起，移送起诉2976人；组织开展针对企事业单位的网络安全服务活动2.2万余次，成功修复安全隐患1.1万余个；侦办造谣传谣案件610起，清理谣言信息7.9万余条，为维护浙江省社会稳定和网络安靖作出突出贡献。（来源：平安时报）

6. 天津警方“净网2024”专项行动取得阶段性成效

9月19日，公安部网安局公布天津市公安机关“净网2024”专项行动工作成果。截至目前，天津市公安侦破各类网络违法犯罪377起，查处涉案人员370名。

打击网络违法犯罪方面，一是依法严打整治网络谣言、清理违法有害信息。健全完善网络谣言打击查处、辟谣宣传、综合整治的全流程处置工作机制，坚持打防管控一体推进，加大全链条、全平台、全领域打击力度，侦破网络谣言案件17起，依法查处造谣传谣人员203名，清理各类违法有害信息7651条，关停违法违规账号2710个；二是依法严厉惩治网络暴力违法犯罪。重拳打击整治造谣诽谤、谩骂侮辱、侵犯隐私等突出网络暴力违法犯罪行为，侦办网络暴力案件30起，依法查处实施网络暴力涉案人员35名，其中依法采取刑事强制措施2名、行政处罚33名；三是依法严厉打击网络黑灰产、网络水军。深入开展网络黑灰产、网络水军领域线索排查，侦办网络黑灰产、网络水军案件82起，打掉违法犯罪团伙19个，抓获犯罪嫌疑人119名，扣押涉案手机683部、涉案手机卡278张。

依法管网治网方面，一是强化监督检查和行政执法。严格落实属地监管责任，督促网络运营者落实安全管理责任，开展执法检查1885家次，依法查处存在不履行信息网络安全管理义务等问题互联网企业6家次，约谈整改462家次；二是强化互联网备案和安全评估。强化互联网备案和安全评估。夯实全市互联网管理基础，完成备案网站869个，开展安全评估149个；针对APP违法违规，推进重点互联网应用的核验纳管工作，检测发现违法手机APP共3.3万余款，预警阻断涉诈访问1.5亿人次，督促指导相关单位开展注册登记及安全评估，完成备案审核121家、安全评估审核29家；三是强化网络和数据安全保护。监督指导行业部门、企事业单位等全面落实网络安全等级保护制度要求，深入组织开展网络定级备案，定期开展等级测评，完成等级测评系统656个。

同期公布天津公安机关“净网2024”专项行动3起典型案例，分别是：

案例一：冀某使用AI软件杜撰“天津河西女子违停与被堵车主发生肢体冲突”网络谣言案

自2024年8月开始，冀某（男，20岁）为博取流量，将网上热点时事导入AI软件自动撰写编辑、生成大量文章并在网络平台发布。2024年8月11日，冀某通过上述方式生成“天津河西女子违停与被堵车主发生肢体冲突”不实信息，在网络平台上发布，扰乱社会公共秩序。现冀某已被公安机关依法予以行政处罚。

案例二：王某某非法获取“明星航班信息”案

2024年5月，王某某（女，24岁）为拍摄明星航班出站现场照片，从折某（因涉嫌侵犯公民信息罪已被外省市公安机关另案查处）处购买某明星航班信息，经查，该行为属于非法获取公民个人信息行为，严重侵犯公民个人隐私。现王某某已被公安机关依法予以行政处罚。

案例三：天津某信息科技公司非法获取公民个人信息案

2024年5月，公安机关在工作中发现，南开区某婚恋公司长期向天津某信息科技公司购买大量涉及婚恋交友的公民个人信息。经核实，该信息科技公司非法出售公民个人信息共计1万余条，非法获利57万余元。现公安机关已对该信息科技公司负责人潘某某（男，36岁）、杨某某（男，31岁）依法采取刑事强制措施，对曾经向该信息科技公司购买公民个人信息的3家线下婚恋公司依法予以行政处罚。（来源：公安部网安局）

7. 内蒙古警方办理 7 起网络安全行政执法案件

9 月 18 日，公安部网安局公布 7 起内蒙古警方办理的网络安全行政执法典型案例。

案例一：内蒙古呼和浩特市某博物馆不履行网络安全保护义务案

2024 年 3 月 20 日，呼和浩特市公安机关在工作中发现，呼和浩特市某博物馆综合安防管理平台软件 Web 界面被攻击篡改。经查，被攻击篡改的系统为该博物馆的综合安防管理平台，该单位网络安全制度不健全，涉案系统未采取有效的技术防护措施，系统高危漏洞隐患长期暴露于互联网上，导致系统界面被黑客攻击篡改，造成不良后果。呼和浩特市公安机关依据相关法律法规，依法对呼和浩特某博物馆处以行政警告。

案例二：内蒙古锡林郭勒盟某公司不履行网络安全保护义务案

2024 年 7 月 15 日，锡林郭勒盟公安机关接到报案，某煤矿公司的服务器无法正常运行，疑似受到病毒攻击。经现场勘查取证发现，该公司未采取有效防范技术措施，系统存在弱口令等问题隐患，不法分子通过暴力破解密码并在服务器植入勒索病毒，致使该公司的监测服务器无法正常运行，导致安全生产数据无法正常回传，致使其公司业务停摆。锡林郭勒盟公安机关依据相关法律法规，依法对该公司处以行政警告。

案例三：内蒙古通辽某热电公司不履行网络安全保护义务案

2023 年 11 月至 2024 年 7 月期间，通辽市公安机关曾多次对通辽某热电公司进行网络安全监督检查，并对同一个网络安全高危漏洞处以行政警告，但该公司一直未开展有效整改，导致系统长期处于“带病工作”状态，

存在拒不履行网络安全保护义务的行为。通辽市公安机关依据相关法律法规，依法对该公司法人曹某栋、网络安全负责人杨某平分别处以1万元、5仟元的行政罚款。

案例四：内蒙古鄂尔多斯市某事业单位不履行网络安全保护义务案

2024年8月12日，鄂尔多斯市公安机关日常检查时发现，鄂尔多斯市某事业单位APP存在配置错误、敏感信息泄露等高危漏洞，并且该APP具有对外公开性，发布各类新闻公告、宣传动态信息等，后台存储大量工作人员信息和用户人员信息，存在数据泄露和个人信息泄露风险。鄂尔多斯市公安机关依据相关法律法规，依法对该事业单位处以行政警告。

案例五：内蒙古某供应链企业不履行网络安全保护义务案

2024年7月15日，鄂尔多斯市公安机关对鄂尔多斯市某供应链企业开展网络安全监督检查发现，该供应链企业主要开发互联网软件等产品，其网络安全产品服务于多个行业和领域，该企业网络安全保护意识淡薄，安全管理制度缺失，其开发的信息系统存在高危钓鱼漏洞，可导致被服务单位敏感数据泄漏等后果发生。鄂尔多斯市公安机关依据相关法律法规，依法对该供应链企业处以行政警告。

案例六：内蒙古鄂尔多斯市某酒店不履行网络安全保护义务案

2024年3月17日，鄂尔多斯市公安机关对鄂尔多斯某酒店开展日常监督检查发现，该酒店IPTV网关设备登录开机界面被非法篡改。经查，该酒店工作人员网络安全保护意识淡薄，网络安全保护责任落实不到位，网络安全管理制度不完善，工作人员为便于远程维护，在无防火墙等技术防护措施的情况下，将酒店所使用的IPTV网关设备直接映射在互联网端，导致

设备登录开机界面被篡改。鄂尔多斯市公安机关依据相关法律法规，依法对该酒店主管杜某、责任人员苏某分别处以5万元、1万元的行政处罚。

案例七：内蒙古赤峰市某培训学校不履行网络安全保护义务案

2024年4月，赤峰市公安机关对属地网站开展线上巡查时发现，某网站被篡改为赌博网站。经查，该网站为某培训学校于2014年7月14日注册，域名到期后未进行续费和注销操作，无人管理，后被不法人员篡改为赌博网站。同时还发现该企业未按相关规定落实网络安全等级保护制度。赤峰市公安机关依据相关法律法规，依法对该培训学校处以行政警告。（来源：公安部网安局）

8. 因系统登录页面被植入违法信息图片，江西省吉安市警方对一公司处以罚款

9月20日消息，江西省吉安市公安局网安支队近日在工作中发现某电子公司系统登录页面被植入违法信息图片，扰乱网络空间秩序，造成不良影响。经调查，该公司既没有制定、落实网络安全管理制度，也没有部署网络安全技术措施，违反《网络安全法》《数据安全法》关于网络运营者应履行安全保护义务的规定。江西省吉安市公安局依据《网络安全法》对该公司处以罚款1万元，并对直接负责的主管人员处以罚款5000元。（来源：公安部网安局）

9. 因未及时修补网页漏洞导致被黑客入侵，山东省淄博市警方对一物流企业进行处罚

9 月 21 日消息，山东省淄博市警方近日破获一起黑客攻击案，并启动一案双查，依法处罚某物流企业不履行网络安全保护义务的违法行为。

淄博市公安网安部门于 2024 年 2 月接到通报，辖区某物流公司视频监控系统遭到入侵，入侵者将网站主页篡改。接到通报后，网安民警迅速到现场进行现场勘验取证。通过研判、寻线追踪，网安民警很快锁定攻击者身份邓某某。2024 年 3 月 20 日在安徽警方的大力配合下，将邓某某抓获。

经审讯，邓某某对其实施网络攻击的行为供认不讳，经查自今年以来，其利用国内某知名视频监控科技企业平台漏洞，对上万台服务器进行漏洞扫描，对其中 500 余台服务器上传木马文件，并将其中 20 余个系统主页实施篡改的犯罪事实。邓某某明知侵入、控制他人的计算机信息系统并篡改网络信息数据属于犯罪，但在寻求刺激等心态的驱使下，邓某某依然实施网络攻击行为。邓某某因非法控制计算机信息系统罪被淄博警方采取刑事强制措施，目前案件正在进一步侦办中。

警方在追查黑客的同时启动“一案双查”工作机制，针对被攻击的某物流企业履行网络安全保护义务的情况进行检查。经查该企业在系统建设过程中未按规定部署日志设备，也未采取防范网络攻击、网络入侵的技术措施，导致网页漏洞未及时修补从而被黑客入侵篡改。依据《网络安全法》第二十一条、第二十五条、第五十九条第一款，对该企业不履行网络安全保护义务的违法行为，予以处罚。（来源：公安部网安局）

10. 广东省公安厅公布10起打击整治网络暴力违法犯罪典型案例

9月3日，广东省公安厅公布打击网络暴力工作情况。今年以来，全省共依法侦办网络暴力案件289起，查处违法犯罪嫌疑人447人，有力打击各类网络暴力违法犯罪活动。同期，公布10起典型案例。

案例一：胡某以散播私密视频的方式对他人实施网络暴力案

2024年3月，广州胡某与前女友分手后，以散播发布前女友私密视频作为要挟，要求继续与其保持男女朋友关系。被拒绝后，胡某将前女友私密视频发布到多个微信群实施网络暴力行为，造成恶劣影响。属地公安机关依法对其予以刑事拘留。

案例二：吴某某有偿提供短信“轰炸”服务实施网络暴力案

2024年7月，东莞吴某某通过搭建网站，有偿提供短信“轰炸”服务，对107名受害人手机进行高频骚扰、“轰炸”，导致受害人手机在嫌疑人设定的时间内不断弹出短信提醒，从而无法正常使用。属地公安机关依法对其予以刑事拘留。

案例三：李某等人通过造谣生事、恶意炒作等方式对他人恶意滋扰实施网络暴力案

2024年4月，江门李某等人为对他人进行“软暴力”催债，通过各种网络平台造谣炒作，滋扰欠款人及其亲属、同事，甚至通过“恶意网评”对欠款人及其亲属的工作单位进行抹黑，严重影响企业单位的生产经营，扰乱正常社会秩序。属地公安机关收网后依法对27名犯罪嫌疑人采取刑事强制措施。

案例四：唐某某为报复前女友编造谣言实施网络暴力案

2024 年 1 月，肇庆唐某某为报复前女友，利用其前女友的私密图片、视频和联系方式编造“交友”“约会”谣言，再通过境外色情网站传播扩散，导致其前女友不断收到网民辱骂与“约会”信息，工作和生活受到严重影响。属地公安机关依法对其予以刑事拘留。

案例五：张某有偿提供辱骂他人服务实施网络暴力案

2024 年 5 月，广州张某在某交易平台有偿提供辱骂他人服务（累计辱骂 80 余人次），每次收费 8 至 9.9 元不等，相关行为已干扰他人正常生活，造成不良影响。属地公安机关依法对其作出行政拘留处罚。

案例六：黄某某编造谣言诋毁前男友实施网络暴力案

2024 年 3 月，深圳黄某某与前男友分手后存在纠纷，为诋毁前男友，黄某某将前男友照片修改为遗像，配上出殡背景音乐，并搭配文字污蔑前男友吸毒、前男友母亲卖淫，在短视频平台发布、扩散。属地公安机关依法对其作出行政拘留处罚。

案例七：马某某编造发布侮辱他人视频实施网络暴力案

2024 年 2 月，河源马某某因感情纠纷在短视频平台发布由多张受害者照片编辑成的视频，并附上受害者身份证、社交账号等信息，且搭配低俗、侮辱性文字，引发网民围观，造成不良影响。属地公安机关依法对其作出行政拘留处罚。

案例八：徐某某为发泄私愤辱骂、诅咒受灾群众实施网络暴力案

2024年6月，梅州徐某某为发泄私愤，通过短视频平台在多个防汛救灾视频下发布辱骂、诅咒受灾群众的评论，引起众多网民关注，造成恶劣影响。属地公安机关依法对其作出行政拘留处罚。

案例九：邓某某捏造事实公然侮辱他人实施网络暴力案

2024年1月，东莞邓某某因对工资金额不满，为发泄个人私愤，多次在短视频平台发布雇主及雇主妻子的照片和视频，并配有大量侮辱诽谤文字，对受害者工作、生活造成严重影响。属地公安机关依法对其作出行政拘留处罚。

案例十：欧某某恶意抹黑侮辱、散布他人隐私信息实施网络暴力案

2024年4月，云浮欧某某为发泄个人私愤，多次编造不实信息对黄某某恶意抹黑侮辱，并配上黄某某及其女儿的照片和个人信息，通过多个短视频平台传播，使黄某某被大量电话骚扰，工作、生活受到严重影响。属地公安机关依法对其予以行政处罚。（来源：广东公安）

11. 广东省公安厅公布5起打击利用FaceTime实施诈骗犯罪典型案例

9月24日消息，今年3月以来，广东省公安厅发现利用苹果手机FaceTime实现通话呼叫功能实施诈骗的新手段，此类作案手法涵盖虚假征信、冒充公检法、冒充客服等类别案件，省公安厅迅速组织多地深入研判，重拳出击，打早打小，局部开展多波次收网打击，并率先在全国范围内发起针对利用苹果手机FaceTime实施诈骗新型犯罪的规模性打击行动。行动

以来，全省共打掉该类诈骗团伙127个，抓获犯罪嫌疑人1056名。同期，公布5起相关典型案例。

案例一：省市公安机关开展“铲诈4号”集群专案收网行动取得重大战果

2024年3月，广东省公安厅组织广州、深圳、佛山、韶关等15个地市发起“铲诈4号”集群战役，对利用苹果手机FaceTime实施诈骗产业链条开展统一收网打击，成功抓获犯罪嫌疑人156名，有效遏制该类犯罪蔓延趋势。为进一步对该类犯罪开展深度打击，4月，省公安厅组织广州市公安机关率先在全国范围内发起针对利用苹果手机FaceTime实施诈骗新型犯罪的规模性打击行动，并成功打掉一个成员遍布全国多地的特大诈骗团伙，抓获包含指挥开工、设备代挂、账号出租等多个环节在内的犯罪嫌疑人434名，核破全国诈骗案件890宗，涉案金额约6000万元，实现对该类犯罪团伙的全链条打击。

案例二：河源打掉利用FaceTime实施诈骗的本地窝点

2024年4月，广东省公安厅指导河源市公安机关对FaceTime黑灰产、高频开卡、高频外呼运营商模型线索进行深挖扩线、研判攻坚，发现该市源城区2个诈骗窝点。该诈骗团伙公司化运作，以虚假人设、统一话术、营造氛围等方式获取信任、增进感情，最后通过赠送廉价酒水收取高额“运费”、哄骗对方到指定“店铺”（实为该诈骗团伙虚构）购买并赠送名贵手提包等物品，诈骗受害人钱财。4月19日至29日，省公安厅组织河源市公安机关开展统一收网，打掉2个诈骗窝点，抓获犯罪嫌疑人154名，全链条打击利用FaceTime实施诈骗的本地窝点。

案例三：深圳打掉4个利用FaceTime引流的代运营类诈骗窝点

2024年4月，广东省公安厅组织深圳市公安机关针对隐匿在本地的电诈链条进行研判攻坚，发现4个利用FaceTime引流的代运营类诈骗窝点。该诈骗团伙以“轻松月入数万”等噱头诱导受害人购买某短视频平台代运营课程，后谎称客户目前套餐不适合业务发展，引诱升级高价代运营套餐以实施诈骗。4月25日至30日，广东省公安厅组织深圳市公安机关开展统一收网行动，规模性打击代运营类诈骗产业链条，打掉4个诈骗窝点，抓获犯罪嫌疑人139名。

案例四：惠州成功捣毁多个涉FaceTime诈骗窝点

2024年3月，惠州市公安机关根据省公安厅下发线索摸排发现，在辖区内有多个通过苹果手机FaceTime视频通话拨打诈骗电话的窝点，进一步开展研判经营，研判出省内外嫌疑人100余名。4月24日至29日，在省公安厅组织下，惠州市公安机关发起“铲诈10号”集群战役收网行动，抓获犯罪嫌疑人109名。

案例五：中山捣毁一批为诈骗提供通话技术支撑的犯罪窝点

2024年5月，中山市公安机关经过缜密侦查，发现一个为FaceTime诈骗提供通话技术支撑的犯罪窝点藏匿于某出租屋内，并围绕该窝点深挖扩线，发现一批隐匿在省内外的犯罪嫌疑人。5月25日至6月11日，中山市公安机关发起“铲诈19号”集群战役收网行动，抓获犯罪嫌疑人117名。（来源：广东公安）

12. 山西省高平市警方成功捣毁一侵犯公民个人信息窝点

9 月 3 日消息，山西省高平市警方近日成功捣毁一个侵犯公民个人信息窝点。

高平市公安局网安大队近日在工作中发现多条疑似从事出售公民个人信息违法活动线索。经侦查发现毕某某有重大作案嫌疑。经查，2024 年以来，犯罪嫌疑人毕某某在网络社交平台创建多个群组，并将非法获取的公民手机号码、短信验证码提供给其他不法人员进行非法获利。高平市警方经深挖细查，成功捣毁窝点，抓获犯罪嫌疑人 6 人，查扣涉案手机 2800 余部，电脑主机 15 台，硬盘 7 个。目前，犯罪嫌疑人毕某某因涉嫌侵犯公民个人信息已被采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

13. 福建警方发布 7 起“净网 2024”专项行动典型案例

9 月 14 日，福建警方发布 7 起“净网 2024”专项行动典型案例。

案例一：沈某某等人帮助信息网络犯罪活动案

2024 年 4 月，漳州市公安机关打掉两个以沈某某等人为首的犯罪团伙，捣毁犯罪窝点 5 个。经查，该团伙利用非法渠道批量注册、收购网络账号，并通过虚构人设，吸引网民添加好友，为电信网络诈骗犯罪团伙提供引流服务。目前，属地公安机关已对犯罪嫌疑人依法采取刑事强制措施。

案例二：黄某等人非法支付结算案

2024 年 4 月，三明市公安机关打掉一个以黄某为首的非法支付结算犯罪团伙，抓获犯罪嫌疑人 6 名。经查，该犯罪团伙通过网络进行虚拟币担

保交易，采取代缴电费、燃气费、电话费等手段，为电信网络诈骗犯罪团伙提供资金非法结算服务。目前，该案已依法移送检察机关审查起诉。

案例三：林某等人侵犯公民个人信息案

2024年7月，福州、三明、龙岩市公安机关打掉以林某等人为首的多个侵犯公民个人信息犯罪团伙，破获系列案件14起。经查，该团伙通过房产、租赁、建材等行业渠道，非法收集、贩卖公民个人信息，严重危害公民个人信息安全。目前，该案已依法移送检察机关审查起诉。

案例四：黄某等人网络盗窃案

2024年7月，厦门市公安机关打掉一个以黄某为首的黑客犯罪团伙，破获利用网站漏洞对电商平台实施盗窃的系列案件5起。经查，该团伙非法获取网站密钥，对多个电商平台实施盗窃、销赃牟利，严重危害网络安全秩序和民营企业合法权益。目前，犯罪嫌疑人已被依法批准逮捕。

案例五：薛某某等人网络诈骗案

2024年8月，莆田市公安机关成功打掉一个在直播平台实施网络诈骗的犯罪团伙。经查，该团伙利用游戏玩家欲快速获取游戏装备的心理，引诱网民参与网络抽奖活动，并以“购买中奖装备”为由实施诈骗。目前，属地公安机关已对犯罪嫌疑人依法采取刑事强制措施。

案例六：江某某发布网络谣言案

2024年8月，南平市公安机关接群众举报：网民江某某在社交平台上发表评论称“8月5日晚上武夷山市区发生命案”“有人被杀”。该言论迅速引发网民关注、评论，并引起恐慌。经查，网民江某某等人看到民警出

警，不了解实情，而主观猜测民警出警原因，并编撰发生命案谣言。属地公安机关现已依法对江某某处以行政处罚。

案例七：周某某实施网络暴力案

2024 年 4 月，泉州网民周某某因与他人存在矛盾纠纷，遂在某视频平台发布视频，公开对方手机号，并恶意诅咒对方家人。鉴于周某某侵犯他人合法权益，扰乱社会公共秩序，属地公安机关依法对其处以行政处罚。（来源：公安部网安局）

14. 四川省遂宁警方公布 10 起涉网违法犯罪典型案例

9 月 15 日，四川省遂宁警方公布 10 起涉网违法犯罪典型案例。

案例一：李某等人侵犯公民个人信息案

2022 年以来，李某等人通过手机群控设备和软件批量注册多个网络平台新用户，帮助商户刷虚假好评、点赞、收藏，提升其知名度和推荐排名，严重扰乱破坏市场公平竞争秩序。2024 年 7 月，李某等 8 名犯罪嫌疑人被公安机关依法采取刑事强制措施。

案例二：涂某某、文某、徐某某等人涉嫌非法获取计算机信息系统数据案

2024 年 4 月，涂某某等人通过搭建嗅探“伪基站”设备，非法捕获公民个人手机号码及验证码，并以 5-10 元不等的价格出售给他人，非法获利 20 万余元。2024 年 6 月，涂某某等 4 名犯罪嫌疑人被公安机关依法采取刑事强制措施。

案例三：张某等人提供侵入计算机程序、工具案

2022年5月以来，张某等人开发虚假文章生成小程序和“防封”系统，出售给网民从事非法引流活动。购买者通过制作、传播“标题党”网文，植入色情、赌博等非法广告，诱骗网民转发，非法谋取利益。2024年3月，张某等2名主要嫌疑人已被法院判处1年不等有期徒刑，涉及全国多地购买者依法被采取刑事拘留或予以行政处罚。

案例四：熊某破坏计算机信息系统案

2023年以来，熊某通过编写“超强短信轰炸机”软件，搭建“呼死你”网站，非法获利10万余元。该软件通过电话、短信的狂轰乱炸，实现对目标对象的骚扰效果，严重干扰正常工作生活。2024年6月，熊某被法院依法判处有期徒刑3年，缓刑5年，并处罚金3万元。

案例五：奉某、唐某等人破坏计算机信息系统案

2023年以来，奉某等人实施黑客行为，对多个黑灰网络平台实施DDOS攻击直至瘫痪，实施网络“黑吃黑”；通过技术手段扫描多个平台漏洞实施渗透，窃取房产、购物等数据贩卖牟利。2023年8月，奉某等4名犯罪嫌疑人被公安机关依法采取刑事强制措施。

案例六：冯某等人帮助信息网络犯罪活动案

2022年以来，冯某、向某等人以轻轻松松日入千元的由头，诱惑他人入伙，在泸州、重庆、成都等地搭建VOIP通讯窝点，为境外诈骗团伙实施电诈提供技术支撑。2024年3月，向某、冯某等13名犯罪嫌疑人分别被法院依法判处6月至2年6个月不等有期徒刑。

案例七：李某、黄某开设网络赌场案

2024年7月，李某、黄某等人在2024欧洲杯比赛之际，在网络群主开设赌博堂口，招揽30余人从事网络赌球活动，涉案资金高达70余万元，李、黄二人从中获利20余万元。目前，李某、黄某已被公安机关依法采取刑事强制措施。

案例八：胡某帮助网络信息犯罪活动案

2024年以来，胡某等人组织他人购买大量虚拟身份，使用特定软件向网民发送擦边、挑逗言语等二维码图片，将网民引流至色情平台，并从中获取非法利益。目前，胡某等3名犯罪嫌疑人已被公安机关依法采取刑事强制措施。

案例九：冯某等人侵犯公民个人信息案

2023年7月以来，冯某等人冒充移动公司工作人员，以新用户赠送面条、纸巾等礼物的由头，骗取群众的电话号码用于注册网络虚拟身份，以每条3.5元至50元的价格贩卖给他人从事“网络水军”活动。2024年4月，冯某等16名犯罪嫌疑人被公安机关依法采取刑事强制措施。

案例十：董某某非法制造火药案

2024年以来，董某某多次在网上购买碳纤维管子、铝合金管子等材料，非法自制“吹箭”管子、火药等违禁物品。2024年4月，董某某被公安机关依法予以处罚。（来源：公安部网安局）

15. 重庆警方公布7起网络暴力违法犯罪典型案例

9月20日，重庆警方公布打击网络暴力违法犯罪活动工作成效。重庆警方在“净网2024”专项行动期间，共侦办网络暴力案件90起，依法查处

实施网络暴力涉案人员96名，其中依法采取刑事强制措施7名、行政处罚89名。同期，公布七起典型案例。

案例一：江津区公安局依法查处张某遭他人“开盒”被实施网络暴力案

2024年5月，江津区张某遭他人网络“开盒”，证件照片被公布到QQ群后遭人网暴，张某的工作和生活遭受严重影响。属地公安机关查明，张某信息系江苏蒋某倒卖，同时查明该蒋多次倒卖公民个人信息非法获利一万余元。经属地公安机关依法对蒋某予以刑事拘留处罚。

案例二：梁平区公安局依法查处赖某某散布他人隐私信息实施网络暴力案

2024年5月以来，梁平区赖某某在网络社交平台上虚构总裁身份与被害人建立网恋关系，期间获取被害人多张隐私照片和私密聊天视频。两人分手后，为胁迫被害人见面并发生性关系，赖某某多次通过网络社交平台和短视频平台散布被害人隐私信息，造成被害人名誉受损，生活受到严重影响。属地公安机关依法对赖某某予以刑事拘留处罚。

案例三：丰都县公安局依法查处刘某散布传播他人隐私照片实施网络暴力案

2024年4月，丰都县刘某与被害人分手后，想继续保持恋爱关系并被拒绝。刘某遂将被害人的裸照通过网络社交平台发送给被害人的亲友，并对其进行诋毁、侮辱，严重影响被害人的正常生活。属地公安机关依法对刘某予以行政拘留处罚。

案例四：忠县公安局依法查处周某某捏造、散布侮辱信息实施网络暴力案

2024年4月，忠县周某某因与被害人存在矛盾，为报复和泄愤，收集被害人的私人生活照片发布在短视频平台，并配文虚构被害人私生活不检点等信息，对被害人工作、生活造成严重影响。属地公安机关依法对周某某予以行政拘留处罚。

案例五：秀山县公安局依法查处安某捏造、散布侮辱信息实施网络暴力案

2024年5月至7月期间，秀山县安某为发泄私愤，多次将被害人照片、电话号码等个人信息编辑成低俗且带有侮辱文字的视频发布至短视频平台，造成被害人被大量电话骚扰，工作和生活受到严重影响。属地公安机关依法对安某予以行政拘留处罚。

案例六：石柱县公安局依法查处刘某某散布、传播隐私信息实施网络暴力案

2024年5月，石柱县刘某某追求被害人未果，在其家中偷偷安装摄像头伺机报复。在获取被害人隐私照片后，通过网络社交平台和短视频平台进行传播，对被害人工作、生活造成严重负面影响。属地公安机关依法对刘某某予以行政拘留处罚。

案例七：长寿区公安局依法查处刘某某造谣诽谤实施网络暴力案

2024年4月至5月期间，长寿区刘某某与被害人因劳资纠纷怀恨在心，多次编造不实信息恶意抹黑侮辱被害人，并通过短视频平台进行传播，对

被害人工作、生活造成严重负面影响。属地公安机关依法对刘某某予以行政拘留处罚。（来源：重庆网警）

16. 新疆公安机关公布“净网2024”专项行动10起典型案例

9月23日，新疆公安机关公布“净网2024”专项行动10起典型案例：

案例一：叶某等人侵犯公民个人信息案。2024年3月，阿勒泰公安机关打掉一个以叶某为首的侵犯公民个人信息犯罪团伙，抓获犯罪嫌疑人4人，破获系列案件26起。经查，2023年以来，该团伙非法收购他人实名注册互联网虚拟账号，供电诈赌博犯罪团伙使用，非法获利12万余元。目前，该案已依法移送检察机关审查起诉。

案例二：依某等人帮助信息网络犯罪活动案。2024年7月，和田公安机关打掉一个以依某为首的帮助信息网络犯罪活动团伙，抓获犯罪嫌疑人3人。经查，依某等人利用两部手机，一部通过网络软件连接境外诈骗分子，另一部本地手机拨打国内受害人电话，实施语音中转，参与电诈犯罪活动，非法获利6万余元。目前，公安机关已依法对犯罪嫌疑人采取刑事强制措施。

案例三：李某传授犯罪方法案。2024年2月，喀什公安机关侦办1起利用网络非法售卖窃听窃照工具并教授他人实施违法犯罪案。经查，犯罪嫌疑人李某通过网络售卖赌博作弊工具设备，并线下教授购买人使用方法进行赌博，李某以抽取赌资方式非法获利3.8万余元。目前，该案已依法移送检察机关审查起诉。

案例四：阿某等人复制、贩卖、传播淫秽信息牟利案。2024 年 4 月，乌鲁木齐公安机关侦办 1 起复制、贩卖、传播淫秽信息牟利案。经查，犯罪嫌疑人阿某先后购买 17 个具有一定粉丝量的微信公众号，大量发布淫秽信息非法获取高额利润。目前，该案已依法移送检察机关审查起诉。

案例五：吴某某组织网络赌博案。2024 年 5 月，乌鲁木齐公安机关侦办 1 起利用网络平台组织赌博案。经查，犯罪嫌疑人吴某某利用赌彩平台组织网民进行赌博，非法获利 30 余万元。目前，公安机关已依法对犯罪嫌疑人采取刑事强制措施。

案例六：张某涉嫌非法经营案。2024 年 4 月，乌鲁木齐公安机关侦办 1 起借助网络平台为他人有偿删帖、虚假刷屏、造谣引流的“网络水军”案。经查，犯罪嫌疑人张某利用搭建中介平台为他人进行点赞、刷粉，非法获利 5 万余元。目前，公安机关已依法对犯罪嫌疑人采取刑事强制措施。

案例七：马某散布网络谣言案。2024 年 6 月，昌吉公安机关工作发现，网民马某通过今日头条平台恶意造谣散布本地一居民因扶摔倒老人，却被老人儿子诬告的谣言信息。目前，公安机关已依法对其处以行政处罚。

案例八：崔某某组织考试作弊案。2024 年 5 月，伊犁公安机关侦办 1 起利用网络实施考试作弊案。经查，崔某某在某资格考试中线下组织好友利用即时通讯工具实施考试作弊活动。目前，公安机关已依法对其处以行政处罚。

案例九：刘某等人破坏计算机信息系统案。2024 年 8 月，乌鲁木齐、昌吉、阿勒泰公安机关联合打掉一个以刘某为首的非法利用加油机作弊设备实施违法犯罪团伙，抓获犯罪嫌疑人 4 人。经查，刘某等人成立某新能

源有限公司，在网上采购加油机作弊设备，自 2022 年 3 月至案发从事工地车辆加油业务，利用加油机计量作弊设备调整实际出油量，非法牟利 200 万余元。目前，公安机关已依法对犯罪嫌疑人采取刑事强制措施。

案例十：库某实施网络暴力案。2024 年 5 月，伊犁公安机关侦办 1 起利用网络直播平台实施网络暴力案。犯罪嫌疑人库某自 2022 年 5 月从事网络平台直播，频繁在直播期间谩骂他人，以达到提高账号关注度、增多粉丝数量目的，且库某曾于 2022 年 10 月、2024 年 3 月在网络平台直播间公然谩骂、侮辱他人被公安机关行政处罚。目前，该案已依法移送检察机关审查起诉。（来源：新疆网警）

17. 浙江省绍兴市新昌警方捣毁开发“外挂”软件、线上线下制售的犯罪产业链

9 月 26 日消息，浙江省绍兴市新昌警方近日成功捣毁一个以开发“外挂”软件、线上线下制售，金额达 3000 万元的犯罪产业链。

2023 年 11 月 10 日，新昌县公安局七星派出所民警走访得知，不少外卖骑手在抢单过程中使用“黑科技”，能够自动在更短时间内抢到金额更大的单子。民警发现这所谓的“黑科技”只是一个外挂软件“死神”，经过几轮优化升级，已经演化为“雷神”“波点”等多个软件，在全国范围内均有兜售。在插件相关的营销页面上，非法销售人员宣称：骑手花几十块钱买到一个激活码后，即可通过该外挂软件非正常抢单。

新昌公安网安部门在互联网平台安全部门的支持配合下，组建省市县三级联合专案组开展专案研判，先后组织多次跨省抓捕行动，出动 120 余

名警力奔赴13省23个城市，抓获39名嫌疑人，扣押涉案手机71只、电脑8台，固定3个后台卡密服务器数据。据统计，全案涉案金额达3000余万元。了解到该案件规模之大、牵连甚广，2024年7月2日，警方发起集群战役，截至目前，已抓获违法犯罪嫌疑人112名（其中，刑事打击14人，行政处罚2人），批评教育71人。

专案组结合线下审讯进行扩线研判，一个涉及金主、开发、破解、卡密、运维、平台、引流、代理、造证等九个层级的全链条犯罪团伙浮出水面。该作案团伙上下游分工明确，结构清晰，从软件开发到渠道销售、运维等，全链路均涉及，并由不同人员负责。销售人员以该外挂软件自动优先抢金额大、性价比高的订单为卖点，通过朋友圈、自媒体平台以及线下张贴广告等渠道进行兜售，并同步上传使用教程。

该案摧毁了目前市面上涉及外卖、货运、快递等App插件的主要黑灰产业链。办案民警表示，此类外挂软件通过非法读取各类App的订单框架，设置抢单条件，实现自动化、定制化抢单功能。目前各类插件的市场均价在150-200元每月，以被告人卢某为例，仅6个月就违法获利超17万余元。案件侦破后，警方从相关平台了解到，目前使用外挂抢单的从业人员工作账号已被严格管控。

该案中为首的犯罪嫌疑人卢某已被依法判处有期徒刑三年半，李某被依法判处有期徒刑一年两个月。案件仍在进一步侦查办理中。（来源：公安部网安局）

（二）网信部门治理实践

1. 北京网信办暑期整治未成年人网络环境，已处置 2.3 万余个违法违规账号

9 月 3 日，北京市网信办公布“清朗·2024 年暑期未成年人网络环境整治”专项行动工作成效。自专项行动启动以来，北京市网信办暑期属地重点网站平台拦截清理涉未成年人违法违规信息 130 余万条，处置违法违规账号 2.3 万余个。

北京市网信办指导属地重点网站平台结合自身产品类型和未成年人上网特点，全面排查产品服务，重点巡查未成年人较为活跃的产品功能和位置版块。针对一些重点问题，北京市网信办指导各平台结合产品特点，对将“二次包装”经典动画、摆拍校园霸凌视频、发布诱导不良交友等 6 个环节 26 项突出问题逐一细化，制定整改方案，及时通报典型处置案例。北京市网信办还督促属地网站按照能用、好用、爱用的标准积极创新改进青少年模式。

此外，北京市网信办坚持将集中治理和长效建设相结合，指导网站健全未成年人网络保护机制，并作为长期重点工作向深入推进。督促属地网站提取涉未成年人违法违规信息共性特征，提高关键词过滤精准度；强化专项培训，提升审核人员对涉未成年人有害信息的识别能力和敏感意识。（来源：网信北京）

2. 因未对公示的个人信息进行脱敏或去标识化处理，江西省南昌市网信办对某学校作出行政处罚

9 月 12 日消息，江西省南昌市网信办近日接上级网信部门通报，南昌市某学校网站上发布的公示信息附件中含有大量学生姓名、身份证号等明文信息，存在个人信息泄露风险。

经过立案调查、远程勘验、现场勘验、笔录问询等工作，查明该学校未采取技术措施和其他必要措施，对公示附件中的学生名字、身份证号等 4000 多条个人信息开展脱敏或去标识化处理，导致信息泄露风险。相关行为违反《网络安全法》第四十二条第二款。南昌市网信办依据《网络安全法》第六十四条第一款，对该学校处以警告。（来源：网信南昌）

3. 因终端感染木马病毒持续对外发起网络攻击，江西省南昌市网信办对属地某企业作出行政处罚

9 月 30 日消息，江西省南昌市网信办近日在日常网络安全监测中发现，属地企业所属 IP 疑似被黑客远控，频繁对外发起网络爆破攻击。

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，查明该企业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，未采取防范计算机病毒和网络攻击等危害网络安全行为的技术措施；该企业未及时处置计算机病毒、网络攻击等安全风险，所属终端感染木马病毒，持续对外发起网络攻击，导致产生危害网络安全的后果。相关行为违反《网络安全法》第二十一条、第二十五条。南昌市网信办依据《网络安全法》第五十九条，对该企业作出

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）

（三）通信管理部门治理实践

1. 北京市通信管理局开展2024年电信和互联网行业网络与数据安全检查

9月4日，北京市通信管理局发布通知，开展2024年电信和互联网行业网络与数据安全检查。

检查针对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。

检查分为自查自纠、通报处置、重点抽查、整改问责四个阶段，其中，北京市通信管理局依托工业和信息化部的网络安全威胁共享平台和北京市通信管理局监测数据，对企业存在高中危漏洞、僵尸网络、移动互联网恶意程序、恶意主机、数据泄露等安全威胁开展专项治理，依法对相关企业采取通报、约谈、（暂停）停止接入、行政处罚等措施。（来源：北京通信业）

2. 工信部、多地通信管理局通报侵害用户权益行为的APP

（1）工信部

9 月 29 日，工信部信息通信管理局通报 2024 年第 8 批，总第 43 批侵害用户权益行为的 APP（SDK）。通报指出，工信部近期组织第三方检测机构进行抽查，共发现 21 款 APP 及 SDK 存在侵害用户权益行为，所涉问题包括信息窗口“摇一摇”乱跳转、违规收集和使用个人信息等。

（2）浙江省

9 月 26 日，浙江省通信管理局通报 2024 年第 8 批侵害用户权益行为的 APP 名单。通报指出，浙江省通信管理局近日组织第三方检测机构对群众关注的学习教育、本地生活、网上购物等类型 APP 进行检查，并书面要求违规 APP 开发运营者限期整改。截至目前，尚有 19 款 APP 未按要求完成整改。上述 APP 开发运营者在 9 月 30 日前完成整改落实工作，整改落实不到位的，将视情采取下架、关停、行政处罚等措施。

（3）北京市

9 月 27 日，北京市通信管理局通报 2024 年第九期问题 APP。

一是通报 2 款存在问题的 APP。通报指出，北京市通信管理局近日通过抽测发现部分 APP 存在侵害用户权益和安全隐患类问题。截至目前，尚有 2 款 APP“17K 小说”和“爱日语”未整改或整改不到位。

二是下架 4 款 APP。通报指出，北京市通信管理局 8 月 30 日通报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 4 款 APP 未整改或整改不到位，予以全网下架处置。

（4）广东省

9 月 29 日，广东省通信管理局通报 14 款未按要求完成整改的 APP 名单。通报指出，广东省通信管理局持续开展 APP 隐私合规和数据安全专项整治

行动，发出《违法违规APP处置通知》责令APP运营者限期整改，并通知相关应用商店协助督促APP运营者整改。截至目前，尚有14款APP未完成整改。被通报的APP应在10月10日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施。

同日，广东省通信管理局发布通报，下架3款侵害用户权益的APP。通报强调，截至通报规定时限，经核查复检，尚有3款APP未按照要求完成整改反馈。为严肃处理上述APP的违规行为，广东省通信管理局决定对该APP予以下架。相关应用商店应立即组织对该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。（来源：工信部、浙江省通信管理局、北京市通信管理局、广东省通信管理局）

（四）其他部门治理实践

1. 上海多部门联动加强未成年人网络保护，发布系列活动成果

9月9日，上海市委网信办公布各部门未成年人网络保护工作成效。

为加强未成年人网络保护工作,7月初上海市委网信办会同市精神文明办、市检察院、市文旅局执法总队、市公安局网安总队等部门开展“清朗守护·为你而来”上海市未成年人网络保护系列主题活动。近两个月来，各部门在通力合作、联合惩治、联合普法等方面取得一系列成果。

其中，专项整治行动方面，市委网信办累计清理涉未成年人违法违规信息354万余条，处置违法违规账号8.2万余个，下架违规商品数量1457个、封禁违规群聊4181个、违规话题637个。对平台用户发布危害未成年人身心健康信息、发布未成年人个人信息、对未成年人恶意损害形象等案件予以查处。市区两级文化执法部门开展未成年人网络保护专项巡查，共出动执法人员1087人次、检查企业834家次，办理一批网络出版、网络视听等领域涉未成年人网络保护案件，关停相关违法违规网站。

全市两级公安网安部门对未成年人用户规模较大的互联网企业开展排摸纳管工作，纳管互联网企业约130余家；对未成年人注册用户量较大的本市互联网企业开展针对内容审核、身份信息核验等方面的专项执法监督检查，共制发公安提示函600余份。全市三级检察机关突出整治胁迫、教唆、引诱、欺骗未成年人参与电信网络诈骗、帮助信息网络犯罪等涉网络犯罪，暑期清朗行动期间共办理相关刑事案件71件。聚焦未成年人网络保护领域深化未检综合履职，办理民事、行政、公益诉讼检察案件8件。

企业合规指引方面，上海市委网信办组织编写《上海属地网络平台履行未成年人网络保护义务的合规指引（试行版）》，将在哔哩哔哩、小红书、阅文集团、喜马拉雅、虎扑等属地重点平台试行。上海市委网信办引导平台发挥社会责任，指导属地小红书、得物、大众点评、七猫、2345、虎扑等20多家重点平台发布《未成年人网络保护社会责任报告》。（来源：网信上海）

2. 北京亦庄完成全市首个数据出境负面清单备案

9 月 11 日，拜耳医药保健有限公司通过中国（北京）自由贸易试验区高端产业片区亦庄组团负面清单备案审核，成为全市首家通过自贸试验区数据出境负面清单政策实现数据合规出境的企业。

《北京市数据跨境流动便利化服务管理若干措施》发布后，北京亦庄率先出台全市首个数据出境负面清单组团实施文件——《中国（北京）自由贸易试验区高端产业片区亦庄组团数据出境负面清单实施意见》，支持企业在自贸试验区适用负面清单开展数据出境，强化数据处理者作为申报主体承担数据出境主体责任，建立企业定期报备、抽检核查等监管闭环机制，逐步形成符合北京亦庄产业发展需求的“四个一批”成果，即一批数据出境负面清单、一套数据出境管理措施、一套数据出境服务体系、一批数据出境典型实践案例。（来源：网信北京）

3. 广州互联网法院发布一起涉数据跨境典型案例

9 月 2 日，广州互联网法院发布一起涉数据跨境典型案例“王某与某咨询公司、某国际酒店公司个人信息保护纠纷案”，涉及个人信息跨境处理行为的合法性审查。

本案中，王某通过某咨询公司运营的微信公众号预定境外酒店过程中，点击勾选了某国际酒店公司的《客户个人数据保护章程》，并提交了姓名、国籍、电话号码、电子邮箱地址、银行卡号等个人信息。事后，王某发现依据《客户个人数据保护章程》规定，其提交的个人信息将被传送共享至

全球多个地区和接收主体，认为两公司跨境处理中国公民个人信息行为违反相关规定，遂向广州互联网法院提起诉讼。

广州互联网法院认为，被告公司为消费者预定域外酒店服务收集案涉个人信息，此种情况下的个人信息出境，属于履行合同必需，不须单独同意。经审理查明，被告公司《客户个人数据保护章程》未依法正确履行告知义务，且被告公司基于商业营销目的还向位于美国和爱尔兰的第三方公司传输处理相关个人信息，超出履行合同必需，也未向王某充分告知并取得其单独同意，属于违法处理行为，侵害了王某的个人信息权益，应当承担民事侵权责任。（来源：广州互联网法院）

4. 上海市金山区人民法院审结一起离职员工利用其掌握的客户信息用于个人生意、侵害原单位商业秘密案

9月9日，上海市金山区人民法院审结一起离职员工利用其掌握的客户信息用于个人生意、侵害原单位商业秘密的案件。

原告力某公司授权达某公司使用其客户信息库，并委托达某公司推销其产品。被告李某系达某公司销售人员。同时，达某公司按照力某公司的要求与李某签订保密协议。双方约定，李某作为保密义务人，未经授权，不得擅自披露、使用商业秘密，服务关系结束后，应将与工作有关的技术资料、试验设备、试验材料、客户名单等交还公司，并要求李某对所获取的商业秘密严加保守，不得以任何理由或借口予以泄露。李某离职后，利用其在达某公司工作期间掌握的力某公司客户信息进行产品推销。后力某

公司接到客户举报，遂将李某诉至金山区人民法院，要求其立即停止侵害公司商业秘密的行为，并要求李某赔偿公司经济损失。

金山区人民法院经审理认为，企业的客户名册中包含众多客户名称、地址、联系方式以及交易记录等特殊信息，并不属于公开信息，并且能为企业带来竞争优势，具有商业价值，应认定为商业秘密。金山区人民法院判决李某立即停止侵害力某公司客户信息的商业秘密，并赔偿力某公司经济损失及维权合理费用。（来源：上海高院）

5. 北京互联网法院与北京市委网信办发布 10 起个人信息保护典型案例

9 月，北京互联网法院与北京市委网信办陆续发布 10 起个人信息保护典型案例，包括：

案例一“关联产品间共享用户数据应获有效同意”；

案例二“搜索引擎服务提供者处理公开个人信息‘通知删除’规则的适用”；

案例三“APP 登陆界面收集用户面像信息未设置拒绝选项侵害用户个人信息权益”；

案例四“个人信息处理者可以依据其信息存储形式和能力选择合理的信息提供方式”；

案例五“死者近亲属对死者个人信息权益的行使应符合合法、正当、必要原则”；

案例六“利用已公开个人信息有误导致受众混淆构成侵权”；

案例七“当事人在诉讼中提交已合法的收集个人信息作为证据属于履行法定义务的行为”；

案例八“信息处理者对其尽到告知同意义务负有相应的举证责任”；

案例九“个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务”；

案例十“未经授权对包含他人肖像的视频进行AI换脸处理，构成对他人个人信息权益的侵害”。（来源：北京互联网法院）

境外前沿观察：月度速览十则

导读：9 月，联合国通过《全球数字契约》，明确 5 项行动目标，将推进负责任、公平和可互操作的数据治理办法，加强人工智能国际治理，造福人类。欧盟委员会表示有超过 100 家公司成为欧盟《人工智能公约》的首批签约方，将在《人工智能法》生效之前开始应用其原则，包括排查人工智能系统，识别根据《人工智能法》可能被归类为高风险的人工智能系统等。美国一家人工智能医疗公司发生服务器配置错误，泄露 5.3TB 敏感心理健康记录，事件源于网络安全研究员发现一个未受密码保护且配置错误的服务器，其中包含来自该公司的机密记录。此外，澳大利亚信息专员办公室发布《2024 上半年数据泄露通报报告》，显示 2024 年上半年向监管机构通报的数据泄露数量处于三年半以来的最高水平。

供应链安全方面，美国商务部工业和安全局发布拟议规则通知，禁止销售或进口集成特定硬件和软件的互联汽车，或单独出售的组件，保障网联汽车供应链安全。美国、英国、澳大利亚成立供应链弹性合作小组，将开发一个专注于电信行业的预警试点，识别和监测电信行业供应链中断的潜在威胁。黎巴嫩连续两天发生大规模传呼机、对讲机等通信设备爆炸事件。安全分析师认为，以色列情报机构很可能是对供应链下手，“对生产过程进行渗透，在传呼机中加入炸药和远程引爆装置，且没有引起怀疑”。

巴西最高法院下令全面暂停社交网络 X 在该国的运营，原因是该平台未能遵守在巴西指定法定代表人的要求。因在内部系统中意外以明文格式

存储数亿用户密码违反 GDRP，社交媒体巨头 Meta 被爱尔兰数据保护委员会罚款 9100 万欧元。此外，美国联邦第三巡回上诉法院做出一项重大裁决，认为当通过其算法主动推荐内容时，平台不能再被视为中立的中介，应对其行为负责。这一裁决或对社交媒体平台运营模式产生深远影响。

关键词：全球数字契约、人工智能公约、供应链安全、数据泄露、传呼机爆炸事件、平台责任

1. 联合国通过《全球数字契约》，为首个全面的全球数字合作和人工智能治理框架

9 月 22 日，联合国通过《未来契约》及其附件《全球数字契约》和《子孙后代问题宣言》，旨在为和平与安全、数字合作等问题提供行动指南。

其中，《全球数字契约》为各国携手应对数字挑战、共同推动数字合作进程提供行动指南，承载着规划世界数字未来图景的重要使命。《契约》明确以下 5 项行动目标：（1）弥合数字鸿沟，加快在实现各项可持续发展目标方面取得进展；（2）为所有人扩大数字经济的包容性和惠益；（3）营造尊重、保护和促进人权的包容、开放、安全和可靠的数字空间；（4）推进负责任、公平和可互操作的数据治理办法；（5）加强人工智能国际治理，造福人类。此外，为实现上述目标，《契约》同时还提出具体承诺及行动计划。（来源：联合国）

2. 美国工业和安全局发布拟议规则通知，保护互联汽车供应链免受外国对手威胁

9 月 23 日，美国商务部工业和安全局（BIS）发布拟议规则通知《保障信息和通信技术及服务供应链：网联汽车》，禁止销售或进口集成了特定硬件和软件的互联汽车，或单独出售的组件，因为这些汽车或与对手国家有充分的联系。

拟议规则侧重于集成到车辆连接系统（VCS）中的硬件和软件以及集成到自动驾驶系统（ADS）中的软件。这些是关键系统，通过特定的硬件和软件，可以在互联汽车中实现外部连接和自动驾驶功能。对这些系统的恶意访问可能允许对手访问和收集美国最敏感的数据，并远程操纵美国道路上的汽车。拟议规则将适用于所有轮式公路车辆，例如汽车、卡车和公共汽车，但不包括未在公共道路上使用的车辆，例如农用车或采矿车辆。（来源：美国工业与安全局）

3. 美国－英国－澳大利亚成立供应链弹性合作小组，以应对供应链威胁

9 月 12 日，美国国土安全部、英国商业和贸易部以及澳大利亚工业、科学和资源部成立美国－英国－澳大利亚供应链弹性合作小组（SCRCG），以加强应对关键供应链面临威胁时的处理能力。该小组将开发一个专注于电信行业的预警试点，旨在识别和监测电信行业供应链中断的潜在威胁；还将加强全球对该行业脆弱性的理解，开发信息共享和共同应对供应链中断的沟通渠道。（来源：美国国土安全部）

4. 澳大利亚信息专员办公室发布《2024 上半年数据泄露通报报告》

9 月 16 日，澳大利亚信息专员办公室（OAIC）发布《2024 上半年数据泄露通报报告》，显示 2024 年上半年向监管机构通报的数据泄露数量处于三年半以来的最高水平。

报告显示，OAIC 在 2024 年 1 月至 6 月期间接到 527 起数据泄露报告。这是自 2020 年 7 月至 12 月以来最高的通知数量,比 2023 年下半年增加 9%。在此期间通报的 MediSecure 数据泄露事件影响大约 1290 万澳大利亚人，这是自数据泄露通报计划生效以来影响人数最多的事件。与之前的报告类似，恶意和刑事攻击是事件的主要来源（67%），其中 57%是网络安全事件。卫生部和澳大利亚政府是通报数据泄露事件最多的部门（分别占所有泄露事件的 19%和 12%）。（来源：澳大利亚信息专员办公室）

5. 百余家公司签署欧盟《人工智能公约》，推动值得信赖和安全的人工智能开发

9 月 25 日，欧盟委员会表示超过 100 家公司成为欧盟《人工智能公约》的首批签约方，这些签约公司主要是 IT、电信、医疗保健、银行、汽车和航空等不同行业的跨国公司和欧洲中小企业。该公约支持行业的自愿承诺，即在《人工智能法》生效之前开始应用其原则，并加强欧盟人工智能办公室与所有相关利益相关者（包括行业、民间社会和学术界）之间的互动。

《人工智能公约》包括三点核心内容：（1）人工智能治理战略。促进组织对人工智能的使用和治理，确保遵守《人工智能法》；（2）高风险人工智能系统映射。排查人工智能系统，识别根据《人工智能法》可能被归类为高风险的人工智能系统；（3）提高员工人工智能素养和意识，确保合乎道德和负责任的人工智能开发。

除了这些核心承诺外，超过一半的签署方还承诺开展其他行动，如确保人工监督、降低风险以及标记某些类型的人工智能生成内容。（来源：欧盟委员会）

6. 美国人工智能医疗公司服务器配置错误，泄露 5.3TB 心理健康记录

9 月 6 日消息，美国人工智能医疗公司 Confidant Health 近日发生服务器配置错误，泄露 5.3TB 敏感心理健康记录，其中包括个人信息、评估和医疗信息，将对患者构成严重隐私风险。

此次泄露事件源于 vpnMentor 的资深网络安全研究员发现一个未受密码保护且配置错误的服务器，其中包含来自该公司的机密记录。该公司已承认数据泄露并限制访问。目前尚不清楚数据库是由该公司直接管理还是由第三方管理。暴露的持续时间和对配置错误服务器的是否有潜在访问仍不可知。

Confidant Health 是一家位于德克萨斯州的人工智能公司，为康涅狄格州、佛罗里达州、新罕布什尔州、德克萨斯州和弗吉尼亚州的居民提供心理健康和成瘾治疗服务。（来源：安全内参）

7. 黎巴嫩传呼机发生大范围爆炸，涉及供应链预置攻击

9 月 17 日、18 日，黎巴嫩连续两天发生大规模传呼机、对讲机等通信设备爆炸事件，造成 37 人丧生，近 3000 人受伤。

据消息人士透露，真主党从一家名为金阿波罗的企业订购5000台传呼机，于今年早些时候交付。17日袭击只影响到那些处于开机状态并收到信息的传呼机。当天下午，这些传呼机收到一条看似来自真主党领导层的消息，响了几秒钟后爆炸。消息人士表示，以色列情报和特勤局（摩萨德）在这批传呼机的“生产层面”就实施改装，在里面植入能接收密码的炸药，用扫描仪或其他设备都“非常难以探测”。有军事和安全分析师认为，以色列情报机构很可能是对供应链下手，“对生产过程进行渗透，在传呼机中加入炸药和远程引爆装置，且没有引起怀疑”。金阿波罗公司18日称，这批传呼机并非该企业生产，而是授权一家名为BAC的企业贴牌生产，金阿波罗没有参与设计或生产，自身也是受害者。

黎巴嫩真主党武装人员近来较为普遍地使用传呼机，是为了避免以军追踪他们的位置。黎巴嫩公共卫生部17日发表声明，要求所有携带传呼机的民众立即将其扔掉。目前，黎巴嫩外交部将爆炸事件定性为“以色列网络攻击”，但没有公布更多细节。（来源：新华网、央广网、央视网）

8. 巴西全面禁止X，使用VPN绕过封锁将面临巨额罚款

9月2日消息，巴西最高法院近日下令全面暂停社交网络X在该国的运营，原因是该平台未能遵守在巴西指定法定代表人的要求。此禁令要求巴西国家电信局在24小时内执行，命令全国超过20000家宽带互联网提供商阻止对X的访问。X所有者埃隆·马斯克对该禁令表示强烈反对，称巴西正

在“关闭真相的主要来源”，但巴西总统反驳称，所有投资者都必须遵守巴西法律。

最初的命令包括要求苹果和谷歌实施技术障碍，防止 iOS 和 Android 用户通过 App 使用 X，并封锁 VPN，但这部分要求最终被撤销。但根据巴西法律，任何试图通过 VPN 绕过封锁的个人或公司将被处以每天 50000 雷亚尔（约 10000 美元）的罚款。（来源：securitylab）

9. 美国法院裁决，社交媒体平台或对算法推荐内容承担法律责任

9 月 2 日消息，美国联邦第三巡回上诉法院近期做出一项重大裁决，可能对社交媒体平台的运营模式产生深远影响。法院判定，社交媒体平台可能需要对其算法推荐的内容承担法律责任。这一裁决源于 10 岁女孩妮拉·安德森因参与 TikTok 上的“危险挑战”而不幸身亡，女孩的母亲起诉 TikTok，指控其算法在明知风险的情况下，仍向儿童推荐危险内容。

此前，这类索赔通常根据《通信规范法》第 230 条被驳回。然而，此次法院裁定认为，当通过其算法主动推荐内容时，平台不能再被视为中立的中介，应对其行为负责。该裁决被视为社交媒体行业的转折点，迫使平台修改其推荐算法并加强内容审核。此外，该判决援引美国最高法院近期在 Moody 诉 NetChoice 案中的裁决，指出包含编辑控制或内容审核元素的算法可以作为一种言论形式受到第一修正案保护。第三巡回法院使用这一逻辑来论证，如果平台算法被视为自己的言论，那么公司应对此负责。（来源：securitylab）

10. 因存储明文密码，Meta 被罚 1.01 亿美元

9 月 27 日消息，社交媒体巨头 Meta 因在内部系统中意外以明文格式存储数亿用户密码，违反欧盟《通用数据保护条例》，被爱尔兰数据保护委员会（DPC）罚款 9100 万欧元（约 1.01 亿美元）。

该问题最早于 2019 年由 Meta 自行发现，当时通知了受影响用户，并强调密码仅在公司内部暴露，没有证据表明密码被滥用。然而，DPC 经过五年调查后认定 Meta 多次违反《通用数据保护条例》，包括未及时通知当局泄漏情况及未实施足够的技术保护措施。DPC 指出，存储明文密码存在严重风险，可能导致用户社交媒体账户被滥用。（来源：The Record）

行业前沿观察一：中央网信办部署开展“清朗·整治违规开展互联网新闻信息服务”、“清朗·规范网络语言文字使用”行动；网信部门曝光涉未成年人乱象

导读：9月8日，2024年国家网络安全宣传周开幕式在广东省广州市举行，本届网安周在全国范围内以会议、论坛、竞赛、展览等多种形式展开，强调全民参与，着力创新成果展示，注重发挥粤港澳大湾区的区位优势，推动网络安全宣传辐射全国。

9月9日，2024年全国数字乡村建设工作现场推进会在四川省绵阳市召开，会议强调，数字乡村战略实施以来取得了积极成效，形成了一批典型经验做法，也面临不少困难和挑战。

9月10日，国家发展改革委办公厅等发布关于推动车网互动规模化应用试点工作的通知。其中提到，按照“创新引导、先行先试”的原则，全面推广新能源汽车有序充电，扩大双向充放电（V2G）项目规模，丰富车网互动应用场景，以城市为主体完善规模化、可持续的车网互动政策机制，以V2G项目为主体探索技术先进、模式清晰、可复制推广的商业模式，力争以市场化机制引导车网互动规模化发展。

关键词：网安周、信息化、数字乡村、网络安全、大湾区、新能源

1. 中央网信办部署开展“清朗·整治违规开展互联网新闻信息服务”专项行动

10 月 3 日从中央网信办获悉，为进一步规范互联网新闻信息服务活动，提升主流新闻舆论影响力，营造清朗网络空间，中央网信办近日印发通知，部署开展为期 3 个月的“清朗·整治违规开展互联网新闻信息服务”专项行动。

据悉，本次专项行动针对违法违规开展互联网新闻信息服务行为，集中整治五类突出问题。

一是编发虚假不实新闻信息，使用与新闻信息内容严重不符的夸张标题，或者恶意篡改、断章取义、拼凑剪辑、合成伪造新闻信息，误导社会公众。二是借舆论监督名义，通过采编、发布、转载、删除新闻信息，干预新闻信息呈现或搜索结果等手段，威胁、要挟他人提供财物、开展商业合作，谋取不正当利益。三是仿冒、假冒新闻网站、报刊社、广播电视机构、通讯社等新闻单位，或者擅自使用“新闻”“报道”等具有新闻属性的名称、标识开设网站平台、注册账号、发布信息。四是未经许可或超越许可范围开展互联网新闻信息采编发布服务、转载服务、传播平台服务。未取得互联网新闻信息采编发布服务资质，违规开展新闻采访、发布新闻信息。五是伪造、倒卖、出租、出借、转让互联网新闻信息服务许可资质。出售、出租或以其他形式 委托第三方主体运营互联网新闻信息服务频道等。通过不正当手段、虚假材料等取得互联网新闻信息服务许可。（来源：中国网信网）

2. “清朗·规范网络语言文字使用”专项行动开展

10 月 11 日从中央网信办获悉，为整治网上国家通用语言文字不规范使用乱象，塑造有利于未成年人健康成长的网络环境和育人生态，中央网信办、教育部近日印发通知，部署开展“清朗·规范网络语言文字使用”专项行动。

专项行动聚焦部分网站平台在热搜榜单、首页首屏、发现精选等重点环节呈现的语言文字不规范、不文明现象，重点整治歪曲音、形、义，编造网络黑话烂梗，滥用隐晦表达等突出问题。

专项行动要求，各地网信、教育部门要强化协同联动，形成依法管理和正面引导合力，坚持问题导向，聚焦群众反映集中的问题，聚焦未成年人等特殊群体权益保护，畅通举报渠道，集中清理不规范、不文明网络语言文字相关信息，严格落实整治任务。鼓励各地结合工作实际，加强语言文字相关法律法规科普宣传，倡导文明用语用字，营造全社会重视和参与的良好氛围。（来源：中国网信网）

3. 2024 年世界互联网大会乌镇峰会将全面聚焦人工智能

记者日前从世界互联网大会获悉，2024 年世界互联网大会乌镇峰会将全面聚焦人工智能，以“拥抱以人为本、智能向善的数字未来——携手构建网络空间命运共同体”为主题，围绕全球发展倡议、数字化绿色化协同转型发展、数字经济、人工智能技术创新与治理等议题举办 20 余场分论坛。

世界互联网大会秘书处负责人表示，2024年乌镇峰会将在往年特色基础上持续推陈出新，颁发“世界互联网大会杰出贡献奖”，成立世界互联网大会人工智能专业委员会，设立世界互联网大会智库合作计划，发起世界互联网大会数字研修院项目，举办全球互联网人才卓越计划研修班等。

2024年世界互联网大会乌镇峰会将于11月19日至22日在浙江乌镇举办。（来源：中国网信网）

4. 网信部门曝光“毒视频”“开盒挂人”等涉未成年人乱象

据“网信中国”微信公众号消息，7月中旬以来，网信部门深入开展“清朗·2024年暑期未成年人网络环境整治”专项行动，全面覆盖直播、短视频、社交、电商等重点环节，集中力量整治危害未成年人身心健康的突出问题。专项行动期间，累计清理拦截涉未成年人违法不良信息430万余条，处置账号13万余个，关闭下架网站平台2000余个，有力维护未成年人合法权益。现将部分典型案例通报如下：

从严处置各类危害未成年人身心健康的“毒视频”。专项行动以涉未成年人主题、未成年人出镜内容为重点，深入整治各类传播不良导向、诱导危险行为的直播和短视频内容。巡查发现，部分短视频将血腥暴力元素强加于经典动画，恶意发布“小马宝莉毁童年血腥版”、“发疯老奶奶偷袭佩奇”等内容。使用低俗粗俗语言篡改儿歌，传递不良价值观。摆拍未成年人吃橡皮泥、厕所抽烟、校园约架等剧情，将儿童包装成所谓“性感辣妹”进行无底线营销。一些直播间让未成年人暖场助力，采取现场打招

呼、视频连线、声音旁白等形式，诱导直接或变相出镜。网信部门指导重点平台完善涉未成年人内容审核标准，将管理要求以治理公告、站内信等形式触达网络主播，从严处置2.1万余个相关违规账号，关停直播3.2万余场。

集中整治针对未成年人的“开盒挂人”乱象。密切关注涉未成年人网暴风险，深入排查“校园墙”、“留言板”等环节“开盒挂人”问题。发现部分超话、贴吧等接受匿名投稿，发布针对未成年人的攻击谩骂言论，曝光未成年人姓名、学校、网络账号等隐私信息。有商家提供有偿代骂服务，部分用户传播“开盒挂人”短视频教程。一些用户组织恶意举报，通过批量举报的方式，实施侵扰、煽动对立。北京、河南、贵州等地网信部门深入核查问题线索，解散关闭1500余个提供挂人服务的话题、超话、贴吧，对存在突出问题的平台予以从重处罚，相关违法线索已转公安机关。

严厉打击隔空猥亵等网上恶性违法犯罪行为。专项行动期间发现，一些不法分子在短视频平台借“举牌”拍摄、贩卖淫秽色情制品；通过“一对一”私聊方式，假借“同龄人”身份与未成年人用户频繁互动，诱骗拍摄私密照片，实施隔空猥亵。天津、广东等地网信部门及时核查网民举报线索，督促平台加大评论区引流信息管理力度，链条式打击隔空猥亵、性引诱等问题，累计关闭相关违规群组1000余个，配合公安机关查办案件70余起。

深入整治网上涉未成年人违规售卖问题。上海、江苏、浙江等地网信部门督促属地电商平台，深入摸排打击售卖涉未成年人违规商品问题。部

分店铺提供动漫抱枕定制服务，在咨询环节发送色情图库链接。以售卖U盘、硬盘名义，变相传播封建迷信信息。教具类商品的评论环节存在谩骂信息，煽动亲子或师生对立。一些主播分享破解防沉迷系统方法，提供有偿“共号”服务，诱导未成年人沉迷网络。专项行动期间，重点网站平台累计下架相关违规商品4.2万余个，对1400余个店铺采取关闭、扣除违约金等处置措施。

排查下架一批涉未成年人违规应用。专项行动期间，应用商店落实上架审核、日常管理、应急处置等管理责任，对面向未成年人提供服务的应用程序强化内容和功能安全审核。

网信部门将持续深化专项行动治理成效，督促网站平台切实履行未成年人网络保护主体责任，对问题突出、整改不力的平台和账号，将依法从严采取处置处罚措施。同时，欢迎广大网民积极参与监督举报，共同为未成年人营造健康安全的网络环境。（来源：中国网信网）

行业前沿观察二：各地协会动态

导读：各地协会活动精彩纷呈，举行高级研修班、协办承办活动等。广东省网络空间安全协会在“国家网络安全宣传周”期间签约信创适配相关战略合作项目；北京网络空间安全协会在京举办“2024 网络与数据安全保障能力提升”高研班；陕西省信息网络安全协会成立陕西省网络安全等级保护定级评审专家团队；西藏自治区互联网协会党支部组织召开 2024 年第十次理论学习会；上海市信息安全行业协会协办 2024 年上海职工职业技能系列竞赛相关赛事；重庆信息安全产业技术创新联盟协办“数据赋能，智汇巴南”交流会；惠州市计算机信息网络安全协会成功承办网络安全攻防演练和网络安全培训活动等。

关键词：高研班、信创大赛、信创适配、数据安全、信息安全、网络安全

1. 广东省网络空间安全协会：“国家网络安全宣传周”期间签约信创适配相关战略合作项目

2024 年“国家网络安全宣传周”开幕式及多个重要活动在广东省广州市成功举行。期间，2024“国家网络安全宣传周”网络安全产品和服务供需洽谈会“信创适配测试认证”战略合作签约仪式在广州市南沙区国际金融论坛会议中心举行。

广东省网络空间安全协会副会长、华南信创适配测试认证中心副主任成珍苑，广东新兴国家网络安全和信息化发展研究院博士工作站办公室主任、华南信创适配测试认证中心副主任吴一丰，揭阳网络空间安全协会秘书长黄丽佳与 10 家从事信创服务的合作单位代表参加签约仪式。

据介绍，此次签约本着资源共享、优势互补、合作共赢的原则，达成在产品与技术交流、供需对接、人才培养、科研成果转化、信息共享、标准制定六方面的战略合作协议，为建立信息共享平台，推动信创适配、网络安全等相关技术创新和产业升级、培养行业优秀人才奠定坚实基础。（来源：广东省网络空间安全协会）

2. 北京网络空间安全协会： 在京举办“2024 网络与数据安全保障能力提升”高研班

为深入学习贯彻党的二十届三中全会精神，不断提升网络与数据安全专业技术人才自主创新能力，2024 年 9 月 23 日至 27 日由北京市人社局批

准并指导、北京网络空间安全协会主办、北京关键信息基础设施安全保护中心承办的北京市专业技术人才知识更新工程“2024 网络与数据安全保障能力提升”高级研修班在北京圆满举行。

本次高研班采取了线下线上学习相结合的形式，来自京津冀 127 名从事网络与数据安全领域相关工作、具有中高级职称的专业技术人员和高级管理人员报名，其中 76 名学员参加了在北京网络空间安全协会培训中心举行的线下研修课程。（来源：北京网络空间安全协会）

3. 陕西省信息网络安全协会：成立陕西省网络安全等级保护定级评审专家团队

为了进一步提高陕西省网络安全等级保护定级评审工作的规范性和科学性，根据《网络安全等级保护条例》中有关定级评审工作的要求，陕西省信息网络安全协会成立了陕西省网络安全等级保护定级评审专家团队，并已开展网络安全定级保护定级评审工作。

为了确保等保定级结果的合理性、准确性以及评审工作的严肃性、专业性和实效性，协会对专家团队进行了政策与规则培训与考核，以助力推进陕西省各领域信息化体系的安全保障能力。（来源：陕西省信息网络安全协会）

4. 西藏自治区互联网协会党支部组织召开2024年第十次理论学习会

近日，西藏自治区互联网协会党支部组织全体党员干部召开第十次政治理论学习会。党支部书记彭坤主持本次学习会。会上主要集中学习习近平总书记在党的二十届三中全会第二次全体会议上的重要讲话精神、习近平总书记在庆祝全国人民代表大会成立70周年大会上的重要讲话精神、习近平总书记在庆祝中国人民政治协商会议成立75周年大会上的重要讲话精神、《习近平著作选读》（第一卷）“建设网络良好生态，发挥网络引导舆论反映民意的作用”内容，以及自主学习《中国共产党党徽党旗条例》《西藏自治区网络信息安全管理条例》内容。

会议强调，全体党员干部要深入领会习近平总书记的重要讲话精神，将其内化于心、外化于行，不断提升自身的政治素养和业务能力；要以此次学习会为契机，将理论学习与实际工作紧密结合，做到学以致用、知行合一，进一步加强学习、提升能力、改进作风，助力西藏互联网行业高质量发展。（来源：西藏自治区互联网协会）

5. 上海市信息安全行业协会：协办2024年上海职工职业技能系列竞赛相关赛事

近日，由上海市总工会主办的“2024年上海职工职业技能系列竞赛--数字安全技能大赛暨第二届浦东新区数字安全风险智慧管控技能竞赛”闭

幕式暨颁奖典礼在上海市浦东软件园三林园成功举行。上海市信息安全行业协会是比赛协办方之一。

大赛吸引来自金融、卫生、通信、航空航天、港口物流、汽车制造等多个重点行业领域，共计123家相关企事业单位、542名选手报名技能竞赛赛道。经过层层选拔，80名选手获得由上海市信息安全行业协会颁发的《数字安全专业人员技术认证证书》，30位选手顺利入围决赛。而在今年特别增设的“数据安全优秀案例评选”赛道，共计36家企业参与，其中，7个创新、先进的产品和解决方案从中脱颖而出。同时，知识赛道以移动端在线进行知识学习、互动、竞答等方式，覆盖市民超过万人参与，有效提升了公众的数字安全防范意识。（来源：上海市信息安全行业协会）

6. 重庆信息安全产业技术创新联盟：协办“数据赋能，智汇巴南”交流会

近日，“数据赋能，智汇巴南”交流会在巴南软件园成功举办。此次交流会由重庆市巴南区经济和信息化委员会等3家单位共同主办，重庆信息安全产业技术创新联盟等5家单位协办，联盟秘书长马传龙受邀出席。现场30余家软信企业，线上近200人共同参与。

交流会上，行业大咖轮番上阵，从数据资产化路径、管理能力成熟度、数据合规挑战到数字安全重要性，多维度、深层次地剖析了数据要素的核心价值与应用前景。联盟理事单位重庆市软件评测中心有限公司副总经理

郑旭飞博士做了《数据管理能力成熟度评估-助力企业数字化转型》主题演讲。

联盟秘书长马传龙表示，随着数据管理能力成熟度评估模型的推广和应用，未来将有更多的企业受益于这一先进的管理理念，实现数字化转型的跨越式发展。（来源：重庆信息安全产业技术创新联盟）

7. 惠州市计算机信息网络安全协会：成功承办网络安全攻防演练和网络安全培训活动

日前，由惠州市计算机信息网络安全协会参与承办的2024年国家网络安全宣传周惠城区网络安全攻防演练和网络安全培训活动在惠州学院成功举行。

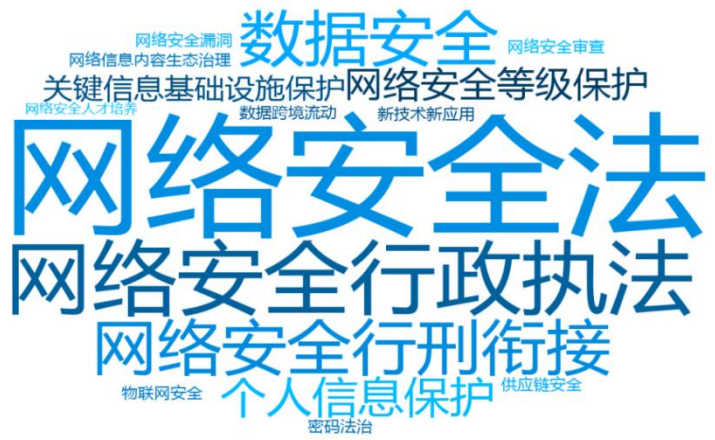
此次演练针对模拟场景以及对惠城区部分网站和信息系统进行实战攻击，目的是为了全方位检验惠城区关键信息基础设施的网络安全防御能力，发现深层次问题和隐患，以演促改、以演促管、以演促建，不断提升各部门各企业关键信息系统网络安全防护和应急处置能力。

此外，惠州学院计算机科学与工程学院和惠州市计算机信息网络安全协会深度融合，组织开展惠州市企业网络和数据安全大会等活动，积极组织学院学生参与全市网络安全攻防演练、专业网络检查工作支撑和网络安全宣传，参与“惠盾”、“粤盾”攻防演练并获得良好成绩。（来源：惠州市计算机信息网络安全协会）

公安部第三研究所网络安全法律研究中心

2016年2月，公安部第三研究所正式成立“网络安全法律研究中心”。 中心成立以来，聚焦前瞻性研究，切实践行理论研究与立法实践深度结合，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用发展及安全风险，并持续推动科研成果应用于网络安全相关立法活动，在国内网络安全法律方面的影响力逐步提升。同时投身警务实践活动和公安一线服务，为公安部门提供立法动态研判和决策研究支撑。

基础性	专业性	针对性



推动立法、服务实务、智库支撑

联系方式

电子邮箱：cslaw@gass.ac.cn　　咨询电话：王老师 18817309169

网络与数据安全法律合规咨询服务

提供《网络安全法》《数据安全法》《密码法》《个人信息保护法》及配套制度为核心的数据安全保护合规体系建设，包括但不限于帮助企业落实网络安全等级保护、关键信息基础设施安全保护、网络安全审查、数据出境安全风险评估、数据交易安全保障、安全事件应急处置等要求。
开展个人信息、重要数据、核心数据等数据安全合规自查、合规差距性分析，发现、识别、分析、研判、控制数据收集、存储、使用、加工、传输、提供、公开等全生命周期的法律风险，提供法律意见和整改建议。

数据安全合规体系构建

为企业提供网络安全漏洞发现与披露、漏洞扫描与渗透测试等安全测试、“白帽子”与众测等业务场景下的合规体系构建，帮助企业厘清行为边界，避免经营风险。

安全测试法律合规体系构建

开展情况调研，评估拟出境活动风险，发现安全风险并提供整改建议，根据客户整改落实情况，出具数据出境安全风险评估报告。

数据出境安全风险评估咨询服务

帮助企业构建事先防范网络安全、数据安全行政与刑事风险框架，指导企业如何正确配合监督检查、理解执法要求等。

网络安全、数据安全执法调查与刑事风险的防范与处置意见

针对《个人信息保护法》第五十五条规定的个人信息处理情形，帮助企业开展个人信息保护影响评估，履行个人信息保护义务。

个人信息保护影响评估/合规审计咨询服务

结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

网络安全、数据安全法律法规专业培训

数据出境安全风险评估咨询服务

近年来，我国在国家数据安全和个人信息保护的顶层设计布局下，加快数据出境相关立法，数据出境规则体系不断完善，数据出境安全评估成为数据出境的重要路径。2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》，落实《网络安全法》《数据安全法》《个人信息保护法》上位法要求，明确数据出境安全评估相关规定。在此形势下，企业普遍面临出境数据识别难、出境风险评估难、申报材料填报难等难题。为帮助企业解决以上难题，及时履行数据出境安全评估申报义务，公安部第三研究所网络安全法律研究中心特推出**数据出境安全风险评估咨询服务。**

数据出境活动

1 境内运营中收集和产生的数据传输、存储至境外

2 数据存储在境内，境外的机构、组织或者个人可以访问或者调用

数据出境安全风险评估咨询服务流程

01 情况调研 — 1 - 3 周

- 开展合规差距分析
- 识别安全风险并划定风险等级
- 针对安全风险提供整改建议

02 风险评估 — 3 - 5 周

03 指导落实整改 — 周期视情况而定

04 出具风险评估报告 — 1 - 2 周

- 结合客户落实整改情况，出具《数据出境风险评估报告》

合规咨询服务项目

中心已为互联网、银行、服装、签证、传统制造业等分属不同行业类别的企业提供APP合规咨询、个人信息保护（隐私政策）评估、个人信息保护合规整改、数据出境安全风险自评估等方面的合规咨询服务，合规咨询服务能力得到客户一致认可。

典型项目

- 某互联网公司APP合规咨询
- 某银行个人信息保护（隐私政策）评估
- 某跨国服装零售企业个人信息保护合规整改
- 某签证跨国集团数据出境安全风险评估咨询
- 某传统制造业跨国集团数据出境安全风险评估咨询

……