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）

2025年9月第9期（总第26期）

2025年9月15日

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：政策立法

导读：8 月，网络安全技术、公共数据开发利用、数据出境管理等方面是国家和地方政策立法重点关注内容，在配套规章、制度层面规定更加细致，并推动相关国家标准的制定。

一方面，《网络安全法》修正工作取得进展。继今年 3 月国家互联网信息办公室发布《中华人民共和国网络安全法（修正草案再次征求意见稿）》之后，8 月，十四届全国人大常委会第十七次会议审议了全国人大常委会委员长会议关于提请审议网络安全法修正草案的议案。

另一方面，网络安全和数据安全、个人信息保护国家标准制定工作持续推进。全国网安标委归口的《网络安全技术 公钥基础设施 证书管理协议》等 7 项网络安全国家标准获批发布。此外，全国网安标委发布《数据安全国家标准体系（2025 版）》（征求意见稿）《个人信息保护国家标准体系（2025 版）》（征求意见稿）。前者提出数据安全国家标准体系由基础共性、数据安全技术和产品、数据安全管理等组成；后者提出个人信息保护国家标准体系由基础共性、个人信息保护技术、个人信息保护管理与权益保障等组成。

地方层面，北京、山西、广西、安徽等省市主要围绕公共数据资源开发利用和数据出境管理两大主题推进政策立法。公共数据资源开发利用方面，《关于加快北京市公共数据资源开发利用的实施意见》《山西省公共数据资源授权运营管理办法（试行）》《黑龙江省公共数据资源登记实施

细则（试行）》以及安徽省《深化公共数据资源开发利用若干举措》分别发布。其中，北京明确将实行统一目录管理，动态更新数据的共享、开放属性；山西省级公共数据资源授权运营模式确立为“一级授权+二级分行业授权”模式；黑龙江要求直接持有或管理公共数据资源的党政机关和事业单位，应当对纳入授权运营范围的公共数据资源进行登记。数据出境管理方面，《中国（广西）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（江苏）自由贸易试验区数据出境负面清单管理办法（试行）》发布，且均附上相应的数据出境负面清单。

关键词：网络安全法修正；公共数据开发利用；数据出境负面清单

（一）国家层面动向

1. 网络安全法修正草案将首次提请审议

2025 年 8 月 26 日，十四届全国人大常委会第四十八次委员长会议在北京举行。委员长会议建议，十四届全国人大常委会第十七次会议审议全国人大常委会委员长会议关于提请审议网络安全法修正草案的议案。（来源：中国人大）

（二）部委层面动向

1. 全国网安标委发布 7 项网络安全国家标准

8 月 1 日，由全国网络安全标准化技术委员会归口的 7 项网络安全国家标准获批发布，分别是：《网络安全技术 公钥基础设施 证书管理协议》、《网络安全技术 公钥基础设施 PKI 组件最小互操作规范》、《网络安全技术 公钥基础设施 时间戳规范》、《网络安全技术 信息安全风险管理指导》、《网络安全技术 云计算服务安全能力评估方法》、《网络安全技术 网络安全运维实施指南》以及《网络安全技术 人工智能计算平台安全框架》。上述标准将于 2026 年 2 月 1 日起正式实施。（来源：全国网安标委）

2. 全国网安标委发布《数据安全国家标准体系（2025 版）》《个人信息保护国家标准体系（2025 版）》征求意见稿

8 月 15 日，全国网络安全标准化技术委员会秘书处发布《数据安全国家标准体系（2025 版）》（征求意见稿）、《个人信息保护国家标准体系（2025 版）》（征求意见稿）。

《数据安全国家标准体系（2025 版）》（征求意见稿）提出，数据安全国家标准体系由基础共性、数据安全技术和产品、数据安全管理、数据安全测评和认证、产品和服务数据安全、行业与应用数据安全六大类标准组成。

其中，基础共性标准作为数据安全标准体系的基础，用于明确数据安全的术语、数据分类分级保护等基础通用规则；数据安全技术和产品标准用于明确数据安全技术及产品的框架、规范和指南；数据安全管理标准用于明确数据处理活动安全、数据安全管理和安全运营的要求、方法和指南；数据安全测评和认证标准用于规范数据安全检测评估、监督检查、安全认证工作；产品和服务数据安全标准在基础共性、数据安全技术和产品、数据安全管理标准之上，聚焦特定系统平台和产品服务的数据安全风险，明确典型平台、系统、产品、服务的数据安全要求和指南；行业与应用数据安全标准位于数据安全国家标准体系最上层，是在其他数据安全标准的基础上，面向重点行业领域和新技术新应用开展数据安全标准研制。

《个人信息保护国家标准体系（2025 版）》（征求意见稿）提出，个人信息保护国家标准体系由基础共性、个人信息保护技术、个人信息保护

管理与权益保障、个人信息保护测评和认证、产品和服务个人信息保护、行业与应用个人信息保护六大类标准组成。

其中，基础共性标准作为个人信息保护标准体系的基础，为标准体系中其他部分提供支撑；个人信息保护技术标准用于明确个人信息保护技术的框架、规范和指南；个人信息保护管理与权益保障标准用于明确个人信息保护管理相关内容，给出个人信息主体权益保障的要求、方法和指南；个人信息保护测评和认证标准用于规范个人信息保护的检测评估、合规审计、安全认证等工作；产品和服务个人信息保护标准在基础共性、个人保护技术、个人信息保护管理与权益保障标准之上，用于明确移动应用、网络平台服务等典型产品和服务的个人信息保护要求和指南；行业与应用个人信息保护标准位于个人信息保护标准体系最上层，是在其他标准的基础上，面向重点行业领域和新兴技术应用开展个人信息保护标准研制。（来源：全国网安标委）

3. 全国数标委发布高质量数据集、全国一体化算力网等 4 个方向的 19 项技术文件

8 月 29 日，全国数据标准化技术委员会发布《关于发布高质量数据集、全国一体化算力网数据基础设施、可信数据空间等 4 个方向 19 项技术文件的通知》。

19 项技术文件中，高质量数据集 4 项、全国一体化算力网 9 项、数据基础设施 3 项、可信数据空间 3 项，具体包括《高质量数据集建设指南》、《高质量数据集格式要求》、《高质量数据集 分类指南》、《高质量数据

集质量评测规范》、《全国一体化算力网 算力并网技术要求》、《全国一体化算力网 算力算效衡量技术要求》、《全国一体化算力网 智算中心算力池化技术要求》、《全国一体化算力网 算力资源管理与调度技术要求》、《全国一体化算力网 算力多量纲计费技术要求》、《全国一体化算力网 算力运营服务与撮合交易技术要求》、《全国一体化算力网 算力监测接口要求》、《全国一体化算力网 算力中心能力评估要求》、《全国一体化算力网 安全保护要求》、《数据基础设施区域/行业功能节点技术要求》《数据基础设施接入管理》、《数据基础设施安全能力通用要求》、《可信数据空间 数字合约技术要求》、《可信数据空间使用控制技术要求》、《可信数据空间技术能力评价规范》。（来源：全国数标委）

（三）地方层面动向

1. 中共北京市委办公厅、北京市人民政府办公厅印发《关于加快北京市公共数据资源开发利用的实施意见》

5 月 6 日，中共北京市委办公厅、北京市人民政府办公厅印发《关于加快北京市公共数据资源开发利用的实施意见》，并于 8 月 12 日对外公布。《实施意见》围绕夯实公共数据资源开发利用基础、畅通公共数据资源开发利用渠道、释放数据要素市场创新活力等六个方面，提出二十条意见。

夯实公共数据资源开发利用基础方面，《实施意见》提出，完善公共数据目录。北京市实行统一目录管理，动态更新数据的共享、开放属性。北京市数据管理部门统筹指导各有关行业主管部门组织本行业公共机构全

量梳理公共数据目录，并由行业主管部门开展目录上链和数据汇聚。开展授权运营的授权主体指导运营机构建立公共数据授权运营产品和服务清单，纳入目录管理。各区（含北京经济技术开发区，下同）负责组织本区公共数据目录管理和数据汇聚，纳入全市目录体系调度。

畅通公共数据资源开发利用渠道方面，《实施意见》提出，有序推动公共数据开放。健全公共数据开放管理制度，在维护国家数据安全、保护个人信息和商业秘密的前提下，依法依规有序开放公共数据。鼓励公共机构开放高价值数据。发布年度公共数据开放计划，动态更新开放目录。优先在与民生紧密相关、社会需求迫切的行业和领域推动全量数据目录和样例数据开放。升级公共数据开放平台，探索以政企合作方式开展开放平台基础设施建设和运营，提升数据产品开发效率和价值转化能力。建立开放数据接诉即办机制，响应社会主体数据需求和应用反馈。各区负责组织本区公共数据开放，并在公共数据开放平台发布。

释放数据要素市场创新活力方面，《实施意见》提出，促进公共数据产品流通交易。充分发挥北京国际大数据交易所枢纽作用，建立与数据流通利用增值协作网络、公共数据专区的联动机制，优先推动金融、医疗健康、交通等领域数据价值高、社会需求大的公共数据产品场内交易，引领高价值、高频次数据流通交易。推进京津冀数据流通交易协同，助力全国一体化数据市场建设。（来源：北京市政务服务和数据管理局）

2. 山西省人民政府办公厅印发《山西省公共数据资源授权运营管理办法（试行）》

8 月 2 日，山西省人民政府办公厅印发《山西省公共数据资源授权运营管理办法（试行）》，自 2025 年 9 月 1 日起施行，有效期两年。《办法》共七章四十条，包括职责分工、授权机制、数据供给等内容。

授权机制方面，《办法》规定，省级公共数据资源授权运营模式为“一级授权+二级分行业授权”模式。“一级授权”是指省级数据管理部门将授权运营平台建设运维、数据资源对接及管理、数据初级加工等授权给某一符合遴选条件的法人组织；“分行业授权”是指省级数据管理部门按规范程序将公共数据按照行业领域分别授权给某一符合遴选条件的法人组织。省级数据管理部门组织开展一级运营主体遴选，并根据遴选结果进行一级授权，依托省公共数据资源授权运营协同机制组织开展分行业授权，定期将授权情况报告省人民政府。省级数据管理部门公开发布公共数据资源授权运营主体遴选通知，一级运营主体由省级数据管理部门以公开招标、邀请招标、谈判等公平竞争方式选定，二级运营主体由省级数据管理部门、行业主管部门以公开招标、邀请招标、谈判等公平竞争方式选定。

数据供给方面，《办法》提出，公共数据资源实行统一目录管理，省级数据管理部门负责组织编制公共数据分类分级指南等相关标准规范，建立公共数据资源目录管理和动态更新机制，建立全省公共数据资源授权运营目录，并向社会公开。各市、县（市、区）数据管理部门负责组织本级行业主管部门开展公共数据资源授权运营目录编制工作，并逐级报送汇总

至省级数据管理部门。各级行业主管部门根据公共数据资源授权运营有关要求，落实公共数据分类分级工作，编制、更新本部门公共数据资源授权运营目录，并报送汇总至本级数据管理部门。省政务信息管理部门负责编制全省政务数据资源目录，并定期向省级数据管理部门推送。（来源：山西省人民政府办公厅）

3. 广西壮族自治区商务厅等四部门印发《中国（广西）自由贸易试验区数据出境负面清单管理办法（试行）》及负面清单

8月4日，广西壮族自治区商务厅、中国（广西）自由贸易试验区工作办公室、广西壮族自治区互联网信息办公室、广西壮族自治区大数据发展局联合印发《中国（广西）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（广西）自由贸易试验区数据出境管理清单（负面清单）（2025版）》。《办法》共六章十八条，包括职责及分工、数据管理、负面清单制定及管理等内容。

《办法》提出，负面清单制定流程主要包括需求调研、重要数据识别、业务场景分析、论证与征求意见、履行审批报备流程。其中，需求调研阶段聚焦广西自贸试验区产业发展和数据处理者实际需求，遴选重点行业领域组织开展调研，从业务场景、类别、量级、字段等方面摸排掌握出境数据情况，作为负面清单制定依据。

《办法》规定，负面清单应至少包含以下两方面内容：（1）需要通过数据出境安全评估的数据清单，主要包括：关键信息基础设施运营者向境外提供个人信息或者重要数据；关键信息基础设施运营者以外的数据处理

者向境外提供重要数据，或者向境外提供达到负面清单要求申报数据出境安全评估的个人信息；（2）需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单，主要包括：关键信息基础设施运营者以外的数据处理者向境外提供达到负面清单要求订立个人信息出境标准合同或者通过个人信息保护认证的个人信息。（来源：中国（广西）自由贸易试验区工作办公室）

4. 中共安徽省委办公厅、安徽省人民政府办公厅印发《深化公共数据资源开发利用若干举措》

8 月 5 日，中共安徽省委办公厅、安徽省人民政府办公厅印发《深化公共数据资源开发利用若干举措》，围绕推动公共数据供给提质增效、规范公共数据资源授权运营等四方面，共提出十五项措施。

推动公共数据供给提质增效方面，《举措》提出加强公共数据高标准管理。制定安徽省公共数据资源登记实施细则，建设省公共数据资源登记平台，对纳入授权运营范围的公共数据资源实行登记管理。建立高效登记、质量核查、问题反馈、异议核实、处理跟踪、应用追溯的公共数据资源登记闭环管理体系。建设安徽省数据资源调度平台，推动包括公共数据资源在内的各类数据资源统一管理、需求统一受理、供需统一对接、资源统一发布、异议统一受理。

规范公共数据资源授权运营方面，《举措》提出打造统建共用的可信数据环境。完善省公共数据运营平台，打造安全可信数据环境，为各级公共数据资源授权运营提供一站式服务。指导监督运营机构履行数据安全主

体责任，采取必要安全措施，保护公共数据安全，通过安全合法合规方式开发数据产品和服务，实现“原始数据不出域、数据可用不可见”。探索公共数据产品和服务场内交易模式。

强化数据赋能场景创新方面，《举措》提出加快推进数据产业发展。完善省级数据企业和数据产业园区培育认定管理制度，推动数据企业申报、典型案例推荐、融资需求登记、上市后备资源管理，建设数据产业园区。在数字化转型、数据基础设施建设等领域，指导企业储备一批、申报一批、建设一批、投产一批高质量项目，培育一批具有全国竞争力、支柱型、特色型的数字产业集群。（来源：安徽省数据资源管理局）

5. 黑龙江省数据局印发《黑龙江省公共数据资源登记实施细则（试行）》

8 月 12 日，黑龙江省数据局印发《黑龙江省公共数据资源登记实施细则（试行）》，自印发之日起试行，有效期 2 年。《细则》共六章二十八条，包括登记要求、登记程序、登记类型等内容。

《细则》规定，直接持有或管理公共数据资源的党政机关和事业单位，应当对纳入授权运营范围的公共数据资源进行登记。鼓励对未纳入授权运营范围的公共数据资源进行登记。鼓励登记主体依托政务数据目录、公共数据开放目录开展登记。鼓励经授权开展运营活动的法人组织，对利用被授权的公共数据资源加工形成的数据产品和服务进行登记。鼓励供水、供气、供热、供电、公共交通等公用企业对直接持有或管理的公共数据资源及形成的产品和服务进行登记。

《细则》提出，公共数据资源登记活动按照申请、受理、形式审核、公示、赋码等程序开展；登记类型主要包括首次登记、变更登记、更正登记、注销登记。登记主体可以自行申请登记，也可以委托代理机构进行登记。涉及多个主体的，可共同提出登记申请或协商一致后由单独主体提出登记申请。

《细则》指出，公示期满无异议的，登记机构应当按照国家数据局制定的统一编码规范向登记主体发放带有登记结果查询码的登记确认单。登记确认单由国家数据管理部门统一监制，通过登记平台核发。任何单位和个人不得变造、伪造、出借或者出卖登记确认单，不得利用登记确认单获取不当得利。（来源：黑龙江省发改委）

6. 江苏省互联网信息办公室等部门印发《中国（江苏）自由贸易试验区数据出境负面清单管理办法（试行）》及负面清单

8 月 13 日，江苏省互联网信息办公室、江苏省商务厅、江苏省数据局印发《中国（江苏）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（江苏）自由贸易试验区数据出境管理清单（负面清单）（2025 版）》。

《办法》共七章二十五条，包括工作机制与职责、负面清单制定及管理、负面清单实施等内容。《办法》提出，负面清单制定工作流程按照需求调研、重要数据识别、业务场景分析、论证与征求意见、履行审批报备流程。其中，负面清单应至少包含两方面内容：一是需要通过数据出境安全评估的数据清单，二是需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单。

《办法》规定，数据处理者向境外提供数据属于已公布负面清单的行业领域，负面清单外的数据可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。未被省级管理部门、省级行业主管部门及有关职能部门、片区管委会告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。负面清单和操作指引未涉及行业领域的数据分类分级参考规则，按照有关规定和标准执行。（来源：江苏网信）

7. 中国（上海）自由贸易试验区临港新片区管理委员会等部门发布《中国（上海）自由贸易试验区临港新片区国际数据加工枢纽建设方案》

8 月 15 日，中国（上海）自由贸易试验区临港新片区管理委员会、上海市商务委员会、上海市数据局、上海市互联网信息办公室发布《中国（上海）自由贸易试验区临港新片区国际数据加工枢纽建设方案》，围绕深化国际数据规则对接与产业合作、健全国际数据加工枢纽创新管理体系、培育发展多元国际数据服务业态等五个方面，提出十五项措施。

深化国际数据规则对接与产业合作方面，《方案》提出，积极对标国际经贸规则与数据标准。加强与 DEPA、CPTPP 的规则对标和压力测试，开展个人信息保护、数据跨境流动、数字产品创新等规则对标试点工作。联动国内外数据治理相关专业咨询机构与认证机构，推动数据治理规则对接、能力互认。鼓励科研院所、企业积极参与数据领域、数据中心相关国

际标准制定，推动国内标准与国际标准对接，提高国际数据加工枢纽的国际认可度。

健全国际数据加工枢纽创新管理体系方面，《方案》提出，构建由政府引导，国内外专业机构、企业代表、行业专家共同参与的独立管理机构，探索透明化、轻量化、非接触式管理模式。搭建国际数据业务创新管理平台，建设国际数据加工枢纽安全威胁感知和监测预警基础设施，统筹网络与数据安全威胁信息的获取、分析、研判和预警工作。建立国际数据业务行业自律与自我管理机制，明确国际数据业务风险评估、沙盒试点等机制，指导企业安全、规范开展国际数据业务。

健全国际数据加工枢纽创新管理体系方面，《方案》提出，鼓励数据服务企业面向全球提供数据采集、数据存储、数据加工、数据标注、数据托管等国际数据服务。围绕人工智能数据标注、数字文化后期制作、跨境直播电商、大模型服务与应用、云协同设计、商业数据分析等领域，打造行业定制化数据加工方案与场景应用标杆。鼓励企业围绕制造、教育、医疗、文旅、城市治理等领域，创新利用海外数据和语料，面向国际市场提供多语言、多模态、多领域的垂域大模型、智能体应用和数字化整体解决方案及服务。（来源：上海自贸区临港新片区管委会）

境内前沿观察二：治理实践

导读：8 月，公安、网信、通信管理部门等机构持续发力，对网络安全、数据安全、个人信息安全等开展治理，助力提升网络安全防护能力，构建天朗气清的网络空间。

公安部公布涉灾情、险情等领域网络谣言 10 起典型案例。辽宁、山西网警相继公布“净网 2025”专项行动工作成效。辽宁省公安厅依法严打网络谣言、侵犯公民个人信息、网络赌博等突出网络违法犯罪情况，已侦破案件 613 起，抓获违法犯罪嫌疑人 1503 人，查扣涉案资金 1.2 亿元。山西公安网安部门开展“净网-2025”专项工作第一次集中收网行动，针对群众反映强烈的侵犯公民个人信息、黑客攻击破坏、网络谣言传播、网络黑灰产等突出网络违法犯罪类型，破获各类网络违法犯罪案件 50 余起，抓获违法犯罪嫌疑人近 100 名。

中央网信办、国家卫生健康委等四部门联合开展规范“自媒体”医疗科普行为的专项行动，要求从强化网络行为规范等八方面采取措施。北京市网信办相继启动“清朗京华•护航文旅”专项行动和发布暑期未成年人网络保护专项举报工作阶段性成果以及典型案例。

工信部以及上海、浙江等省市通信管理局发布侵害用户权益行为 APP（SDK）名单，并要求相关 APP（小程序）进行整改。

关键词：网络谣言；净网 2025；规范“自媒体”医疗科普行为；用户权益保护

（一）公安机关治理实践

1. 公安部公布涉灾情、险情等领域网络谣言 10 起典型案例

8 月 27 日，公安部公布涉灾情、险情等领域网络谣言 10 起典型案例。

案例一：陆某兴编造传播“四川泸定桥发生塌方”网络谣言案

近日，四川公安网安部门查明，陆某兴（男，55 岁）为吸粉引流、博取关注，通过“移花接木”的方式，拼凑合成地质灾害、塌方等视频，并在某短视频平台发布，谣称“泸定桥发生塌方”，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例二：田某平编造传播“河南夏邑发生洪涝自然灾害”网络谣言案

近日，河南公安网安部门查明，田某平（男，46 岁）为吸粉引流、博取关注，发布内容为“河南夏邑发生洪涝自然灾害”的虚假灾情信息，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例三：朱某龙编造传播“广西来宾市忻城县大塘镇六安村突发内涝，房屋被淹”网络谣言案

近日，广西公安网安部门查明，朱某龙（男，25 岁）为获得某平台创作者奖励，使用 AI 工具生成主题为“广西来宾村庄突发内涝，建筑半浸水中”的谣言信息，发布在某社交平台，并附有房子被淹的照片，误导大量网民关注和讨论，扰乱社会公共秩序。

案例四：王某编造传播“广西隆林洪灾山体滑坡目前 3 人死亡”网络谣言案

近日，广西公安网安部门查明，王某（男，52 岁）为博取流量、吸粉引流，在某短视频平台发布内容为“2025 年 7 月 1 日，广西隆林山体滑坡，给当地人民带来深重的灾难，目前 3 人死亡，1 人受伤”的谣言信息，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例五：宋某涛编造传播“温州平阳遭遇暴雨山洪袭击”灾情谣言案

近日，浙江公安网安部门查明，宋某涛（男，47 岁）为吸引眼球、博取关注，在某短视频平台发布内容为“7 月 27 日浙江温州平阳大暴雨引发山洪，地质灾害气象风险红色预警”的谣言信息，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例六：樊某旺编造传播“山东菏泽龙卷风致 5 人死亡，国道中断”网络谣言案

近日，山东公安网安部门查明，樊某旺（男，35 岁）为博取流量、吸粉引流，在多个短视频平台发布内容为“2025 年 7 月 8 日，牡丹区王浩屯镇出现龙卷风，多家企业和居民受到影响，240 国道的交通一度中断，另有官方消息，该灾难造成 5 人死亡，83 人受伤”的谣言信息，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例七：吴某妹编造传播“景德镇地震”网络谣言案

近日，江西公安网安部门查明，吴某妹（女，59 岁）在某短视频平台发布内容为“景德镇地震”的虚假灾情信息，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例八：沈某编造传播“浙江宁波一涵洞内车辆被淹，3 人死亡”网络谣言案

近日，浙江公安网安部门查明，沈某（女，23 岁）在某社交平台发布内容为“宁波台风，一涵洞内车辆被淹，有 3 人淹死”的谣言信息，误导大量网民关注和讨论，扰乱社会公共秩序。

案例九：朵某娟编造传播“兰州一化工仓库附近突发爆炸”网络谣言案

近日，甘肃公安网安部门查明，朵某娟（女，41 岁）为博取流量、吸粉引流，在某社交平台发布内容为“兰州市西固区一处化工仓库附近突发爆炸，已启动应急响应”的谣言信息，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

案例十：吉某编造传播“昌乐化工厂爆炸事故 7 死 4 伤”网络谣言案

近日，山东公安网安部门查明，吉某（男，34 岁）为博取流量、吸粉引流，利用 AI 工具捏造“昌乐化工厂爆炸 7 死 4 伤”谣言信息，并发布于某短视频平台，误导大量网民关注和讨论，引发当地居民恐慌，扰乱社会公共秩序。

以上人员均已被依法追究相应法律责任。（来源：公安部）

2. 辽宁网警公布“净网-2025”专项行动打击成效，查扣涉案资金 1.2 亿元

8 月 5 日，辽宁省公安厅召开新闻发布会，介绍今年以来全省公安机关开展“净网-2025”专项行动，依法严打网络谣言、侵犯公民个人信息、网络赌博等突出网络违法犯罪情况。截至目前，已侦破案件 613 起，抓获违法犯罪嫌疑人 1503 人，查扣涉案资金 1.2 亿元。

网络谣言、网络暴力、“网络水军”等违法犯罪严重影响社会安全稳定，公安机关坚持打治一体，同步进行网站平台综合治理与普法宣传教育。铁岭公安机关侦破一起网络谣言案件，网民衣某为博眼球制作虚假视频，将打架事件编造为“杀人案件”散播，现已被依法处以行政拘留。公安机关对侦破的网络暴力案件，关停违法违规账号4个，对侦破的网络谣言案件，通过政务新媒体等方式公开辟谣11次。

按照“打源头、摧平台、断链条”思路，全省公安机关建立群众举报、网络巡查、警企合作等多渠道线索收集机制，严厉打击侵犯公民个人信息和黑客犯罪。沈阳公安机关侦破汤某某等人利用公共场所计算机窃取平台账号信息，用于发布电诈、赌博引流视频的案件。大连公安机关侦破陈某等人非法改装机顶盒，盗看有线电视节目的案件，为相关企业挽回大量经济损失。

网络赌博、网络色情、网络黑灰产等违法犯罪严重败坏社会风气，侵害群众合法权益。全省公安机关深挖严打境外源头和境内黑灰产链条，今年以来已侦破系列相关案件。丹东公安机关侦破张某某等人充当赌博网站客服，诱导网民下载赌博软件，进行网络赌博的案件，捣毁犯罪窝点5个。鞍山公安机关侦破一起通过“发红包”换积分返利实施诈骗的黑灰产案件，打掉涉诈黑灰产团伙3个，破获全国各地电信诈骗关联案件115起。（来源：公安部网安局、辽宁省人民政府）

3. 山西网警开展“净网 2025”第一次集中收网，抓获犯罪嫌疑人近 100 名

8 月 23 日消息，为深入推进“净网-2025”专项工作，持续加大对网络违法犯罪的打击力度，在山西省公安厅网安总队的统一部署与精准指挥下，山西公安网安部门近日成功开展“净网-2025”专项工作第一次集中收网行动，有力筑牢网络安全防护屏障。

此次集中收网行动中，山西网安部门精准聚焦前期研判锁定的重点目标案件，针对群众反映强烈的侵犯公民个人信息、黑客攻击破坏、网络谣言传播、网络黑灰产等突出网络违法犯罪类型，集中优势警力展开攻坚。收网范围不仅覆盖本地重点区域，还延伸至外省涉案关联地区，通过跨区域警务协作机制，实现线索互通、行动联动，确保收网工作科学有序推进。

行动期间，全省网安民警挂图作战、昼夜攻坚，成功摧毁多个盘踞在网络空间的违法犯罪团伙。截至行动结束，共破获各类网络违法犯罪案件 50 余起，抓获违法犯罪嫌疑人近 100 名。（来源：公安部网安局）

4. 海南网警发布网络直播典型案例

8 月 11 日，海南网警发布一起网络直播典型案例。

海南公安网安部门近日在工作中发现，本地 5 名主播在某短视频平台以“PK”的形式进行低俗直播活动。为博取流量、诱导打赏，他们通过海南方言表达不良内容，涉及淫秽、低俗言语、性暗示、挑逗性言语等行为，严重扰乱社会公共秩序，造成极为恶劣的社会影响。

发现该违法行为后，属地公安机关联合属地网信部门依法对涉事主播陈某某、郑某某、莫某某、文某某、吴某某等人进行约谈，指出在其直播过程中存在的违法违规行为等问题，并责令低俗主播立即整改。同时，现场向他们普及互联网法律法规知识，要求严守法律红线、道德底线，传播正能量，切实履行社会责任。

经批评教育，5 名主播均深刻认识到低俗直播造成恶劣社会影响，承诺在今后直播的过程中将严格遵守法律法规，坚决杜绝低俗、庸俗、媚俗等不良内容的传播，主动传播积极健康的网络文化。目前，已依法对违法行为人陈某某、郑某某、莫某某、文某某、吴某某作出行政处罚。（来源：公安部网安局）

5. 江西吉安网警破获一起买卖账号案件，出售账号 4000 余个

8 月 18 日消息，江西吉安网安部门近日在工作中发现辖区有人涉嫌通过互联网从事违法犯罪活动。经过调查研判，民警很快锁定嫌疑人罗某身份。民警火速出击于当天晚上在罗某家中将其抓获，同时现场查获 10 余部作案手机及硬盘。

罗某对其违法事实供认不讳，并交代其在家上网时无意中看到高价收购社交账号的广告，在明知违法的情况下，罗某通过上网大批量购买虚拟手机号再注册某 APP 账号售卖非法获利。期间向不特定人员出售某 APP 账号高达 4000 余个，非法获利巨大。目前，公安机关依法对罗某作出没收违法所得、罚款并处行政拘留的处罚决定。（来源：公安部网安局）

6. 山东网警侦破一起因支付密码简单而被盗刷案，抓获犯罪嫌疑人 15 名

8 月 21 日消息，山东烟台公安网安部门近日破获一起因支付密码过于简单而导致支付账号被盗刷案件。

烟台公安网安部门连续接到多名群众报警称其网上支付平台账号被人盗刷近万元。经过分析研判，成功抓获以张某某、王某某等人为首的犯罪嫌疑人 15 名。经查，该犯罪团伙非法获取用户网上支付平台账号和个人身份信息，利用用户网上支付平台支付密码简单的漏洞，多次破解用户支付平台支付密码，盗刷账户内资金。目前，张某某、王某某等人已被依法采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办等部门开展规范“自媒体”医疗科普行为行动

7 月 28 日，中央网信办秘书局、国家卫生健康委办公厅、市场监管总局办公厅、国家中医药管理局综合司联合印发《关于规范“自媒体”医疗科普行为的通知》，规范“自媒体”医疗科普信息发布传播行为，提升“自媒体”规范开展医疗科普行为意识，支持专业医疗科普内容生产传播。

《通知》要求从分类核查认证账号资质、清晰展示账号资质信息、严格标注医疗科普信息来源、认真做好资质核验工作、严禁无资质账号生产发布专业医疗科普内容、强化网络行为规范、严禁违规变相发布广告、严处违法违规信息及账号八方面采取措施。其中，《通知》要求网站平台应

明确告知“自媒体”账号不得以介绍健康、养生知识等形式，变相发布医疗、药品、医疗器械、保健食品、特殊医学用途配方食品广告。介绍健康、养生知识的，不得在同一页面或者同时出现相关医疗、药品、医疗器械、保健食品、特殊医学用途配方食品的商品经营者或者服务提供者地址、联系方式、购物链接等内容。

此外，《通知》要求网站平台应坚决清理传授无底线蹭流量打造“网红医生”、借两性健康知识传播色情擦边内容、利用 AI 编造发布涉医领域同质化文案、编造健康故事售卖商品或药品、假冒医生身份开展科普、为售卖保健品鼓动拒绝就医等违法违规信息。对存在不按要求或虚假标注信息来源、无资质认证且持续生产发布专业医疗科普内容、违规发布广告、不遵守医疗科普行为规范等问题的账号，要依法依约采取取消互动功能、清理粉丝、取消营利权限、禁言、关闭等梯度措施。（来源：网信中国）

2. 国家网信办发布互联网新闻信息服务“持证亮牌”工作成果

8 月 1 日，国家网信办发布互联网新闻信息服务“持证亮牌”工作成果。2025 年以来，国家网信办部署指导地方网信办提升审批质效，督促腾讯、抖音、快手、微博等 15 家获批提供互联网新闻信息传播平台服务资质的网站平台优化完善系统功能，加强服务资质核验，对获批提供互联网新闻信息服务的公众账号统一增加红“V”标识，基本实现图文、音频、直播、短视频等内容场景全覆盖。

截至2025年7月25日，共有13516个公众账号加注红“V”标识并明示服务主体名称、许可证编号和服务类别，4401家网站、平台等服务形式明示许可信息。（来源：网信中国）

3. 北京市网信办启动“清朗京华•护航文旅”专项行动，重点整治六类文旅领域网络乱象

8月1日，北京市网信办宣布会同北京市文旅局联合开展为期1个月的“清朗京华•护航文旅”专项行动。专项行动聚焦在线旅游、短视频直播、网络社交等重点网站平台，集中整治涉京旅游虚假宣传、宣推京内野景点、“黄牛”倒票营销、发布软文或虚构人设进行线下引流、冒充正规旅行社违规揽客、恶意拼接炒作误导消费者等六类突出问题，切实为广大游客营造安全、舒心的旅游环境。（来源：网信北京）

4. 北京市网信办发布暑期未成年人网络保护专项举报工作阶段性成果以及典型案例

8月6日，北京市网信办发布“互联护苗2025”暑期未成年人网络保护举报专项工作成果。截至公告，北京市网信办指导属地各平台清理涉未成年人违法和不良信息36万余件，依法依规处置违法违规账号3700余个。

典型案例一：依法查处侵犯未成年人名誉权类信息和账号。账号“二手***”等将未成年人苏**照片及姓名擅自剪辑视频发布，恶意曲解未成年人视频动作意思，并加以夸张说明后传播，引发恶意言语攻击该未成年人言论，对未成年人造成心理伤害。接到举报后，已对该视频内容以及同质

的250余条视频内容作删除处理，对账号作出相应处置。账号“脸有***”“何**”发布某未成年人视频图片，对该未成年人进行侮辱贬损，涉及侵犯未成年人权益。接到举报后，已删除侵权视频，涉及的账号已被封禁或禁言处置。

典型案例二：依法查处涉未成年人不良交友类群组和账号。社交类APP“火*”中的群组版块，有用户以未成年人恋爱为名，建立名为“16-22处对象暧昧 唱歌”“交友，处cp的来，限14至17岁”“处大象 cpdd（14-18）”等交友群组，吸引未成年人聚集。接到举报后，已对上述群组以及据此倒查出的50余个含有未成年人恋爱交友等关键词的群组作解散处置，对创建相关群组的违规用户19335、19299等账号封禁处置。

典型案例三：依法查处虚构剧情恶意摆拍类账号。账号“加油**”、“于**”发布未成年人演绎偷拍“家长穿低胸露脐装遭受陌生人性侵”和“顶撞反抗家长教育”等不良导向内容。接到举报后，对账号予以禁言90日、暂停粉丝数增长90日、暂停营利权限180日、清除因违规行为增加的粉丝量等处罚，对上述账号所属MCN机构“古麦**”限制MCN账号管理功能30日处置。账号“农村***”发布未成年人整蛊视频，利用未成年人生吞虫子、蜗牛、野草等内容博取眼球，严重危害未成年人身心健康。接到举报后，清理删除相关视频501条，对账号作出禁言30天处置。（来源：网信北京）

5. 河北省网信办发布“清朗·燕赵净网”网络生态治理成果

8 月 13 日，河北省网信办发布 2025 年 7 月份“清朗·燕赵净网”网络生态治理专项行动成果。专项行动集中整治人民群众反映强烈的网络生态突出问题，全省网信系统查处违法违规网站 161 家；查处违规互联网用户账号 33 个；处置违法和不良信息 29235 条，其中网络谣言类 552 条，赌博诈骗类 269 条，涉未成年人类 96 条，色情低俗庸俗类 184 条，“自媒体”乱象类 129 条，破坏营商网络环境类 22 条，假冒侵权类 47 条，黑公关、网络水军类 3229 条，生成合成类 17 条，其他违法和不良信息 24690 条。（来源：网信河北）

6. 河北省网信办发布第一期网络执法典型案例

8 月 13 日，河北省网信办发布第一期网络执法典型案例。

案例一：低俗直播破坏网络生态案

2025 年 5 月，主播刘某、徐某等人在直播过程中进行“皮带抽打”“别针穿唇”等表演；2025 年 7 月，主播文某、郑某在直播 PK 过程中，制造性暗示、性挑逗氛围，诱导低俗互动。上述主播为吸引关注、赚取流量，直播过程中互相挑衅、拉踩引战、刻意营造冲突对抗，刺激打赏，传播血腥、残忍致人身心不适和“泛黄”“软色情”易使人产生性联想的低俗庸俗内容，破坏网络生态，严重违背社会公序良俗。属地网信部门依法对上述主播进行约谈，明确指出其违法违规行为，阐明相关法律规定及后果，使其深刻认识到自己的错误行为。公安机关依据《治安管理处罚法》，依法对上述主播的违法违规行为作出相应的行政处罚。

案例二：杨某、李某编造发布网络谣言案

2025 年 4 月，杨某在抖音上内容为某老年公寓着火的视频下，发表评论称死了 50 多人；2025 年 6 月，李某在抖音上发布视频称某地因下暴雨冲走两个人。经核查，上述评论、视频内容均为谣言信息。杨某、李某为博取关注、吸引流量，在未经核实的情况下，公然编造虚假信息，通过账号在商业平台散布传播，引发大量网民围观，导致局部社会恐慌情绪蔓延，严重扰乱正常社会秩序，影响极其恶劣。属地网信部门依据《网络安全法》《网络信息内容生态治理规定》等法律法规，依法约谈杨某、李某，明确指出其违法违规行为的性质及危害，责令其删除相关违法违规信息，消除不良影响。公安机关依据《治安管理处罚法》，对二人扰乱公共秩序的违法行为，分别给予罚款、拘留的行政处罚。（来源：网信河北）

（三）通信管理部门治理实践

1. 工信部以及上海、浙江等省市通信管理局发布侵害用户权益行为 APP（SDK）名单

（1）工业和信息化部信息通信管理局

8 月 4 日，工业和信息化部信息通信管理局发布 2025 年第 4 批（总第 49 批）侵害用户权益行为的 APP（SDK）名单。工业和信息化部近日组织第三方检测机构进行抽查，共发现 23 款 APP 及 SDK 存在侵害用户权益行为。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工业和信息化部将依法依规组织开展相关处置工作。

（2）上海通信管理局

8 月 5 日，上海市通信管理局发布 2025 年第 6 批侵害用户权益行为的 APP 名单。上海通信管理局近日组织第三方检测机构对上海市 APP（SDK）进行抽查，共发现 145 款 APP（SDK）存在侵害用户权益行为。上述 APP（SDK）应对存在的问题立即整改，并对该 APP（SDK）个人信息和用户权益保护工作开展全面自评估，自通报之日起 30 日内将整改报告和自评估报告书面报告上海通信管理局。对未能在限期内完成整改并提交报告的，上海通信管理局将依法依规予以处理。

（3）安徽通信管理局

8 月 5 日，安徽省通信管理局发布通报，指出 2025 年第 5 批次整改不到位的 APP 中，尚有 5 款（载拉货、来爱宇宙、炫之坞、加密图库、装修设计户型）逾期未完成整改。安徽省通信管理局组织对上述 APP 进行下架，相关应用商店应立即对名单中的应用软件进行下架处理。（来源：工业和信息化部、上海通信圈、安徽省通信管理局）

2. 浙江省通信管理局举办“之江铸网-2025”网络安全攻防演练

8 月 7 日消息，浙江省通信管理局近日联合浙江省经信厅共同举办“之江铸网-2025”浙江省公共互联网、工业互联网和车联网网络安全攻防演练。本次演练在巩固传统领域防御能力的基础上，深化“公共互联网、工业互联网和车联网平台安全”赛道，增设“智能网联汽车实车攻防”和“大语言模型安全靶场”赛道。同时，演练聚焦人工智能浪潮下的新型风险，打造专业化“大语言模型安全靶场”，以文本对话大模型为基础，构建关键

词过滤、诱导式防御、多轮检测三阶动态防御靶标模型，通过越狱攻击、提示词攻击等方式突破模型防线、诱导模型输出违规内容“夺旗”得分。（来源：浙江省通信管理局）

3. 甘肃省通信管理局组织开展2025年全省信息通信业网络数据安全应急演练

8月12日，甘肃省通信管理局组织开展2025年全省信息通信业网络数据安全应急演练。本次演练由甘肃电信承办，4家基础电信企业共同参与，主要聚焦公共互联网网络数据安全领域突出风险，针对勒索病毒、钓鱼邮件、敏感信息泄露、数据误操作擦除等典型场景，采用模拟实战的方式开展全流程闭环演练。（来源：甘肃省通信管理局）

（四）其他部门治理实践

1. 军地职能部门发布涉军自媒体账号违法违规典型案例

8月14日，军地职能部门发布一批涉军自媒体账号违法违规典型案例。

案例一：冒充官方账号。网络账号“南部卫士”、“联参智库服务”、“联勤保障”等与军队单位开办的网络账号雷同，以高仿账号冒充官方账号，发布内容多为涉军信息，蹭炒军事热点吸粉牟利。

案例二：编撰军事谣言。网络账号“乖乖兔军情”利用AI编造“中国四大镇魂武器”等谣言信息，误导认知。网络账号“军事课代表”发布所

谓“解析装备细节”、“分析战术战法”、“解读军事行动”等内容，部分文章需付费购买浏览，借军事话题违规牟利。

案例三：歪曲解读军史。网络账号“红小岩的自留地”、“红小岩谈古论今”、“红小岩的后花园”等，称抗美援朝志愿军飞行员、空军一级战斗英雄张积慧“战绩有水分”，质疑污蔑英烈功绩，借党史军史严肃话题引流牟利。

案例四：抹黑军队形象。网络账号“军创怡姐”、“苏州怡姐”利用所谓“答疑视频”，发布“在XX地服役有什么危害”等误导性内容，抹黑军队形象。

案例五：消费拥军情怀。网络账号“秦淮河畔”自称退役军人，长期发布身穿各式军服或军服仿制品的短视频，为个人账号违规引流。

案例六：暴露部队营区。网络账号“杨阳阳”自称90后留守军嫂，发布多篇“部队家属院”短视频，内容含各类训练设备，并标注定位，暴露军队敏感信息。（来源：网信中国）

境内观察三：人工智能安全专题

导读：8 月，人工智能政策立法主要关注人工智能赋能产业发展、人工智能科技伦理和数据知识产权登记等方面。

国务院印发《国务院关于深入实施“人工智能+”行动的意见》，围绕加快实施重点行动、强化基础支撑能力两方面提出多项意见，包括“人工智能+”科学技术、“人工智能+”产业发展、提升模型基础能力、强化政策法规保障等。

工信部会同中央网信办、国家发展改革委、科技部等联合发布《人工智能科技伦理管理服务办法（试行）（公开征求意见稿）》，细化落实《关于加强科技伦理治理的意见》《科技伦理审查办法（试行）》等要求。

上海市人民政府办公厅印发《上海市具身智能产业发展实施方案》，围绕模型创新驱动、打造公共平台、应用示范标杆等五方面提出多条措施。浙江省知识产权局发布《浙江省人工智能领域数据知识产权登记申请指引（2025 版）》（征求意见稿），明确产权登记对象和可以申请登记人工智能领域数据知识产权的数据处理者。

关键词：人工智能+；科技伦理；具身智能；数据知识产权

1. 国务院印发《国务院关于深入实施“人工智能+”行动的意见》

8 月 26 日，国务院印发《国务院关于深入实施“人工智能+”行动的意见》，要求加快实施六大类十四小类重点行动和强化八项基础支撑能力。

六大类重点行动分别是“人工智能+”科学技术、“人工智能+”产业发展、“人工智能+”消费提质、“人工智能+”民生福祉、“人工智能+”治理能力、“人工智能+”全球合作。其中，“人工智能+”治理能力方面，《意见》提出，推动构建面向自然人、数字人、智能机器人等多元一体的公共安全治理体系，加强人工智能在安全生产监管、防灾减灾救灾、公共安全预警、社会治安管理等方面的应用，提升监测预警、监管执法、指挥决策、现场救援、社会动员等工作水平，增强应用人工智能维护和塑造国家安全的能力。加快推动人工智能赋能网络空间治理，强化信息精准识别、态势主动研判、风险实时处置等能力。

强化八项基础支撑能力包括提升模型基础能力、加强数据供给创新、强化智能算力统筹、优化应用发展环境、促进开源生态繁荣、加强人才队伍建设、强化政策法规保障、提升安全能力水平。其中，强化政策法规保障方面，《意见》提出，完善人工智能法律法规、伦理准则等，推进人工智能健康发展相关立法工作。优化人工智能相关安全评估和备案管理制度。提升安全能力水平方面，《意见》提出，推动模型算法、数据资源、基础设施、应用系统等安全能力建设，防范模型的黑箱、幻觉、算法歧视等带来的风险，加强前瞻评估和监测处置，推动人工智能应用合规、透明、可信赖。建立健全人工智能技术监测、风险预警、应急响应体系，强化政府

引导、行业自律，坚持包容审慎、分类分级，加快形成动态敏捷、多元协同的人工智能治理格局。（来源：国务院）

2. 工信部等部门发布《人工智能科技伦理管理服务办法（试行）（公开征求意见稿）》

8 月 22 日，工业和信息化部会同中央网信办、国家发展改革委、科技部等部门发布《人工智能科技伦理管理服务办法（试行）（公开征求意见稿）》。公开征求意见稿共六章三十七条，包括人工智能科技伦理支持与促进、实施主体、工作程序等内容，是《关于加强科技伦理治理的意见》《科技伦理审查办法（试行）》等在人工智能领域的细化和落实。

公开征求意见稿规定，从事人工智能科技活动的高等学校、科研机构、医疗卫生机构、企业等是本单位人工智能科技伦理管理服务的责任主体。有条件的单位应设立人工智能科技伦理委员会，应配备必要的工作人员、办公场所和经费等条件，采取有效措施保障委员会独立开展工作。鼓励有资质的相关单位开展人工智能科技伦理管理体系相关认证。

公开征求意见稿指出，地方、相关主管部门可结合实际情况依托相关单位建立专业性人工智能科技伦理服务中心，接受其他单位委托，提供人工智能科技活动伦理审查、培训、咨询等服务。服务中心应建立规范的管理制度和程序，配备具有人工智能科技伦理服务能力的专职人员，接受地方或相关主管部门监督。

公开征求意见稿提出，科技部负责统筹指导全国科技伦理监管工作，工业和信息化部会同有关部门负责人工智能科技伦理治理工作，加强应急

伦理工作的协调指导。各部门依照职责权限负责本行业本系统人工智能科技伦理的管理服务工作，各地方依照职责权限负责本地区人工智能科技伦理的管理服务工作。（来源：工业和信息化部）

3. 上海市人民政府办公厅印发《上海市具身智能产业发展实施方案》

7 月 28 日，上海市人民政府办公厅印发《上海市具身智能产业发展实施方案》，围绕模型创新驱动、打造公共平台、应用示范标杆等五方面，提出二十四条措施。

模型创新驱动方面，《方案》提出支持企业、高校和科研院所联合研发多模态数据融合处理技术，打造自主操作系统。与机器人制造商、科研机构合作，推动具身智能操作系统在工业制造、物流配送、商业服务等领域试点应用，推动版本迭代优化，逐步构建成熟、可靠、广泛应用的具身智能操作系统生态。

打造公共平台方面，《方案》提出创新语料采集方式、场景、任务和动作技能，建设数字孪生实训场，实现“仿真训练—真实验证—迭代学习”的数字孪生实训闭环，赋能具身智能大模型实训。

群链协同发展方面，《方案》提出支持以公版机为代表的终端研发，推动量产进程；鼓励开发操作型、智慧型具身智能终端产品，打造“热销单品”，推荐纳入上海市创新产品推荐目录。分阶段培育具身智能产业化能力，推动从成熟应用场景到试点应用场景的大规模商业化应用。（来源：上海市政府办公厅）

4. 上海市三部门联合印发《上海市加快推动“AI+制造”发展的实施方案》

8 月 11 日，上海市经济和信息化委员会、上海市发展和改革委员会、上海市国有资产监督管理委员会印发《上海市加快推动“AI+制造”发展的实施方案》，围绕攻关基础和前沿技术、建设关键要素平台、推动重点行业应用等六方面，提出二十四项措施。

建设关键要素平台方面，《方案》提出打造工业语料公共服务平台。推动语料企业、制造企业、服务商等联合打造工业语料公共服务平台，建设船舶、航空、汽车、能源、钢铁等行业高质量多模态语料库，形成工业战略语料库以及模型微调数据、强推理数据、评测语料、实体知识图谱、稀缺场景语料等工业专业语料资源。探索嵌入式积分等多元利益分享和激励机制，促进语料高效汇聚与共享流通。推动链主企业基于行业上下游需求，打造工业数据空间，实现同行业语料汇聚和跨行业语料共享。引导中小企业提升数据治理能力，建立内部知识库，应用知识图谱、检索增强生成（RAG）等技术，在场景端快速应用模型。

积极营造发展生态方面，《方案》提出完善标准和安全体系。围绕语料、模型、平台、智能体、产品、应用等环节，增加基础共性、关键技术等标准供给，完善安全治理规范。加强工业数据语料安全、模型算法安全、系统安全、应用安全等，打造安全可信基座。依托第三方机构为模型、智能体和具身智能等提供测试验证服务。构建全面的智能化评测框架和指标

体系，科学评价企业智能化水平。建立健全知识产权保护机制，为工业智能创新应用提供制度保障。（来源：上海市经济和信息化委员会）

5. 河南省人民政府印发《河南省支持人工智能产业生态发展若干政策措施》

8 月 4 日，河南省人民政府印发《河南省支持人工智能产业生态发展若干政策措施》，提出包括加强模型研发应用、强化算力供给服务、促进数据开发利用等十项措施。

强化算力供给服务方面，《措施》提出，建立以算力券为核心的算力平台运营结算分担机制，每年发放总规模不超过 5000 万元的算力券。对使用超算中心、算力规模 100PFLOPS（每秒浮点运算次数）以上人工智能计算中心、1000 个标准机架以上数据中心算力资源的企业、科研机构、高校等，按照算力资源使用费的 20%予以奖励，每个使用单位每年可享受不超过 100 万元算力券奖励，所需资金由省、市级财政按照 1∶1 比例共同分担。

促进数据开发利用方面，《措施》提出，围绕工业、农业、文化和旅游、交通运输、医疗等重点行业，支持人工智能语料库建设，加快汇聚行业通用知识语料和特定语料资源，推动形成开放式语料合作生态，每年对用于大模型开发、训练和微调的高质量语料库每个给予最高 100 万元补助。（来源：河南省人民政府）

6. 浙江省知识产权局发布《浙江省人工智能领域数据知识产权登记申请指引（2025 版）》（征求意见稿）

8 月 19 日，浙江省知识产权局发布《浙江省人工智能领域数据知识产权登记申请指引（2025 版）》（征求意见稿）。

征求意见稿指出，人工智能领域数据知识产权登记对象包括：（1）基于人工智能大模型，通过预训练等方式形成适配专项能力或特定任务解决能力要求，所形成的算法、参数、模型等数据处理规则和数据集合；（2）基于人工智能相关技术，通过智能体、脑机接口、具身智能、生物启发等应用创新技术，所形成的算法、参数、模型等数据处理规则和数据集合。

征求意见稿指出，申请登记人工智能领域数据知识产权的数据处理者包括但不限于：原始数据采集方、加工处理方，以及在数据处理全流程中投入实质性技术资源或智力劳动的模型开发者、服务提供者等。（来源：浙江省市场监督管理局）

7. 国内多数 AI 模型训练使用的中文数据占比已超 60%

8 月 14 日，国务院新闻办公室举行新闻发布会介绍“十四五”时期数字中国建设发展成就。新闻发布会期间，国家发展改革委党组成员、国家数据局局长刘烈宏介绍，在人工智能时代，Token 作为处理文本的最小数据单元，如同互联网时代的“流量”。2024 年初，中国日均 Token 的消耗量为 1 千亿，截至今年 6 月底，日均 Token 消耗量已经突破 30 万亿，1 年半时间增长了 300 多倍，反映中国人工智能应用规模的快速增长。

刘烈宏表示，中文数据在国内大模型的训练性能提升方面发挥着重要作用。国内多数模型训练使用的中文数据占比已经超过了60%，有的模型已达到80%。中文高质量数据的开发和供给能力持续增强，推动中国人工智能模型性能的快速提升。（来源：国家数据局）

境外前沿观察：月度速览十则

导读：8 月，境外国家和地区持续推动网络安全领域政策法律，重点关注人工智能、数据安全、网络安全等方面。

人工智能方面，欧盟委员会发布关于《通用人工智能实践守则》的评估意见。评估针对守则是否覆盖《人工智能法》相关要求和守则在制定过程中是否兼顾相关利益方需求等。亚太经合组织数字和人工智能部长会议召开，并就人工智能发展发布联合声明。联合国批准成立首个人工智能治理小组并决定建立全球人工智能治理对话机制等。美国联邦贸易委员会正式批准针对 Workado 的禁令，要求该公司在缺乏充分可靠证据支持的情况下，不得继续宣称其人工智能内容检测产品具有所声称的准确性或有效性。

数据安全方面，英国《数据（使用与访问）法》首批条款届期生效。该批条款的实施重点在于开放客户数据与商业数据的使用，推动市场竞争和数字经济发展。法国第三大移动通信运营商 Bouygues Telecom 遭遇严重网络攻击，导致 640 万名客户的个人信息及银行账户数据被非法访问。

网络安全方面，巴西总统签署制定《国家网络安全战略》行政令，旨在加强巴西的网络安全成熟度和治理水平。加拿大下议院及国家网络安全机构正调查一起重大数据泄露事件。据内部邮件披露，一名身份不明的“威胁行为者”利用微软系统最新漏洞，非法访问用于管理计算机和移动设备的数据库，导致政府雇员私人信息外泄。

关键词：人工智能；数据安全；网络安全

1. 欧盟委员会发布关于《通用人工智能实践守则》评估的意见

8 月 1 日，欧盟委员会发布关于《通用人工智能实践守则》的评估意见。欧盟委员会从以下方面对守则进行评估：（1）该守则是否覆盖《人工智能法》第 53 条和 55 条规定的义务：守则通过“透明度”“版权”和“安全与系统性风险”三个章节，分别覆盖了通用人工智能提供者的文档义务、版权合规政策，以及高风险模型的风险识别、评估、缓解和重大事故报告等要求。委员会评估认为整体覆盖充分；（2）是否包含实现目标的措施和报告机制：守则通过“承诺+措施”的形式提出操作性要求。透明度和版权部分主要依赖文档、政策和流程，而安全与系统性风险部分则要求提供者定期向 AI Office 提交相关报告，便于监管方掌握风险状况；（3）是否兼顾相关利益方需求：守则在制定过程中吸纳产业界、学界、社会组织、下游提供者及权利人意见。（来源：欧盟委员会）

2. 亚太经合组织数字和人工智能部长会议召开，就人工智能发展发布联合声明

8 月 4 日至 6 日，亚太经合组织（APEC）数字和人工智能部长会议在韩国仁川召开。本次会议围绕“创新”“互联”“安全”三个议题展开讨论。一是“推动 ICT • 数字 • 人工智能创新以应对挑战”。各成员经济体分享人工智能与数字政策及创新案例，探讨利用新兴数字技术提升生产效率、应对社会问题的方案；二是“增强普惠性和有意义的数字互联”。会议强调消除数字鸿沟、强化数字素养，以及扩大基于人工智能的云计算与下一

代通信基础设施投资的必要性；三是“构建安全可信的数字·人工智能生态系统”。

本次会议还讨论通过《亚太经合组织数字和人工智能部长声明——迈向共同繁荣和可持续发展的数字化与人工智能转型》。声明明确三大关键行动领域：一是促进数字与人工智能创新以应对社会经济挑战。该声明呼吁，各经济体应以负责任的方式安全运用信息通信技术与人工智能等数字技术，提升生产力，提高效率和韧性，培育支持经济发展的创新路径。二是为所有人增强数字连接。该声明指出，随着信息通信技术和数字技术对于经济发展的影响增强，普遍和有意义的数字连接的重要性显著提升，需要弥合经济体内部和经济体之间的数字鸿沟，包括阻碍个人充分参与数字经济的数字鸿沟。三是构建安全可信与可靠的数字与人工智能生态。该声明强调，随着数字化转型的推进，确保安全、保障、可访问性、可信度和可靠性是实现数字化惠及所有人的关键。（来源：亚太经合组织）

3. 巴西总统签署制定《国家网络安全战略》行政令

8 月 5 日，巴西总统签署制定《国家网络安全战略》行政令，旨在加强巴西的网络安全成熟度和治理水平。行政令指出，该战略框架包括：公民与社会的保护及意识提升、基本服务与关键基础设施的安全与韧性、公私机构合作与整合、国家主权与治理等内容。

一是公民与社会保护及意识提升。行政令指出战略要为弱势群体创造可以安全使用的网络环境，主要措施包括：（1）推动安全网络行为；（2）

扩展网络犯罪受害者支持服务；（3）将网络安全纳入教育课程；（4）促进公私协作打击网络犯罪；（5）完善网络犯罪举报渠道及执法能力。

二是基本服务与关键基础设施安全与韧性。行政令提出战略要预防和应对网络事件，主要措施包括：（1）推动高风险行业实施风险管理；（2）建立国家网络安全高风险清单及认证标志；（3）鼓励采用网络安全保险；（4）定期开展行业韧性演练。

三是公私机构合作与整合。行政令认为战略要促进国内外网络安全信息交流，主要措施包括：（1）建立网络事件响应团队和国家级信息共享中心；（2）加强国际合作及参与国际论坛等。（来源：巴西政府）

4. 韩国发布《生成式人工智能开发与应用个人信息处理》指南

8 月 6 日，韩国个人信息保护委员会发布《生成式人工智能开发与应用个人信息处理》指南，旨在为企业和机构在开发、部署生成式人工智能服务过程中提供清晰的个人信息保护依据，减少法律适用不确定性，推动合规和创新并行。

指南提出生成式人工智能全生命周期的四个主要阶段——目的设定、策略制定、训练与开发、应用与管理，并针对各阶段明确最低限度的安全措施与法律考量，包括信息主体权利保障、数据合法获取与使用、开发过程中的数据污染防控、多层次安全机制及治理结构建设等。此外，指南还结合韩国在医疗、公共、金融等领域积累的大规模数据资源背景，提出以首席隐私官（CPO）为核心的治理框架，鼓励企业通过迭代优化持续完善系统。

指南同时纳入近期政策与执法实践，包括事前实态检查、监管沙盒与适正性审查，并结合具体案例提供法律解读和风险缓解措施。指南亦关注最新技术趋势，如人工智能代理、知识蒸馏及机器学习等，以确保其与国内外隐私保护政策演变相适应，并计划随技术发展持续更新。（来源：韩国个人信息保护委员会）

5. 德国 BSI 与法国 ANSSI 联合发布《零信任 LLM 系统设计原则》

8 月 11 日，德国联邦信息安全局（BSI）和法国国家信息系统安全局（ANSSI）联合发布《零信任 LLM 系统设计原则》。

文件主要内容包括：一是认证与授权。所有用户、代理的每次交互均需实时认证授权，实施动态访问控制和最小权限原则，禁用 LLM 自身认证功能；二是输入输出限制。严格验证/过滤所有输入输出数据，通过网关检测信任度、标签区分来源可信度、信任算法动态评估等方式，并设置“护栏”阻止有害内容生成；三是沙盒隔离。强制隔离用户会话、内存及环境，限制插件权限，敏感操作需断开网络；确保上下文不含敏感信息，开发/生产环境分离；四是实时监控、报告和控制。持续观察和记录所有请求，部署异常检测和自动响应机制，对用户和设备实施令牌限制，定期进行测试；五是威胁情报整合。主动收集分析新型攻击手法，通过威胁情报源阻断恶意 IP，定期审计并移除受损组件；六是安全意识培养。对开发者和用户进行攻击案例培训，明确“不盲信人工智能输出”，提升系统决策透明度及风险认知。（来源：德国联邦信息安全局）

6. 英国《数据（使用与访问）法》首批条款届期生效

8 月 20 日，英国《数据（使用与访问）法》首批条款届期生效。该批条款的实施重点在于开放客户数据与商业数据的使用，推动市场竞争和数字经济发展。

该阶段生效的主要内容包括：（1）客户数据与商业数据的相关定义：明确“客户数据”和“商业数据”的范围，界定“数据持有人”“交易者”“授权第三方”等概念，奠定法律适用的基本框架；（2）客户数据的提供义务：客户有权要求数据持有人提供其客户数据，或经客户授权，提供给特定的第三方服务商。此条还允许客户要求更正不准确的数据；（3）客户数据的补充规定：规范客户授权程序、请求方式、数据提供频率、使用接口，并规定数据持有人需建立投诉与争议解决机制；（4）商业数据的提供与公开：规定数据持有人可被要求向客户或其他指定第三方公开或提供商业数据，包括价格、服务质量、用户反馈等，以提升市场透明度；（5）决策者机制：建立“决策者”制度，负责判定第三方是否符合接收数据的资格，并可监督、撤销授权，保障制度公正性等。（来源：英国政府）

7. 联合国批准成立首个人工智能治理小组，并决定建立全球人工智能治理对话机制

8 月 26 日，联合国大会在第七十九届会议上正式通过《人工智能独立国际科学小组和人工智能治理全球对话的职权范围和设立及运作方式》决议。联合国将设立由专家组成的人工智能小组，以评估人工智能风险、机

遇和影响。此外，联合国将开展全球对话，开展政策讨论并达成共识，以加强全球人工智能治理，支持可持续发展目标并弥合数字鸿沟。

同时，大会决定建立全球人工智能治理对话机制，为各利益相关方提供讨论国际合作、分享最佳实践和经验教训的包容性平台，旨在通过国际互动缩小全球数字鸿沟并落实可持续发展目标。工作重点包括：（1）开发安全、可靠且值得信赖的人工智能系统；（2）弥合人工智能能力差距，借助现有的联合国及多利益攸关方机制，支持发展中国家开展人工智能能力建设，进而弥合人工智能鸿沟、便利人工智能应用程序的使用，并建立高性能计算相关能力与配套技能；（3）关注人工智能在社会、经济、伦理、文化、语言和技术层面的影响；（4）推动提升人工智能治理方法的互操作性与兼容性等。（来源：联合国）

8. 法国 Bouygues 电信遭网络攻击，640 万客户账户信息泄露

8 月 4 日，法国第三大移动通信运营商 Bouygues Telecom 遭遇严重网络攻击，导致 640 万名客户的个人信息及银行账户数据被非法访问。黑客通过未授权方式侵入其客户数据库，获取包括银行国际账户号码、联系方式、合同资料以及部分商业客户企业信息在内的敏感数据。

公司警告称，客户可能因此面临诈骗风险，犯罪分子或以 Bouygues Telecom、银行、保险等机构名义进行钓鱼邮件或电话诈骗，试图获取银行卡号、登录信息等敏感数据。公司提醒客户切勿泄露账户信息和密码，如接到可疑来电，应立即挂断并通过官方渠道联系银行或顾问。公司提醒客

户及时核查账户扣款情况，并依据银行规定在 13 个月内对未经授权的扣款提出异议。

目前，公司已将此次事件通报法国国家信息与自由委员会（CNIL），并向司法机关提交正式投诉。但公司尚未公布漏洞被封堵的具体时间，也未明确攻击持续的时长。（来源：Bouygues）

9. 加拿大众议院遭网络攻击致敏感员工信息泄露

8 月 14 日，加拿大下议院及国家网络安全机构近日正在调查一起重大数据泄露事件。据内部邮件披露，一名身份不明的“威胁行为者”利用微软系统的最新漏洞，非法访问用于管理计算机和移动设备的数据库，导致政府雇员私人信息外泄。

该事件于 2025 年 8 月 8 日发生，下议院于 8 月 11 日向员工发出通知称包括雇员姓名、职务、办公地点、电子邮件地址以及与其工作设备相关的部分非公开信息遭窃取。加拿大通讯安全局已介入协助应对并开展初步调查。目前尚未确认攻击来源。

下议院呼吁所有员工及议员提高警惕，防范因信息外泄可能引发的诈骗或身份冒用风险。官方尚未披露受影响员工数量。（来源：cbc 新闻）

10. 美国 FTC 判决 Workado 公司对其人工智能内容检测产品虚假宣传

8 月 28 日，美国联邦贸易委员会（FTC）正式批准针对 Workado 的禁令，要求该公司在缺乏充分可靠证据支持的情况下，不得继续宣称其人工智能内容检测产品具有所声称的准确性或有效性。

Workado 公司面向消费者推出的“人工智能内容检测器”，主要用于判断文本内容是由人类撰写还是通过生成式人工智能技术生成。该公司曾声称，该检测器通过整合博客文章、维基百科条目等广泛材料进行训练，可为普通用户提供更高准确性。但根据 FTC 于 2025 年 4 月提起的诉讼，驱动该检测器的人工智能模型实际仅针对学术类内容进行了专门训练或优化。

这项最终禁令旨在杜绝 Workado 公司再次进行类似虚假、误导性或缺乏依据的广告宣传。根据禁令条款，Workado 公司必须遵守以下规定：（1）禁止对其人工智能内容检测产品的效果作出任何误导性陈述，且所有宣传主张必须在发布时具备充分可靠的证据支持；（2）保存所有支持产品功效声明的证据材料；（3）通过电子邮件通知符合条件的消费者有关禁令及与 FTC 达成和解的情况；（4）在禁令颁布一年后及随后三年内，每年向 FTC 提交合规报告。（来源：美国联邦贸易委员会）

行业前沿观察一：2025 年国家网络安全宣传周开幕；《国家网络安全事件报告管理办法》发布；《关于推进“宽带林草”建设的通知》发布；“京粤港澳互联 共育网安新星——‘京粤汇’大湾区研学夏令营”成功举办；

导读：8 月 17 日-23 日，一场汇聚智慧、链接未来的人才培养之旅——“京粤港澳互联·共育网安新星——‘京粤汇’大湾区研学夏令营”成功举办；9 月 15 日，2025 年国家网络安全宣传周开幕式在云南省昆明市举行。

近日，国家互联网信息办公室发布《国家网络安全事件报告管理办法》（以下简称《办法》），自 2025 年 11 月 1 日起施行。《办法》共十四条，主要对网络安全事件报告适用范围、监管职责、报告主体、报告流程、报告时限、报告内容等提出规范要求。

据工业和信息化部官网，工业和信息化部、国家林业和草原局联合发布了《关于推进“宽带林草”建设的通知》。“宽带林草”总体目标是，到 2027 年底，林场（所）驻地通 4G/5G 网络比例达到 90%，人口聚居区、重点防火瞭望塔等重要点位 4G/5G 网络覆盖水平明显提升，国家级自然保护地等范围内的关键点位基本实现宽带网络覆盖，穿越林区和草原的国道和重点省道沿线按需实现 4G/5G 网络覆盖。

关键词：互联网、人工智能、网络安全、网信办、AI

1.“京粤港澳互联·共育网安新星——‘京粤汇’大湾区研学夏令营”成功举办！

8 月 17 日-23 日，一场汇聚智慧、链接未来的人才培养之旅——“京粤港澳互联·共育网安新星——‘京粤汇’大湾区研学夏令营”成功举办，来自北京高校的 10 名网络安全相关专业优秀学生和 2 名领队老师，怀揣对互联网科技和网络安全技术的热情与向往，从首都奔赴广州、深圳、香港、澳门、珠海等粤港澳大湾区核心城市进行了为期一周的网安研学之旅。

本次夏令营活动由北京市教育委员会为指导单位，北京网络空间安全协会、广东省网络空间安全协会、香港网络空间安全协会为主办单位，广州网络空间安全协会为承办单位，香港城市大学、澳门大学、澳门国际科技产业发展协会为协办单位，广州华南检验检测中心有限公司、国源天顺科技产业集团有限公司为支持单位。活动的成功举办，标志着“京津冀+粤港澳”两大区域在网络安全人才培养领域的协同合作迈入了崭新的阶段。

活动以网络安全为主题，深入贯彻落实习近平总书记关于网络强国的重要思想，立足于粤港澳大湾区战略定位，旨在充分发挥北京网络安全资源优势与广东科研创新优势，深度融合广东及港澳地区在高校科研创新与前沿产业实践方面的领先动能，为学员提供前沿技术培训、攻防演练实践及产学研用一体化课程。

为期七天的活动中，学员们探访了腾讯科技、小鹏汽车、奥威亚科技、安恒信息、联通（广东）等网络安全、通信、科技领域的领军企业，探访了国家级科研机构及关键信息基础设施单位解密智慧城市安全防护体系，

参访白云区数据安全监测和运行中心，实时跳动的数据监测大屏、精准的风险预警系统，让学子们直观感受到城市级数据安全防护的“广州方案”。走访了香港中文大学、香港城市大学、澳门大学、广东省网络空间安全协会、澳门国际科技产业发展协会等湾区名校和网络社会组织，开展了网络安全技术交流和攻防演练，走进了黄埔军校旧址、辛亥革命纪念馆等红色教育基地，参观探索了香港星光大道、澳门回归纪念馆、渔人码头、珠海日月贝等湾区城市印记.....在七天六城的丰富行程中汲取湾区“科技创新+历史底蕴”并存沃土的丰厚营养。在这过程中开展前沿技术培训，攻防演练实践，产学研用一体化培训，与顶尖企业安全专家进行零距离分享、交流，提升自我思想高度和网络安全实战技能，为筑牢国家网络安全防线贡献出更加磅礴的青春智慧与力量。

粤港澳大湾区作为国家科技创新中心的核心承载地和国家网络安全的“南大门”，以其汇聚的“国之重器”和深厚的红色底蕴，成为了未来网安人才梦想启程的“练兵场”。

2.2025 年国家网络安全宣传周开幕式在云南昆明举行

9 月 15 日，2025 年国家网络安全宣传周开幕式在云南省昆明市举行。中央宣传部副部长、中央网信办主任、国家网信办主任庄荣文出席开幕式并讲话，云南省委书记、省人大常委会主任王宁出席开幕式并致辞。云南省委副书记、省长王予波主持开幕式。

庄荣文指出，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。党的十八大以来，我们深入学习贯彻习近平总书记关于网络强国的

重要思想，贯彻落实总体国家安全观，扎实推进关键信息基础设施安全保护、网络数据安全管理、人工智能安全治理等重点工作，全面加强网络安全保障体系和能力建设，国家网络安全工作迈上新台阶。

庄荣文强调，要深刻把握网络安全工作面临的新形势新任务，大力推进国家网络安全体系和能力现代化，以高水平网络安全保障高质量发展。要强化系统思维，加强信息互通和工作衔接，将有关资源力量进行系统整合、统一调度，加强国家网络安全防御体系建设，打造体系化安全防护优势。要强化重点防护，统筹做好风险应对，完善应急预案、拓展应急手段、强化应急处置、加强应急演练，不断提升关键信息基础设施安全韧性，切实提高网络安全防护能力。要强化规范引导，深入实施“人工智能+”行动，不断完善人工智能安全监管制度和标准规范体系，促进人工智能健康有序发展。要强化融合发展，坚持网络安全教育、技术、产业发展相融合，加快形成人才培养、技术创新、产业发展相互促进的良性生态，夯实国家网络安全工作基础。要强化宣传教育，积极宣传网络安全理念，广泛普及网络安全知识，大力推广网络安全技能，构筑网络安全人民防线，形成网络安全共建共享局面。

王宁向国内外嘉宾表示欢迎。他说，云南深入学习贯彻习近平总书记关于网络强国的重要思想，全面落实总书记考察云南重要讲话精神，推动网信事业高质量发展，为现代化建设提供了有力支撑。安全、便捷、智慧、开放的网络已成为云南高质量发展、高水平开放的新优势。如今，安全便捷的网络铺就了边疆各族群众的“幸福路”，融入老百姓生活的方方面面，筑牢网络安全防线就是守护千家万户的幸福。安全智慧的网络织密了绿水青

山的“防护网”，开辟了生态保护治理新途径，筑牢网络安全防线就是夯实生态保护的“数字屏障”。安全开放的网络架起了区域交流合作的“连心桥”，“数字丝路”成为“一带一路”不可或缺的联通方式，筑牢网络安全防线就是护航畅通与繁荣。特别是随着昆明国际通信业务出入口局开通，云南将成为重要的国际通信枢纽，算力服务、数字文创、跨境电商、智慧物流等一批数字产业将卓然兴起。我们愿与大家共同推进网络安全技术创新，发展网络信息产业，为网络强国建设作出新的更大贡献。欢迎广大海内外专家学者、企业家和网络技术人才，来云南旅居创业，在线下享受“有一种叫云南的生活”，同时也在线上分享幸福、拥抱世界。

中国人民银行党委委员、副行长邹澜，国家广播电视总局党组成员、副局长刘建国出席开幕式并讲话。中央网信办副主任、国家网信办副主任杨建文，共青团中央书记处常务书记、全国青联主席徐晓，全国妇联副主席、书记处书记冯玲，国家市场监督管理总局党组成员、副局长柳军，中国电信集团有限公司党组副书记、总经理刘桂清，中国人民解放军网络空间部队信息工程大学校长蒋猛，全国总工会书记处书记潘健，全国政协委员、中国工程院院士吴世忠等出席开幕式。

开幕式上，庄荣文、王宁、王予波等共同出席 12387 网络安全事件报告平台启动仪式。开幕式后，与会领导嘉宾还参观了网络安全博览会。

本届网安周主题为“网络安全为人民，网络安全靠人民——以高水平安全守护高质量发展”，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等十部门联合举办。中央和国家机关有关部门负责同志，云

南省及有关省（区、市）有关方面负责同志，专家学者、企业和高校代表、新闻媒体记者以及港澳和国外嘉宾等共1200余人参加开幕式。

网安周期间，还将举办网络安全技术高峰论坛、网络安全博览会暨网络安全产品和服务国际推介会、网络安全和信息化人才招聘会、网络安全及数字产业投资会、主题日和网络安全“七进”等活动。

9月15日至21日，2025年国家网络安全宣传周在全国范围内统一开展。

3.国家互联网信息办公室发布《国家网络安全事件报告管理办法》

近日，国家互联网信息办公室发布《国家网络安全事件报告管理办法》（以下简称《办法》），自2025年11月1日起施行。

《办法》共十四条，主要对网络安全事件报告适用范围、监管职责、报告主体、报告流程、报告时限、报告内容等提出规范要求。

国家互联网信息办公室有关负责人指出，为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，落实《网络安全法》《关键信息基础设施安全保护条例》等法律法规，国家互联网信息办公室制定《国家网络安全事件报告管理办法》，进一步规范和明确网络安全事件报告流程和要求。

目前，网信部门已开通12387网络安全事件报告热线、官网、微信公众号、微信小程序、邮件、传真等六类网络安全事件报告渠道，网络运营者、社会组织和个人可通过上述渠道向网信部门报告网络安全事件。

国家网络安全事件报告管理办法

（2025 年 9 月 11 日 国家互联网信息办公室）

第一条 为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者，在发生网络安全事件时，应当按照本办法的规定进行报告。

第三条 国家网信部门负责统筹协调全国网络安全事件报告管理工作。省级网信部门负责统筹协调本行政区域内网络安全事件报告管理工作。

第四条 网络运营者在发现或获知涉及本单位的网络安全事件时，应当按照《网络安全事件分级指南》（见附件）进行研判，属于较大以上网络安全事件的，按以下程序报告：

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过 1 小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过 2 小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过4小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过1小时，并同时向同级有关部门通报。

本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告。

涉嫌违法犯罪的，网络运营者应当及时向公安机关报案。

第五条 网络运营者应当以合同等形式要求为其提供网络安全、系统运维等服务的组织或个人，及时向其报告监测发现的网络安全事件，并协助其按照本办法规定报告网络安全事件。

第六条 鼓励社会组织和个人报告所获悉的较大以上网络安全事件。

第七条 报告网络安全事件时，应当包括下列内容：

（一）涉事单位名称及涉事系统或设施基本情况；

（二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等；

（三）事态发展趋势及可能造成的进一步影响和危害；

（四）网络安全事件原因初步分析意见；

（五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等；

（六）拟进一步采取的应对措施以及请求支援事项；

（七）网络安全事件现场保护情况；

（八）其他应当报告的情况。

对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。

网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。

第八条 网络安全事件处置工作结束后，网络运营者应当于30日内对相关事件发生原因、应急处置措施、造成的危害、责任追究、完善整改情况、教训等进行全面分析总结，形成事件处置总结报告按照原渠道上报。

第九条 网信部门建设12387网络安全事件报告热线电话和网站、邮箱、传真等方式，统一接收网络安全事件报告。

第十条 网络运营者未按照本办法规定报告网络安全事件的，有关主管部门按照有关法律、行政法规的规定进行处罚。

因网络运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对网络运营者及有关责任人依法从重处罚。

承担网络安全事件报告的部门未按照本办法规定报告网络安全事件的，依据有关法律、行政法规和网络安全工作责任制追究相关单位和人员责任。

第十一条 发生网络安全事件时，网络运营者已采取合理必要的防护措施，按照应急预案进行处置、有效降低网络安全事件影响和危害，并按照本办法规定及时报告的，可视情从轻或不予追究相关单位和人员责任。

第十二条 本办法所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息

系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

本办法所指网络运营者是指网络的所有者、管理者和网络服务提供者。

本办法所指《网络安全事件分级指南》参照《信息安全技术 网络安全事件分类分级指南》国家标准（GB/T 20986-2023）制定，以有限枚举的方式给出相关事件的分级定量指标。

第十三条 涉及国家秘密的网络安全事件报告，按照有关部门规定执行。

第十四条 本办法自 2025 年 11 月 1 日起施行。

附件

网络安全事件分级指南

一、特别重大网络安全事件

符合下列情形之一的，为特别重大网络安全事件：

1.重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

2.核心数据、重要数据、海量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为特别重大网络安全事件：

1.省级以上党政机关门户网站、中央重点新闻网站因攻击、故障，导致 24 小时以上不能访问。

2.关键信息基础设施整体中断运行6小时以上或主要功能中断运行24小时以上。

3.影响一个或多个省级行政区50%以上人口，或者1000万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.核心数据、重要数据泄露或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

5.泄露1亿人以上公民个人信息。

6.省级以上党政机关门户网站、中央重点新闻网站、超大型网络平台等被攻击篡改，导致违法有害信息特大范围传播。以下情况之一，可认定为“特大范围”：

（1）在主页上出现并持续6小时以上，或在其他页面出现并持续24小时以上；

（2）通过社交平台转发10万次以上；

（3）浏览或点击次数100万以上；

（4）省级以上网信部门、公安机关认定为是“特大范围传播”的。

7.造成1亿元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

二、重大网络安全事件

符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

1.重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

2.核心数据、重要数据、大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为重大网络安全事件：

1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致6小时以上不能访问。

2.关键信息基础设施整体中断运行1小时以上或主要功能中断运行3小时以上。

3.影响一个或多个地市级行政区50%以上人口，或者100万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等的工作、生活。

4.核心数据、重要数据泄露或被窃取、篡改、仿冒，对国家安全和社会稳定构成严重威胁。

5.泄露1000万人以上公民个人信息。

6.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站，大型以上网络平台等被攻击篡改，导致违法有害信息大范围传播。以下情况之一，可认定为“大范围”：

（1）在主页上出现并持续2小时以上，或在其他页面出现并持续12小时以上；

（2）通过社交平台转发1万次以上；

（3）浏览或点击次数 10 万以上；

（4）省级以上网信部门、公安机关认定为是“大范围传播”的。

7.造成 2000 万元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

三、较大网络安全事件

符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

1.重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

2.重要数据、较大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为较大网络安全事件：

1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 2 小时以上不能访问。

2.关键信息基础设施整体中断运行 10 分钟以上或主要功能中断运行 30 分钟以上。

3.影响一个或多个地市级行政区 30%以上人口，或者 10 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.重要数据泄露或被窃取，对国家安全和社会稳定构成较严重威胁。

5.泄露 100 万人以上公民个人信息。

6.党政机关、企事业单位门户网站，重点新闻网站，网络平台等被攻击篡改，导致违法有害信息较大范围传播。以下情况之一，可认定为“较大范围”：

（1）在主页上出现并持续 30 分钟以上，或在其他页面出现并持续 2 小时以上；

（2）通过社交平台转发 1000 次以上；

（3）浏览或点击次数 1 万以上；

（4）省级以上网信部门、公安机关认定为是“较大范围传播”的。

7.造成 500 万元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

四、一般网络安全事件

除上述网络安全事件外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

注：本指南中的“以上”均包括本数。

4.工信部、国家林草局联合推进“宽带林草”建设

据工业和信息化部官网，工业和信息化部、国家林业和草原局联合发布了《关于推进“宽带林草”建设的通知》。“宽带林草”总体目标是，到 2027 年底，林场（所）驻地通 4G/5G 网络比例达到 90%，人口聚居区、重点防火瞭望塔等重要点位 4G/5G 网络覆盖水平明显提升，国家级自然保护地等

范围内的关键点位基本实现宽带网络覆盖，穿越林区和草原的国道和重点省道沿线按需实现4G/5G网络覆盖。

全文如下：

工业和信息化部 国家林业和草原局关于推进“宽带林草”建设的通知

工信部联通信〔2025〕192号

各省、自治区、直辖市通信管理局、林业和草原主管部门，新疆生产建设兵团林业和草原局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国广播电视网络集团有限公司、中国铁塔股份有限公司，大兴安岭林业集团，内蒙古、吉林长白山、龙江、伊春森工集团：

为贯彻落实党中央、国务院决策部署，加快提升林区和草原通信网络供给水平，支撑林区和草原高质量发展和高水平保护，服务美丽中国建设，现就推进“宽带林草”建设有关工作通知如下。

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入践行习近平生态文明思想，认真贯彻落实习近平总书记关于防灾减灾救灾重要指示精神，以加快林区和草原通信网络高质量发展为目标，以强化林区和草原通信基础设施建设要素保障、优化用地用林用草审批为重点，以促进资源双向开放共享为抓手，扎实推进林区和草原通信基础设施建设，加快先进网络和信息技术部署和应用，有力支撑林区和草原生态保护、火灾防控、经济转型，助力实现人与自然和谐共生。

到2027年底，林场（所）驻地通4G/5G网络比例达到90%，人口聚居区、重点防火瞭望塔等重要点位4G/5G网络覆盖水平明显提升，国家级自然保护地等范围内的关键点位基本实现宽带网络覆盖，穿越林区和草原的国道和重点省道沿线按需实现4G/5G网络覆盖。

二、重点任务

（一）深化重要点位网络覆盖

1．深化人口聚居区网络覆盖。持续深化林场（所）驻地、自然保护地管护站点、森林草原防火集中靠前驻防点、20户以上人口聚居区等宽带网络覆盖，加快向5G网络和千兆光网升级。按需拓展20户以下人口聚居区移动网络覆盖。升级扩容林场驻地至外部的传输网络，提升网络综合业务承载能力。

2．深化林草防火点位网络覆盖。探索适宜森林、草原、湿地及自然保护地等场景的宽带接入技术和组网方案，充分利用管护站、监测站、生态定位站、防火瞭望塔、森林草原防火靠前驻防点、监控塔等设施资源，按需拓展移动通信网络、移动物联网等覆盖范围，加大森林草原防火通信基础设施建设力度。

（二）加强重点区域网络建设

3．加强生产经营区域网络建设。加强林区和草原经营区光缆、基站等设施建设条件保障，灵活采用中频和低频5G基站，逐步推进5G网络向森林和草原牧区、林下种植、养殖、产品采集加工等区域延伸覆盖，提升移动通信网络覆盖广度和深度。拓展偏远山区以数字宽带自组网为主的森林防火专网覆盖范围。

4．加强自然保护地网络建设。结合国家公园、自然保护区、自然公园等各类自然保护地，以及世界自然遗产（自然与文化双遗产）、世界地质公园等用网需求和保障条件，合理选择光纤、微波、卫星等传输方式，积极优化移动和固定网络覆盖，提升重要点位网络接入能力，支撑加快数字化管理运营。

（三）优化网络建设施工环境

5．优化审批流程。按照《中华人民共和国森林法》第五十二条规定，在林地上修筑直接为林业生产经营服务的通信基础设施，符合国家有关部门规定标准的，由县级以上人民政府林业主管部门批准，不需要办理建设用地审批手续；超出标准需要占用林地的，应当依法办理建设用地审批手续。根据《自然资源部办公厅 国家林草局办公室关于推广江苏省、山东省临沂市用地用林联动审批典型经验做法的通知》（自然资办函〔2025〕47号）要求，各地林草主管部门要按照“只跑一次”“一个口进出”的目标，结合实际谋划推动用地用林等审批事项协同办理，优化流程、提高效率。

6．加快项目审批。各地林草主管部门要进一步做好林区和草原通信基础设施建设项目要素保障工作，主动指导并建立绿色审批通道，畅通沟通渠道，及时办理通信基础设施建设涉及的相关审核审批手续。对于申请材料齐全的用林用地项目，林草主管部门应在15个工作日内完成本级审查工作。

7．减免相关费用。各地林草主管部门要积极协调森工集团、国有林场等单位减免林区内通信基础设施建设涉及的林地补偿费、林木补偿费等费用，不得收取进场费、协调费、分摊费、管理费、资源占用费、通信设备

接入和挂载费等不合理费用，降低通信基础设施建设和运行维护成本；要积极协调有关林业设计单位减免林区内通信基础设施建设涉及的设计、评估等各类相关费用。

（四）提升网络维护和使用水平

8．加强运行维护。基础电信企业要加强通信基础设施运行维护，积极探索共管共维模式，定期开展巡检巡查，及时发现并处理故障隐患，为用户提供优质通信服务；可委托林业工作人员开展代维服务，共同做好林区网络日常运行维护。各地通信管理局要组织基础电信企业开展应急通信保障，积极配合林草主管部门做好森林草原火灾扑救等重大突发事件处置。基础电信企业在林区组织工程施工、巡检维护等过程中，林区经营单位要精简优化相关流程，提供通行便利。

9．发挥网络效能。充分发挥基础电信企业在通信专业运营、系统集成和通信资源等方面的优势，鼓励林区各单位与基础电信企业在信息化建设、通信网络维护、呼叫中心运营管理等方面开展深度合作。鼓励基础电信企业为林区森林防火预警监测系统、森林旅游服务平台、智慧林业云平台等信息化项目提供网络和算力等支持，为提升林区信息化建设水平、实现智慧林草提供保障。

三、保障措施

（一）建立协调机制。各地通信管理局会同林草主管部门及基础电信企业、林区经营单位等建立沟通协调机制，定期召开联席会议，按照电信基础设施共建共享要求，统筹建设需求、加强统一实施，合理安排建设计划，研究明确争议解决机制和协调程序，积极解决林区和草原通信基础设

施建设中遇到的问题。林区经营单位结合需求实际，进一步与基础电信企业签订有关合作协议，开展深度合作，推动林区网络深化覆盖。

（二）分类组织实施。各地林草主管部门梳理林区范围内人口聚居区、生产作业区、景区、自然保护地、国有林场、防火点位等各类重点场景以及国省道沿线重要点位，明确支持政策，细化电力引入等各项配套措施。各地通信管理局组织基础电信企业梳理上述点位通信网络覆盖情况，并结合林草主管部门和林区各单位已明确的支持政策和配套措施，在合理论证通信基础设施建设可行性基础上，分类分级明确建设计划，扎实开展施工建设。基础电信企业集团公司要保障“宽带林草”建设项目资金投入，在相关绩效考核中，统筹考虑各地公司“宽带林草”推进落实情况。

（三）强化工作引导。各地通信管理局会同林草主管部门建立定期通报制度，重点对本地林区和草原通信基础设施建设过程中的有益经验做法和正面案例，以及涉及流程多、审批难、费用高等方面负面案例，及时予以通报。工业和信息化部、国家林草局组织梳理全国范围内的典型做法和案例，适时在行业内予以通报。

（四）加强配套支持。各地林草主管部门在组织修建森林草原防火道路时，应优先考虑同步组织林区通信基础设施建设，对符合用地条件的公众通信基础设施，落实依规发放许可、开放公共设施等政策；积极推动将“宽带林草”建设项目以及其他涉及用林用草的通信基础设施建设项目纳入省级重点项目清单，给予林草要素保障。鼓励地方政府给予资金等各类政策支持“宽带林草”建设项目。

（五）促进合作共享。林区经营单位将林区和草原建筑物、防火瞭望塔和微波铁塔等各类资源向通信基础设施建设项目免费开放，并保障通信设施平等进入；承担瞭望塔加固、引电、供电、用地等配套设施建设，协助报装直供电；在杆塔、机房、传输引接等建设方面予以协调支持；为基础电信企业施工作业提供相应人力、特种车辆等支持和通行便利。铁塔、杆路等通信基础设施应向林业相关单位积极开放，支持加强森林防火、野生动植物保护、有害生物预防等监控检测感知设备建设。支持林区优先开展异网漫游，进一步推动网络开放共享、减少重复建设。

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，开展主题党日活动，举办高级研修班，召开全体会员大会，举行反诈知识普及、保密技能培训等活动。广东省网络空间安全协会举办“人工智能安全创新发展与人才培养”高级研修班；中关村可信计算产业联盟开展主题党日活动；沈阳市网络安全协会与银行联合开展反诈知识普及、保密技能培训等活动；宁波市计算机信息网络安全协会：召开教育行业工作委员会工作交流会；安徽省网络安全协会成功召开第三届第二次全体会员大会；湖南省网络空间安全协会走访数字湖南有限公司|深化网安合作，共筑数字湖南屏障；上海市信息安全行业协会召开2025上海网络安全产业创新大会；甘肃省商用密码行业协会举办甘肃省“密码法治陇原行——庆阳站”活动等。

关键词：选举、调查活动、论坛、网络安全、信息安全

1.广东省网络空间安全协会举办“人工智能安全创新发展与人才培养”高级研修班

为深入贯彻落实国家关于人工智能发展的战略部署，积极应对日益严峻的AI安全挑战,着力培养兼具创新能力和安全意识的高层次复合型人才，为我国在新一轮科技竞争中筑牢安全底座，2025年9月3日上午，由广东省人力资源和社会保障厅主办、广东省网络空间安全协会承办的“人工智能安全创新发展与人才培养”高级研修班开班仪式在广州成功举行。

广东省人力资源和社会保障厅专技处一级主任科员杨斌彬，广东省网络空间安全协会常务副会长方满意、副会长成珍苑等领导出席了高研班开班仪式。本次研修班吸引了来自广州、佛山、肇庆、潮州、惠州、茂名、清远、汕头、汕尾、韶关、云浮、中山等多个地区，从事人工智能领域相关工作，具备中高级职称（职业资格）的专业技术人员、经营管理人员以及在企事业单位有关管理岗位工作的154人通过线上和线下参加开班仪式，共同开启人工智能安全领域的知识盛宴。

2.中关村可信计算产业联盟开展主题党日活动

为纪念中国人民抗日战争暨世界反法西斯战争胜利80周年，进一步弘扬伟大抗战精神，近日，中关村可信计算产业联盟党支部会同会员单位党支部一同前往中国人民抗日战争纪念馆，开展了“铭记抗战历史 传承红色基因 砥砺奋进力量”主题党日活动。

参观过程中，全体党员、干部怀着崇敬的心情，在珍贵展品前驻足凝视，深入学习感悟。参观结束后，党员、干部们深受触动，一致表示此次参观学习是一次触及灵魂的精神洗礼和一堂生动深刻的党性教育课。

3.沈阳市网络安全协会与银行联合开展反诈知识普及、保密技能培训等活动

近期，浙商银行沈阳分行紧密联系沈阳市网络安全协会，在协会专业指导下深化反诈与保密领域的交流合作，联合开展反诈知识普及、保密技能培训等共建活动。通过一系列有力度、有温度、有创新的实践举措，分行既为群众财产安全筑起“防护墙”，也为自身稳健发展筑牢“安全网”，生动诠释了金融机构在社会治理与风险防控中的责任担当。

该行表示，未来将继续强化保密管理，创新反诈举措，深化多方协作——在与沈阳市网络安全协会的联动中凝聚安全合力，以更扎实的行动守护金融安全，既践行网络安全共建使命，也为社会治理贡献更多金融力量。

4.宁波市计算机信息网络安全协会：召开教育行业工作委员会工作交流会

9月8日，宁波市计算机信息网络安全协会召开教育行业工作委员会第二次会议，会上刘柏嵩会长致开幕词，他指出：随着人工智能的兴起，网络安全的范畴从传统领域的走向更新的发展，我们各高校既要管理好各种的网络领域，更好拓展视野研究新业态下的网络安全。

宁波市公安局网安支队吴益明大队长通报了今年宁波市攻防演练中高校行业暴露出来的一些问题，并提出了改进建议。会议还介绍了宁波大学网络安全的先进经验。北京天融信和北京蔷薇灵动科技的技术专家在会上做了技术交流。

5.安徽省网络安全协会成功召开第三届第二次全体会员大会

近期，安徽省网络安全协会第三届第二次全体会员大会成功召开。安徽省公安厅网安总队和安徽省民政厅社会组织管理有关领导，协会会长俞能海、秘书长吴文涛以及协会理事和会员代表、拟增补单位代表出席会议，协会副秘书长郭天奇、协会专家委员苗刚中主持会议。

会议的成功召开，为安徽省网络安全协会 2025 -2026 年的工作指明了方向，加强了协会与会员单位之间的沟通与协作，对于推动安徽省网络安全事业的高质量发展具有重要意义。

6.湖南省网络空间安全协会走访数字湖南有限公司|深化网安合作，共筑数字湖南屏障

为进一步深化网络安全领域政企协同，强化行业资源整合与技术交流，9 月 3 日，湖南省网络空间安全协会在理事长苏金树教授的带领下，前往数字湖南有限公司开展专项走访交流活动。

在数字湖南公司总经理石凌凡、相关部门负责人陪同下，协会一行参观了公司安全体系大屏。安全和科技部总经理燕玮现场讲解，汇报了公司在网络安全态势感知、风险预警及应急响应等方面的技术架构与实战能力。

协会主管单位省公安厅网络安全支队杨军副支队长、协会理事长苏金树教授向数字湖南公司颁发“副理事长单位”牌匾,标志着双方正式建立更深层次的协作关系。

7.上海市信息安全行业协会召开 2025 上海网络安全产业创新大会

8 月 28 日，2025 上海网络安全产业创新大会顺利召开。大会在上海市经信委和普陀区人民政府的指导下，由上海市信息安全行业协会、普陀区科学技术委员会主办，市经济信息化委总工程师裘薇、普陀区副区长周如意出席大会。上海市委网信办、市公安局、市通信管理局、市卫生健康委、国家金融监管总局上海监管局、市密码管理局等市级部门领导，各区安全主管部门负责同志，以及高校专家、企业代表共 300 余人出席活动。

作为上海网络安全领域的年度盛会，上海网络安全产业创新大会已连续举办 4 届，本次大会以“产业赋能 生态打造”为主题，重点围绕人工智能时代的网络安全产业发展开展思想交流、技术研讨和成果发布，加快推动网络安全产业高质量发展。

8.甘肃省商用密码行业协会举办甘肃省“密码法治陇原行——庆阳站” 活动

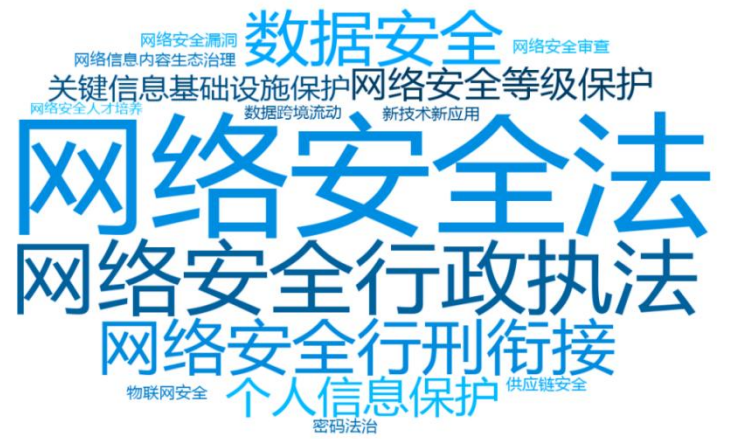
近日，作为 2025 年“全国网络普法行——甘肃站”系列重要活动之一，由由甘肃省国家密码管理局指导，甘肃省商用密码行业协会主办，庆阳市国家密码管理局承办的“密码法治陇原行——庆阳站”活动成功举办。甘肃省国家密码管理局与庆阳市委分管领导出席启动仪式并致辞。

此次活动聚焦商用密码技术在国家级算力枢纽建设中的支撑作用。来自庆阳市、县两级相关部门、各重要网络与信息系统运营单位负责同志、行业专家以及十余家密码领域头部企业代表，共计 150 人参加活动。

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

……